INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals

Sarah M. Mountin

90 INT'L L. STUD. 101 (2014)

Volume 90 2014

CONTENTS

The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals

Sarah M. Mountin[*]

I. INTRODUCTION

Commercial communication satellite systems have become essential and ubiquitous elements of almost every aspect of modern life.[1] Both civilian and military sectors[2] increasingly rely on satellites to advance important social, economic and military goals. Global communications are part of and inextricably tied to national and international economies, critical State and global infrastructures, national and international business, banking and financial systems, air traffic control, electricity grids, early warning systems and the mass media, as well as fully integrated into national security programs and military operations.[3] The space systems advancing these vital objectives and achieving these wide-ranging effects, however, are vulnera-

*B.S., University of Wisconsin- Madison; J.D., University of Wisconsin Law School; L.L.M., McGill University, Institute of Air and Space Law. The author is currently the Chief of Space Law for United States Strategic Command at Offutt Air Force Base, Nebraska. The views and opinions expressed in this article are those of the author alone and do not necessarily reflect those of the United States Department of Defense, the United States Air Force, or any other government agency.

1. David A. Koplow, *ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons*, 30 MICHIGAN JOURNAL OF INTERNATIONAL LAW 1187, 1190 (2009).

2. Deborah Housen-Couriel, *Disruption of Satellite Transmissions* ad Bellum *and* in Bello*: Launching a New Paradigm of Convergence*, 45 ISRAEL LAW REVIEW 431 (2012).

3. LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 1 (1998); Housen-Couriel, *supra* note 2, at 437.

ble. Their signal transmissions can be disrupted by unintentional, accidental or feckless operator errors, equipment malfunctions, poorly installed equipment, inadvertent misuse or uncoordinated use of the already congested radio frequency spectrum.[4]

More ominously, as this article will discuss, satellite signals have become increasingly attractive targets for intentional interference (the deliberate targeting and disruption of satellite signals intended to interrupt, degrade or limit the performance of the targeted signal) such as deliberate jamming[5] by State and non-State[6] actors.[7] "Jamming," a type of intentional interference, involves overloading targeted radio frequencies with so much electronic noise that communications cannot get through to their intended destinations.[8] Interference and disruptive jamming effects are accomplished non-kinetically and disturb the communications of the satellites (radio waves or links) on Earth and to and from satellites based in space.[9] Disruptions may also result from physical destruction of a satellite or ground stations relaying satellite transmissions.

Commercial communication satellite capabilities enable many components of modern societies. The strengths secured by these new advanced systems, however, means that their vulnerabilities serve as modern-day Achilles heels. So while more and more State and non-State entities depend

4. Ram Jakhu & Karan Singh, *Space Security and Competition for Radio Frequencies and Geostationary Slots*, 58 ZLW 79, 83–85 (2009); Mike Gruss, *Panel Ties U.S. Troop Rotations to Satellite Interference Spikes,* SPACE NEWS (June 24, 2013), http://www.spacenews.com/article/military-space/35948military-satellite-communications-panel-ties-us-troop-rotations-to#.Ue254RZsWR8; Ram Jakhu, Presentation delivered at the Radio Frequency Interference & Space Sustainability Panel Discussion, Washington, DC: Satellites: Unintentional and Intentional Interference (June 17, 2013) [hereinafter Jahku, *Satellites*].

5. JAMES G. SAVAGE, THE POLITICS OF INTERNATIONAL TELECOMMUNICATIONS REGULATION 134 (1989).

6. For example, the Falun Gong, a banned spiritual movement in China, has repeatedly jammed satellites based in China and Hong Kong and broadcast its own message. *See Falun Gong Jams Official Chinese TV*, WASHINGTON POST (July 9, 2002), http://articles.chicagotribune.com/2002-07-09/news/0207090078_1_falun-gong-li-hongzhi-hong-kong-based-human-rights-group.

7. HANK RAUSCH, JAMMING COMMERCIAL SATELLITE COMMUNICATIONS DURING WARTIME: AN EMPIRICAL STUDY: PROCEEDINGS OF THE FOURTH IEEE INTERNATIONAL WORKSHOP ON INFORMATION ASSURANCE, 2006 (2006).

8. SAVAGE, *supra* note 5, at 134.

9. Housen-Couriel, *supra* note 2, at 436.

on high-capacity satellite communications,[10] the electromagnetic waves carrying data that underlie communications lack adequate protections against deliberate interference and jamming.[11] Now the number of interference and jamming incidents are growing dramatically[12] and the frequency of such events is accelerating, as is the range of actors capable of exploiting signal vulnerabilities.

As this article will describe, modern-day satellite jamming often involves using crude techniques, sloppy in their application. Jamming intended for one signal often disrupts other signals.[13] For example, when the Libyan government jammed two telecommunication satellites in 2007, dozens of television and radio stations serving Britain and Europe were knocked off the air and American diplomatic, military and FBI communications were severely disrupted.[14]

Moreover, even though more than 80 percent of satellite jamming incidents historically have been precipitated by diplomatic and political differences among nations,[15] jamming is increasingly being employed to control, deny and degrade information needed for strategic, economic and military purposes.[16] Jamming is especially troublesome for the U.S. military because it relies on dual-use commercial satellites for 80 to 90 percent of its satellite communications needs.[17] Jamming also poses challenges for States when the effects are generated within their borders or by its citizens. As this article will describe, States may be held responsible for failing to contain and constrain jamming activities under international law and "States directly menaced [by jamming] can reasonably be expected to take measures against

10. Ronald C. Wilgenbusch & Alan Heisig, *Command and Control Vulnerabilities to Communications Jamming*, 69 JOINT FORCE QUARTERLY 56, 57 (2013), *available at http://www.ndu.edu/press/lib/pdf/jfq-69/JFQ-69_toc.pdf*.

11. *Id.* at 57.

12. Gruss, *supra* note 4.

13. SAVAGE, *supra* note 5, at 135.

14. Matthew Kleiman & Sonia McNeil, *Red Lines in Outer Space*, THE SPACE REVIEW (Mar. 5, 2012), http://www.thespacereview.com/article/2038/1.

15. Mohammad Ghazai, *Satellite Channel Jamming Rose Sharply After Arab Spring*, JORDAN TIMES (May 15, 2013), http://jordantimes.com/satellite-channel-jamming-rose-sharply-after-arab-spring.

16. Jakhu, *Satellites*, *supra* note 4.

17. Loren B. Thompson, *Lack of Protected Satellite Communications Could Mean Defeat for Joint Force in Future War,* LEXINGTON INSTITUTE EARLY WARNING BLOG (Apr. 14, 2010), http://www.lexingtoninstitute.org/lack-of-protected-satellite-communications-could-mean-defeat-for-joint-force-in-future-war.

such threats wherever they occur."[18] Moreover, if States are unable to take responsive measures, it may invite intervention by other States.

Intentional interference or jamming activities have not targeted only communication satellites. They present a growing problem for other dual-use systems such as the Global Positioning System (GPS).[19] In May 2012, South Korea accused the government of North Korea of interfering with and jamming GPS signals for over one thousand military and commercial airline flights and over 250 ships on three occasions between 2010 and 2012.[20] While none of the reportedly targeted flights or ships were subjected to serious danger,[21] the acts, if reported correctly, demonstrate an emerging reality and a growing global threat. The acts also underscore a serious concern for the global economic infrastructure because GPS signals, like commercial communication satellite signals, are so integrated into daily life and commerce that their disruption could hobble much of the global economy.[22]

Despite treaty attempts to prohibit harmful interference with satellite transmissions,[23] jamming incidents continue. Governments and the satellite industry have reacted to the growing problem of interference by applying political pressure on States where interference activities originate, and have developed new technologies to combat jamming and strengthen international regulatory regimes.[24] To date, however, such efforts are largely ineffective. States responsible for putting an end to interference within their borders often fail to take actions necessary to comply with their international obligations and frequently ignore calls to stop unlawful interference

18. MYRES S. MCDOUGAL, HAROLD D. LASSWELL & IVAN A. VLASIC, LAW AND PUBLIC ORDER IN SPACE 284 (1963).

19. Gruss, *supra* note 4.

20. Choe Sang-Hun, *Seoul Says North Korea Tries to Disrupt Air Navigation*, NEW YORK TIMES (May 2, 2012), http://www.nytimes.com/2012/05/03/world/asia/seoul-says-north-korea-tries-to-disrupt-air-navigation.html?_r=0; Jonathan Saul, *Governments Confront Rising Threat to Ships from Signal Jamming*, REUTERS (May 30, 2013), http://www.reuters.com/article/2013/05/30/shipping-navigation-gps-idUSL5N0E926V20130530.

21. Sang-Hun, *supra* note 20.

22. Frank Oliveri, *The Pentagon's GPS Problem*, CONGRESSIONAL QUARTERLY (Feb. 9, 2013), http://public.cq.com/docs/weeklyreport/weeklyreport-000004218242.html.

23. Constitution of the International Telecommunication Union art. 45*, reprinted in* COLLECTION OF THE BASIC TEXTS OF THE INTERNATIONAL TELECOMMUNICATION UNION ADOPTED BY THE PLENIPOTENTIARY CONFERENCE*,* 2011 (2011) [hereinafter ITU Constitution].

24. Jakhu, *Satellites*, *supra* note 4.

originating from their territory.[25] For example, the Iranian government was called upon several times between 2010 and 2012 by the International Campaign for Human Rights in Iran, the International Telecommunication Union (ITU), the European Union, the governments of the United Kingdom, United States and France, and the Broadcasting Board of Governors to put an end to interference and cease jamming of satellite broadcasts.[26] Iranian officials, however, have yet to take any visible efforts to comply with these requests.[27]

Further complicating the problem of satellite signal interference is that many States are reluctant to report jamming incidents; some suggest this is because these silent States too are developing and employing their own jamming technologies and capabilities for use against adversaries.[28] Moreover, the applicable international regulatory regimes do not contain substantive provisions requiring States to take forcible corrective actions to bring the interference and jamming to an end.[29] Thus, many States struggle with how to protect their interests against satellite signal interference, while at the same time preserving their own national prerogatives and freedom of action.

Satellite signal interference has become a growing phenomenon which poses serious social, political, economic and military consequences. This not only challenges existing legal frameworks applicable to satellite communications, namely international telecommunications law, international space law and international humanitarian law (IHL), but also finds interference occurs within an evolved political and technological reality that now calls for a reexamination of that framework.

---

25. *Satellite Jamming in Iran: A War Over Airways,* PBS (Nov. 2012), http://www.pbs.org/wgbh/pages/frontline/tehranbureau?satelliteJammingInIranSmallMedia.pdf.

26. *Id.*

27. The Iranian government sees satellite broadcasts originating from outside the country as a Western front in the "soft war" being waged against their rule and a "weapon" intent on undermining the country's religious and cultural beliefs. *Id.*

28. Many countries such as the United States, Russia, China, Iran, Cuba, Iraq and North Korea have military jamming capabilities. *See* TOM WILSON, COMMISSION TO ASSESS UNITED STATES NATIONAL SECURITY SPACE MANAGEMENT AND ORGANIZATION, THREATS TO UNITED STATES SPACE CAPABILITIES (2000), *available at* http://www.fas.org/spp/eprint/article05.html.

29. Ram Jakhu, *Regulatory Processes for Communications Satellite Radio Frequencies*, *in* THE HANDBOOK OF SATELLITE APPLICATIONS 271, 287 (Joseph N. Pelton, Scott Madry & Sergio C. Lara eds., 2013) [hereinafter Jakhu, *Regulatory Processes*].

Accordingly, this article addresses some of the rules applicable to satellite signal interference in peacetime, as well as during armed conflict. In doing so, this article first differentiates unlawful interference incidents that cause temporary, reversible, interruptions from those that could constitute a prohibited use of force under Article 2(4) of the Charter of the United Nations (UN). This article then asserts that, because unlawful interference with satellite signals can lead to devastating consequences and can pose a fundamental threat to States, satellite signal interference may, in certain circumstances, amount to an armed attack justifying the exercise of individual or collective self-defense pursuant to Article 51 of the Charter.

Understanding how satellite signal interference should be characterized in the international legal framework is important for a number of reasons. First, it helps States understand which legal regime applies. For instance, unlawful satellite signal interference not amounting to a use of force under Article 2(4) is governed by the regulatory regime under the ITU and under international space law. If, however, satellite signal interference were to constitute a use of force or rise to the level of an armed attack, international laws governing a decision to resort to the use of force (*jus ad bellum*) and laws governing the conduct of hostilities (*jus in bello*) would apply.

Second, determining the threshold for what constitutes a use of force in the context of satellite signal interference is important for understanding peacetime operations by States and militaries. Clarifying possibilities of permissible interference in peacetime dictates when treaty obligations are triggered, and determines whether and when UN Security Council authorization may be required.

Third, characterizing the legal implications of satellite signal interference is imperative because armed conflict has obvious consequences. Commercial communication satellites and their signals are and will continue to be targets due to the military's heavy reliance on these systems for communications and operations. Commercial systems usually provide cost-effective solutions to information requirements and allow for surge during crisis circumstances. It is therefore necessary for States to understand what rules apply in advance of armed conflict and the legal parameters of a legitimate response to satellite signal interference.[30]

30. Housen-Couriel, *supra* note 2, at 434–35.

II. THE IMPORTANCE OF SATELLITE COMMUNICATIONS AND THE GROWING THREAT OF INTENTIONAL INTERFERENCE WITH SATELLITE SIGNALS

Before considering the circumstances under which satellite signal interference may be unlawful and the permissible responses to such acts, it is important to briefly address the extent to which satellites are integrated into modern life. It is also imperative to explore why and how interference with satellite signals is emerging as a serious threat to space systems—military and civilian—all around the world. Without proper context, evaluating the emerging problem, its implications and the applicable normative frameworks would have little meaning.

A. The Emergence of Satellites in the Modern World

The exploration and use of outer space has rapidly expanded since Sputnik I, the first satellite launched into orbit by the Soviet Union in 1957.[31] Outer space is no longer the sole domain of the original dueling "space powers," the Soviet Union and the United States, and satellites are more useful now than was ever realized at the dawn of the "Space Age." Technological advances and scientific developments have made space more accessible to people everywhere,[32] and space-based technologies, specifically satellites and their transmissions, have become critically important to almost every aspect of modern day life.[33]

Decades ago, satellites were primarily used by the United States and the Soviet Union for maintaining peace and security through reconnaissance and intelligence-gathering; arms control monitoring and compliance; missile warning weapons detection; survivable strategic, global, and regional communications; meteorology; and precision navigation and timing systems.[34] Now, satellite-based technologies are indispensable to a variety of civilian, space, science and commercial applications, to include communica-

31. MANFRED LACHS, THE LAW OF OUTER SPACE: AN EXPERIENCE IN CONTEMPORARY LAW MAKING 1(1972).

32. Jakhu & Singh, *supra* note 4, at 74.

33. Koplow, *supra* note 1, at 1190.

34. Laura Grego, *A History of Anti-Satellite Programs*, UNION OF CONCERNED SCIENTISTS (Jan. 2012), http://www.ucsusa.org/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf; Elizabeth S. Waldrop, *Integration of Military and Civilian Space Assets: Legal and National Security Implications* 5 (2003) (unpublished LL.M. thesis, McGill University Institute of Air and Space Law).

tions, meteorology and remote sensing. For example, of the 1,046 satellites currently orbiting Earth, approximately 59 percent are used for communication purposes, 9 percent for remote sensing, 8 percent for navigation, 7 percent for military surveillance, 5 percent for space science and 4 percent for meteorology.[35] Additionally, the U.S. Air Force's GPS constellation, originally developed for military purposes, now provides the foundation for nearly all global commercial space-based navigation and timing.

1. Commercial Uses of Satellites

In 2001, Dr. Steven Lambakis of the U.S. Missile Defense Agency, noted "the services provided by communications satellites are woven into the fabric of our lives. They were, and are, the true catalyst for globalization, or the worldwide melding together of different financial and economic systems."[36] Commercial satellites relay hundreds of television programs and thousands of telephone calls at the same time.[37] Commercial satellites also provide global connectivity and enable instantaneous communications and sharing of critical human, social, political and economic information on a worldwide scale via the Internet.[38] Commercial satellites support voice, data and mobile networks when wired capabilities are absent,[39] supplement fiber networks and are integral to private networks transmitting financial transactions between banks.[40]

Commercial communication satellite systems are also important in maintaining the international economy, transportation systems and emergency services.[41] This is especially evident with the GPS satellite system,[42]

35. *UCS Satellite Database*, UNION OF CONCERNED SCIENTISTS, http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html (last visited Feb. 11, 2014); *see also* Koplow, *supra* note 1, at 1190.

36. STEVEN J. LAMBAKIS, ON THE EDGE OF EARTH: THE FUTURE OF AMERICAN SPACE POWER 15 (2001).

37. John E. Oberright, *Artificial Satellites*, NASA (2004), https://www.nasa.gov/worldbook/artificial_satellites_worldbook.html.

38 OLAF ACKER, FLORAN POTSCHER & THIERRY LEFORT, WHY SATELLITES MATTER: THE RELEVANCE OF COMMERCIAL SATELLITES IN THE 21ST CENTURY—A PERSPECTIVE 2012–2020 (2012), *available at* http://www.esoa.net/mwg-internal/de5fs23hu73ds/progress?id=CTYE8Rwtig.

39. *Id.*

40. *Id.*

41. Ryan McClure, *International Adjudication Options in Response to State-Sponsored Cyber-Attacks Against Outer Space Satellites*, 18 NEW ENGLAND JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW ANNUAL 431, 433 (2012).

which is integrated into smart phones, law enforcement operations, and the navigation and positioning of cars, airplanes, ships, as well as in the fleet management of trucks,[43] and many aspects of the world's economy and commerce,[44] e.g., the Society for World Interbank Financial Telecommunication (SWIFT) system of international monetary transfer. Without access to the SWIFT system, it is not possible to wire money or deposit a check sent from another country.[45]

Thousands of companies and governments around the world use GPS signals to timestamp contractual agreements and financial transactions.[46] The shipping industry relies on satellite navigation services to avoid underwater hazards and stay within shipping channels, and on commercial communications systems to talk with shipping centers, schedule port arrivals and report emergencies or maintenance requirements.[47] Even the On-Star service used in automobiles utilizes commercial communication and satellite navigation services to detect and report malfunctions, unlock doors and locate stolen cars, and for emergency response.[48] GPS is so integrated into modern life that a loss could have devastating effects. A disruption of GPS timing signals could disable cellular phone and computer networks around the world, disrupt the global banking and financial systems, and interrupt the operation of electrical power distribution systems.[49]

2. Military Uses of Satellites

Satellite technologies, applications and capabilities have also revolutionized military operations. Today, satellites are incorporated into almost all modern military weapons (e.g., precision-guided munitions and unmanned aerial

42. The United States operates the GPS system, China operates the BeiDou Navigation Satellite System, Russia operates the GLONASS system and Europe operates the Galileo system.

43. FRANCIS LYALL & PAUL LARSEN, SPACE LAW: A TREATISE 389–90 (2009).

44. Oliveri, *supra* note 22.

45. Joy Gordon, *The U.S. Embargo against Cuba and the Diplomatic Challenges to Extraterritoriality*, 36 FLETCHER FORUM OF WORLD AFFAIRS 63, 70 (2012).

46. LYALL & LARSEN, *supra* note 43, at 390; ACKER, POTSCHER & LEFORT, *supra* note 38.

47. Paul W. Gydesen, *What Is the Impact to National Security Without Commercial Space Applications* 9 (Air War College, Maxwell Air Force Base, Alabama, Research Paper, 2006), *available at* http://www.au.af.mil/au/awc/awcgate/awc/gydesen.pdf.

48. *Id.*

49. WILSON, *supra* note 28, at IV(B); Norman Martello, *Where in the World?*, 24 ELECTRIC PERSPECTIVES 14, 17 (Mar./Apr. 1999).

vehicles), operations, communications and command and control systems.[50] The U.S. military relies on satellites to gather intelligence, conduct surveillance and photoreconnaissance, locate and track troop and ship movement, enable precision-guided munitions, monitor weather patterns and detect missile attacks.[51] However, the United States is not alone in pursuing these technologies and applications; other countries including Russia and China increasingly rely on satellites for active military support and operations.[52]

U.S. military reliance on satellites for military operations, communications, and command and control is not a new phenomenon. During the first Gulf War, the "the first space war,"[53] the U.S. military relied on satellites to conduct military operations and provide instantaneous global communications.[54] The military communications element alone consisted of 118 mobile ground stations and twelve commercial satellite terminals that provided 329 voice and thirty message circuits that handled approximately seven hundred thousand telephone calls and 152,000 messages daily.[55] More than thirty-five thousand tactical radio frequencies were also used.[56]

3. The Military's Increasing Reliance on Commercial Satellites

Even though the U.S. military has long maintained its own satellite assets and network, it is now increasingly dependent on commercial space assets owned and operated by domestic, foreign and even international entities.[57] This is mostly due to greater cooperation between military and non-military

50. GREENBERG ET AL., *supra* note 3, at 1.

51. Michael N. Schmitt*, International Law and Military Operations in Space*, 10 MAX PLANCK YEARBOOK OF UNITED NATIONS LAW 89, 90 (2006) [hereinafter Schmitt, *Military Operations in Space*].

52. Grego, *supra* note 34; Housen-Couriel, *supra* note 2, at 438.

53. Ivan A. Vlasic, *Space Law and the Military Applications of Space Technology*, *in* PERSPECTIVES ON INTERNATIONAL LAW 385, 388 (Nandasiri Jasentuliyana ed, 1995).

54. Jackson N. Maogoto & Steven Freeland, *Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?,* 41 INTERNATIONAL LAWYER 1091, 1104 (2007).

55. Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARVARD INTERNATIONAL LAW JOURNAL 272, 282 (1996), citing ALVIN TOFFLER & HEIDI TOFFLER, WAR AND ANTI-WAR: MAKING SENSE OF TODAY'S GLOBAL CHAOS 79 (1993).

56. Kanuck*, supra* note 55, at 282, citing TOFFLER & TOFFLER, *supra* note 55, at 69–70.

57. Waldrop, *supra* note 34 at 1, 17–18.

entities over the past few decades,[58] as well as the military's desire to capitalize on technical expertise and avoid duplicating efforts.[59] Additionally, the technologies and applications employed on commercial satellites are inherently dual-use in nature, and thus capable of providing the military with communications and data needed to operate.[60]

Almost all satellites in orbit are dual-use, that is, they can perform missions supporting both military and civilian applications. Commercial remote sensing satellites allowing us to view our neighborhoods from outer space on Google Earth can also be used to track military operations in conflict.[61] GPS navigation and timing signals directing civilians to gas stations and supermarkets are tied into ATMs, the power grid and cellular phone systems, and are used by over eight hundred thousand U.S. military receivers.[62] Commercial satellites enabling video chat via computers with friends across the country and around the world also allow operators to surf the Internet on international flights and also carry between 80–90 percent of all U.S. military communications,[63] making the U.S. military the global satellite communication industry's biggest single customer.[64]

U.S. military operational needs for versatile communications and bandwidths[65] have increased so rapidly that military satellites are no longer able to meet ever-expanding demands.[66] The U.S. military increasingly looks to commercial operators to provide more and more services, and even turns to foreign providers and States for help. In fact, the U.S. military's burgeoning thirst for satellite communications and bandwidth over the African continent is swelling so fast the United States recently signed a one-year, ten million dollar lease with the Chinese company operating the

58. *Id.* at 6–9.

59. Paul B. Stares, *Space and U.S. National Security*, *in* NATIONAL INTERESTS AND THE MILITARY USE OF SPACE 41 (William Durch ed., 1984).

60. Robert W. Jarman, *The Law of Neutrality in Outer Space* 6–7 (2008) (unpublished LL.M. thesis, McGill University Institute of Air and Space Law).

61. Matthew Burris, Presentation online U.S. Air Force JAG Corps: U.S. Space Security: History, Law & Policy (Apr. 25, 2013).

62. *Id.*

63. Thompson, *supra* note 17.

64. Gruss, *supra* note 4.

65. Over the past few decades, satellites are increasingly used by the military during peace and in war as "force multipliers" and "force enablers" to improve performance, lethality and effectiveness of ground, air and naval forces, as well as weapons. Stares, *supra* note 59, at 35.

66. Jakhu & Singh, *supra* note 4, at 82.

Apstar-7 satellite.[67] While some U.S. officials and military pundits publically and loudly expressed concern over data passing through Chinese space assets because China is a potential military competitor, the fact remains: "Every new drone feed and every new soldier with a satellite radio creates more appetite for bandwidth—an appetite the military can't hope to fill with military spacecraft alone."[68] This trend of relying on commercial and foreign satellite providers is unlikely to abate in the near future because, as noted by U.S. Air Force Space Commander, General C. Robert Kehler, "space capabilities . . . are embedded in all of our combat operations. They're also embedded in our military operations, short of combat, across the board. . . . [W]e cannot fight the way America fights without space capabilities."[69] Finally, U.S. national space policy encourages the support of U.S. commercial space activities by requiring the "[p]urchase and use [of] commercial space capabilities to the maximum practical extent when such capabilities and services are available in the marketplace and meet United States Government requirements."[70]

Satellites have evolved significantly over the last sixty years. Satellites not only improve the lives of billions of people everywhere, they also fundamentally change the way the world communicates, conducts business, governs and provides education, and transforms the way militaries fight and win wars.[71] At the same time, however, such overwhelming dependence on commercial communication satellites and their transmissions presents a national security vulnerability that has become an attractive target for exploitation by potential State and non-State adversaries.

B. Emerging Threats to Commercial Communication Satellites

1. Kinetic Weapons and the Space Debris Problem

Spacefaring nations will likely pursue non-kinetic measures that are both temporary and reversible within outer space in future conflicts due to the

67. Noah Shachtman, *Pentagon Paying China—Yes, China —To Carry Data*, WIRED (Apr. 29, 2013), http://www.wired.com/dangerroom/2013/04/china-pentagon-satellite/.

68. *Id.*

69. Kate Rust, *Kehler: 'The Future of Space is Now,'* AIR FORCE SPACE COMMAND (Dec. 7, 2007), http://www.afspc.af.mil/news/story.asp?id=123078666.

70. Office of the President of the United States, National Space Policy of the United States 10 (2010).

71. GREENBERG ET AL., *supra* note 3, at 1.

environmental threat caused by kinetic weapons and the expense in deploying traditional anti-satellite weapons. Until recently, it was thought that to disrupt or disable a satellite system, an adversary needed to either destroy a satellite's Earth-based station or the satellite itself[72] by way of kinetic attacks through the use of anti-satellite weapons (ASATs),[73] which are "direct ascent and co-orbital systems that employ various mechanisms to affect or destroy an on-orbit spacecraft."[74] ASATs include high-altitude nuclear explosions, kinetic-energy weapons, directed energy weapons and ballistic missiles.[75] However, only a few well-financed State actors with the requisite sophistication and technical know-how can acquire and deploy ASAT weapons.[76] Kinetic attacks are also very expensive and responsibility for such attacks can easily be attributed with relative certainty.[77] Moreover, physically destroying a satellite seriously threatens the long-term space environment by creating hundreds of thousands of pieces of space debris.

Space debris is one of the greatest concerns with employing kinetic ASATs because "what goes up" does not necessarily come down.[78] An object launched into space must either be brought back down to Earth by deliberate deorbiting, or, depending on its orbit, the object will fall out of orbit to return to Earth.[79] Generally, the further out into space an object is located, the longer it will take to reenter Earth's atmosphere. Atmospheric phenomenology, solar events, and object mass, shape and density also affect the equation on how soon an object will deorbit. Space objects and debris located in low earth orbit (LEO), an altitude of approximately 65–310 miles (104–500 kilometers) above Earth's surface,[80] can reenter Earth's atmosphere in approximately ten years.[81] Debris orbiting further away, however, such as within the geosynchronous orbit (GEO) at an altitude of

72. Kleiman & McNeil, *supra* note 14.

73. *Id.*

74. U.S. Department of the Air Force, AFDD 2-2.1, Counterspace Operations 33 (2004).

75. For an excellent discussion on ASATs, see Brandon L. Hart, *Anti-Satellite Weapons: Threats, Laws and the Uncertain Future of Space* (2007) (unpublished LL.M. thesis, McGill University Institute of Air and Space Law).

76. *Id.*

77. *Id.*

78. LYALL & LARSEN, *supra* note 43, at 96.

79. *Id.* at 96–97.

80. *Id.* at 245–46.

81. *Id.* at 96.

approximately 22,000 miles (35,400 kilometers)[82] can remain in orbit for hundreds of years.[83] Regardless of where space debris is located in outer space, satellite operators must continually manage and minimize collision risks.

A single collision can be catastrophic. Such an event, involving sufficiently large objects and satellites, can produce hundreds of thousands of fragments,[84] which, depending on the orbit, can trigger other collisions, thereby causing a cascade of subsequent collisions.[85] Put another way, not only is there a prompt and pervasive debris environment, but also additional collisions with that debris imperil space objects and make orbits completely unusable, especially if debris continues to collect indefinitely.[86]

The extent of the problem of space debris was brought to the fore on January 11, 2007 when the Chinese launched a solid-fuel, medium range ballistic missile at its own weather satellite, Feng-Yun-1C.[87] When the missile collided with the Chinese satellite, it created a debris cloud containing over two million pieces measuring between one millimeter and one centimeter, over forty thousand pieces of debris between one centimeter and ten centimeters (slightly larger than a baseball)[88] and over nine hundred pieces of trackable debris measuring over ten centimeters.[89] The smaller pieces cannot be tracked. A piece larger than one centimeter can destroy a satellite, damage the space shuttle and ruin an astronaut's day.[90]

---

82. *Id.* at 246.

83. Theresa Hitchens, *Debris, Traffic Management, and Weaponization: Opportunities for and Challenges to Cooperation in Space*, 14 BROWN JOURNAL OF WORLD AFFAIRS 173, 175 (2007) [hereinafter Hitchens, *Debris*].

84. LYALL & LARSEN, *supra* note 43, at 305.

85. *Id.*

86. David Finkleman et. al., Center for Space Standards and Innovation Analytical Graphics, Inc., *Space Debris Birth to Death Analysis from Concern to Consequences,* http://www.amostech.com/TechnicalPapers/2008/Orbital_Debris/Finkleman.pdf (last visited Feb. 11, 2014).

87. Brian Weedon, *2007 Chinese Anti-Satellite Test Fact Sheet*, SECURE WORLD FOUNDATION (Nov. 23, 2010), http://swfound.org/resource-library/international-security-and-space/ (then 2007 Chinese Antisatellite Test Fact Sheet hyperlink); Hart, *supra* note 75, at 1.

88. Hitchens, *Debris*, *supra* note 83, at 175.

89. Weedon, *supra* note 87; Hart, *supra* note 75, at 1–2; Noah Shachtman, *China Space Attack: Unstoppable*, HUFFINGTON POST (Jan. 18, 2007), http://www.huffingtonpost.com/noah-shachtman/china-space-attack-unstop_b_38999 .html.

90. John Kelly, *Debris is Shuttle's Biggest Threat*, SPACE.COM (Mar. 5, 2005), http://www.space.com/792-debris-shuttle-biggest-threat.html; Tariq Malik, *Station Astro-*

Within minutes of the Chinese ASAT event, a debris cloud started spreading through the satellite's original orbital plane.[91] Ten days later, the debris cloud spread through the entire orbital plane, resulting in a "ring" of debris,[92] orbiting at speeds up to 29,400 miles per hour (seventeen times the speed of a bullet fired from a machine gun).[93] Three years later, the debris was spread throughout much of LEO.[94] Most of the debris will remain in orbit for decades, thereby posing a collision threat to other space objects,[95] including the International Space Station. The debris threatens several hundred satellites on a daily basis and will remain in orbit for over one hundred years.[96] With these points in mind, it is easy to see how and why destroying a satellite through kinetic means is a significant threat to the space environment, and is increasingly seen by many States as a method of last resort.[97]

2. Non-Kinetic Satellite Signal Interference

Over the last few years, non-kinetic threats to space systems have emerged. One of these threats garnering significant attention is computer network attacks (CNAs).[98] Another much less sophisticated threat is intentional interference with satellite signals. While CNAs are increasingly recognized as a significant threat, little attention is paid to intentional interference with

nauts Take Shelter from Space Debris, SPACE.COM (Mar. 12, 2009), http://www.space.com/6410-station-astronauts-shelter-space-debris.html.

91. Weedon, *supra* note 87.

92. *Id.*

93. Hart, *supra* note 75, at 2.

94. Weedon, *supra* note 87.

95. *Id.*

96. Hitchens, *Debris, supra* note 83, at 175.

97. Grego, *supra* note 34.

98. Even though CNAs will not be discussed in great detail, it is necessary to point out that CNAs and intentional interference are both non-kinetic capabilities and are increasingly being employed by a variety of State and non-State actors. Moreover, CNAs and interference seek to exploit vulnerabilities, and in doing so have similar effects despite the fact they employ very different technologies. Additionally, CNAs and interference have similarly revealed themselves as growing global threats. Thus, while the current analysis mainly focuses on intentional interference with satellite signals, and not CNAs, the analysis will at times draw from legal literature and discussions on CNAs, rely on them and analogize the relevant principles to make conclusions applicable to the growing problem of intentional interference. This is because CNAs are more widely discussed than is interference or jamming, and some of the legal discussions on CNAs have direct application to satellite signal interference.

communication signals.[99] This is surprising since intentional interference with electromagnetic signals was long ago identified as a serious threat to States.[100] In any event, enemy communications have long been considered valid and traditional military targets.[101]

Intentional interference with satellite signals is more than a mere hypothetical possibility.[102] It occurs regularly and costs commercial operators and end-users millions of dollars each year. These costs include lost revenue opportunities, a loss of customers, specialized personnel costs, and the price of interference protection and detection systems.[103] Long-term costs may include erosion of the company's reputation as a reliable service provider. A satellite operator or owner could also lose the investment in the satellite itself, as well as future profits. Finally, without sufficient, dependable access to satellite communications, military forces could be rendered blind and deaf. As can be seen, satellite signal interference is a matter of concern for operators and users, military and civilian alike.

In one of the earliest and most notorious jamming incidents in 1986, "Captain Midnight" used commercially available equipment to overpower the Home Box Office (HBO) channel and broadcast a message protesting HBO's rise in fees.[104] The thirty-minute text message was transmitted to all HBO customers in the eastern half of the United States.[105] Even though Captain Midnight's actions only achieved a temporary disruption to HBO's connection with its customers, it nonetheless demonstrated how quickly

---

99. Wilgenbusch & Heisig, *supra* note 10, at 57.

100. MCDOUGAL, LASSWELL & VLASIC, *supra* note 18, at 284.

101. Telegraph, telephone and undersea transmission cables have always been considered valid military targets in armed conflict. *See* Hague Convention No. IV Respecting the Laws and Customs of War on Land arts. 8, 9, Oct. 18, 1907, 36 Stat. 2277, *reprinted in* 2 AMERICAN JOURNAL OF INTERNATIONAL LAW SUPPLEMENT 90 (1908). *See also* International Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 18 U.S.T. 380, *available at* http://iscpc.org/information/Convention_on_Protection_of_Cables_1884.pdf. Article 15 explicitly provides that belligerents retain "freedom of action" during armed conflict.

102. DAVID WRIGHT ET AL., THE PHYSICS OF SPACE SECURITY: A REFERENCE MANUAL 121 (2005).

103. Jakhu & Singh, *supra* note 4, at 84; Greg Berlocher, *Interference: Operators Making Advances in Flight*, SATELLITE TODAY (June 1, 2008), http://www.satellitetoday.com/via/featires/23237.html.

104. WILSON, *supra* note 28, at IV(F).

105. *The Story of Captain Midnight*, SIGNAL TO NOISE, http://web.archive.org/web/20070128101239/http://www.signaltonoise.net/library/captmidn.htm (last visited Feb. 11, 2014).

and easily jamming can be employed to disrupt satellite communications and how far reaching the effects can extend.

Intentional interference with commercial communication satellite signals is an even bigger concern today than it was in 1986. The magnitude of the problem is revealed in several ways. As discussed above, there are simply not enough dedicated military satellites capable of providing the requisite bandwidth, coverage and capabilities needed by military forces.[106] Moreover, commercial communication satellite systems are not designed or built with the technologies and capabilities necessary to protect against malicious interference or jamming.[107] Consequently, space systems providing asymmetric advantages to twenty-first century militaries are themselves tempting targets to those that could never win a war against a highly technical military by using troops, tanks and planes.[108]

Second, boundaries once separating military and commercial space assets are vanishing; civilian objects are increasingly intermingled with military objectives, and civilian and military satellite systems and supporting networks are increasingly interconnected. This interconnectivity empowers potential adversaries to threaten both military and civilian operators and end-users as intentional disruptions of signals are not necessarily confined to a single intended targeted signal. The disruption of one signal can have wide ranging effects on adjacent signals resulting in a sequence of disruptions.[109]

One such example occurred in 2007 when the Libyan government jammed two telecommunication satellites owned by Thuraya Satellite Telecommunications of Abu Dhabi in an effort to block incoming news channels and communications from the outside world. The single event not only knocked dozens of television and radio stations serving Britain and Europe off the air, it also disrupted U.S. diplomatic, military and FBI communications.[110] Likewise, targeting and intentionally disrupting military transmissions in an armed conflict may unintentionally disrupt civilian transmissions that may be fundamental for civilian or commercial services such as financial transactions, emergency notification networks and commercial air traffic control systems. Results could include economic chaos,

106. Jakhu & Singh, *supra* note 4, at 84.

107. Wilgenbusch & Heisig, *supra* note 10, at 57.

108. Al Santoli, *Beijing Describes How to Defeat U.S. in High-Tech War*, CHINA REFORM MONITOR (Oct. 10, 2000).

109. Gydesen, *supra* note 47, at 19.

110. Kleiman & McNeil, *supra* note 14.

widespread panic and even death, if, for example, the stock market crashes, essential State services become unavailable or those unable to obtain basic needs turn to violence.[111] Intentional interference with satellite signals during war thus poses a serious challenge to the rules of IHL,[112] which requires parties to a conflict to distinguish between civilians, civilian objects and military objectives at all times.

Even though there are no known instances of satellite signal interference where injury or death to the civilian population resulted, it is certainly possible. Hypothetically speaking, what if the GPS satellite signal carrying data to an unmanned armed military aerial vehicle was replaced with a false signal?[113] The pilot or drone might believe it was somewhere different than where it was and fire a missile on a civilian (and unintended) target. While this scenario may seem purely speculative, the 2011 capture of a U.S. military drone by Iran is claimed by Iranians to have resulted from a jamming attack causing the pilot to accidentally land the plane in Iran, believing he was landing the drone at a military base in Afghanistan.[114] As another example, consider what could happen if the communication signals between a satellite operator and a satellite were interfered with, rendering the satellite unable to maneuver in space. The satellite could crash into another satellite causing it and many other space objects significant damage. Financial losses would be substantial in terms of the damage to the satellites and lost revenues as well. If communication signals using the lost or damaged systems were not rapidly moved to other satellite transponders, civilian business and monetary transactions could be interrupted or prevented resulting in worldwide financial losses (or gains).

Illustrating this point is the financial losses occurring after the September 11, 2011 airline terrorist attacks on New York and the Pentagon. The International Organization of Securities Commissions concluded the financial maneuvers and stock market trading just prior to the attacks amounted to several hundred million dollars, constituting "the most important crime of insider trading ever committed."[115] Profits went to "someone, some-

111. Gydesen, *supra* note 47, at 16–20.

112. Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protections of Civilians*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 1, 7 (2013).

113. *See* WRIGHT ET AL., *supra* note 102.

114. Oliveri, *supra* note 22.

115. *9/11 Terrorists Made Millions on the Stock Market*, CHARLES STURT UNIVERSITY, (Sept. 10, 1011), http://news.csu.edu.au/director/features.cfm?itemID=4C5F5C13C6A538CCE83C67E0784596AA.

where," but were never traced.[116] If terrorists had insider information about the attacks and purchased financial derivatives before the attack, they may have made millions from the subsequent market moves.[117] This money could easily fund terrorism activities for years. Similar effects might occur if informed investors conducted similar trading maneuvers in advance of well-coordinated jamming attacks targeting commercial communication satellite systems.

Third, the frequency, complexity and sophistication of intentional interference incidents are escalating, while the cost of conducting such attacks and the skills needed to use jamming technologies are decreasing.[118] Locating sources of interference and distinguishing a bona fide jamming attack from other forms of communication degradations or disruptions caused by systemic disturbances or natural phenomena like solar flares and astronomical storms is also difficult.[119] Moreover, non-State entities, terrorist cells and enemy combatants are increasingly engaged in jamming activities or attacks.[120] These facts illuminate the current challenges faced by States, most notably the problem of attribution.

For example, consider a situation where a terrorist organization jams the radio communications of two U.S. commercial airplanes and, unable to communicate with each other, the planes collide over New York City. As witnessed by the 9/11 attacks, fatalities, financial damage and property losses would be substantial. Now assume the U.S. determined the incident was an armed attack, thereby invoking its right of self-defense and justifying a use of force response. If following international law, the United States would want to identify the perpetrator and attribute the act to a responsible party or State before determining the appropriate response. This scenario highlights the range of technical challenges and legal considerations States will face if satellite signal interference becomes more prevalent—and perhaps even destructive.

---

116. *Id.*

117. Hugh McDermott, *How Financial Markets Finance Terrorism*, LAW–CRIME–POLITICS (July 8, 2011), http://lawcrimepolitics.com/how-financial-markets-finance-terrorism.

118. *Information Assurance: Trends in Vulnerabilities, Threats, & Technologies* (Working Paper delivered at the National Defense University, Center for Technology and National Security Policy, Washington DC, Jacques S. Gansler & Hans Binnendijk eds., 2004), *available at* http://www.hsdl.org/?view&did=448237 [hereinafter Trends in Information Assurance].

119. *Id.*

120. *Id.*

Finally, whereas the ITU legal regime was once somewhat effective in helping States resolve incidents of intentional interference through diplomatic and political channels, its normative framework is now proving to be insufficient and ill equipped to do so. Regulations requiring States to prevent and stop interference originating from within their borders are being increasingly ignored, and States are reluctant to give the ITU enforcement powers. As a result, satellite owners and operators feel compelled to constantly develop new technologies to protect against intentional interference, while continually improving and advancing their own technological capabilities to employ intentional interference offensively. In other words, States are struggling with how to protect themselves from the consequences of satellite signal interference, but at the same time are expanding both their peacetime and warfare capabilities. However, as States pursue these competing interests, new threats to international stability and space security are emerging.[121]

The range of impacts described above suggests a myriad of bad actors have, can and will continue to exploit satellite transmission vulnerabilities.[122] These vulnerabilities represent not just a U.S. military problem, but also a national security problem, a space security problem, an environmental problem, a law enforcement problem and a business security problem.[123] For these reasons, it is necessary to re-examine the framework applicable to satellite communications, the emerging trends and their implications.

III. THE TECHNICAL AND LEGAL ASPECTS OF SATELLITES AND SATELLITE SIGNAL INTERFERENCE

This Section explores how satellites function, how interference with satellite signals occurs and why commercial communication satellites are increasingly vulnerable to disruptions. This discussion is necessary to understand how satellites operate, how their signals are transmitted to and from Earth or between satellites, and how satellite transmissions are temporarily disrupted through electromagnetic interference without physically destroying the satellite or components within its system.

---

121. Space security means "secure and sustainable access to, and use of, outer space and freedom from any threats or unreasonable (unjustified) barriers to such access and use." *See* Jakhu & Singh, *supra* note 4, at 76.

122. Trends in Information Assurance, *supra* note 118.

123. *Id.*

This Section also examines the legal norms applicable to satellite transmissions under the International Telecommunications Union and international space law (ISL). This Section concludes existing norms are not equipped to handle the range of impacts emerging as more and more State and non-State actors engage in satellite signal interference. Finally, implications of satellite signal interference under IHL will be addressed. This Section reveals that, because IHL cannot adequately protect commercial communication satellites, incidents of intentional interference are likely to continue, impacts may become increasingly widespread and severe, and the civilian population may suffer significant harm in future armed conflicts.

A. The Basic Components of a Satellite System

A satellite system is comprised of the satellite, the ground control station used to operate and control the satellite, communication stations and radio links allowing communication between satellites and ground stations.[124] All satellite components are susceptible to physical attacks and/or sabotage;[125] however, some components are more susceptible to non-kinetic attacks, such as intentional interference or jamming.[126] This Section briefly addresses major elements of a common satellite system and focuses on those most vulnerable to non-kinetic disruptions caused by intentional interference or jamming.

1. The Components and Elements of a Satellite

Generally speaking, satellites are comprised of a satellite bus, payload, solar panels, communication devices, and receiving and transmitting antennas.[127] The satellite bus is the central metal structure or body to which other components are attached.[128] The bus carries the payload(s) and is comprised of subsystems, including the power supply, antennas, and mechanical and

124. WRIGHT ET AL., *supra* note 102, at 109. For a graphic depicting the components of a satellite system, *see* U.S. GENERAL ACCOUNTING OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: COMMERCIAL SATELLITE SECURITY SHOULD BE MORE FULLY ADDRESSED 8, GAO Rpt. No. GAO-02-781 (Aug. 2002) [hereinafter CRITICAL INFRASTRUCTURE PROTECTION].

125. *Id.* at 12.

126. WRIGHT ET AL., *supra* note 102, at 109.

127. *Id.* at 110.

128. *Id.*

thermal control subsystems.[129] The bus is durable enough to sustain launch stresses and is designed to protect components within from threats such as solar heat and some laser attacks.[130] The solar panels, attached to the satellite bus, are the main power source.[131] Electricity generated by the solar panels is stored in rechargeable batteries.[132] Without the ability to generate and/or store power, a satellite will not function properly, send or receive signals, or communicate with its Earth-based operator.

If a satellite or its components are damaged, they cannot be repaired.[133] A fatally damaged satellite has to either be deorbited and returned to Earth or propelled further up into outer space and into a "graveyard," "disposal," or "junkyard" orbit.[134] If communication with a damaged satellite is impossible or the satellite cannot be deorbited or launched into a graveyard orbit, it will remain in the orbit and become space debris, an uncontrollable projectile capable of devastating effects.

The payload, which differs for every satellite, includes all mission-specific components necessary to accomplish an intended purpose or specific tasks.[135] For example, the payload for a communications satellite includes radio receivers, transmitters and transponders[136] for collecting, relaying or rebroadcasting television or telephone signals.[137] A payload for a reconnaissance satellite includes high-resolution telescopes and cameras to capture images of Earth during the day and night, as well as in all types of weather conditions.[138] Regardless of payload, any interference with signals received or transmitted by the satellite or payload can have similar effects. The satellite may not function properly, its mission will be impaired and disruptions could reverberate globally.

---

129. CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 125, at 3.

130. WRIGHT ET AL., *supra* note 102, at 110.

131. *Id.*

132. *Id.*

133. *Id.*

134. Graveyard orbits, normally located beyond the geostationary orbit some 22,236 miles above Earth's equator, are used for satellites that are too expensive, too difficult or too dangerous (such as containing nuclear or radioactive materials) to deorbit. LYALL & LARSEN, *supra* note 43, at 246.

135. CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 125, at 3.

136. A transponder receives a transmission, amplifies it and transmits it to Earth or to another satellite, possibly at a different frequency. WRIGHT ET AL., *supra* note 102, at 113.

137. CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 125, at 3.

138. Stephen Clark, *Reconnaissance Satellites Launched by H-2A Rocket*, SPACEFLIGHT NOW (Jan. 27, 2013), http://www.spaceflightnow.com/h2a/f22/#.UbdxspVsWR8.

The on-board computer, located within the bus, monitors the satellite, controls its actions and processes collected data.[139] In some specialized or highly protected satellites like military satellites, the on-board computer may also utilize anti-jamming computer software.[140] Most non-military commercial satellites and their on-board computers are relatively unprotected from jamming attacks.[141] This is because they are designed for cheap and easy access and are not equipped to protect against interference.[142] As a result, commercial satellites fall victim to an increasing number of jamming attacks.[143] For example, Eutelsat reported deliberate jamming increased dramatically, going from fifty-four cases in 2010 to over 340 in 2012 by the first of November.[144]

There are also numerous incidents of jamming by State and non-State actors. In 2003, Iran used a jamming device located in Cuba to block American media transmissions from the Telestar-12 satellite into Iran.[145] In 2004, the non-State entity, Falun Gong, jammed a Hong Kong based satellite and instead broadcast its own message.[146] In 2009 and 2010, Iran jammed Intelsat satellite broadcasts into Iran.[147] Then, in 2010, Brazilian hackers disrupted the U.S. Navy's satellite, FLTSAT-8.[148] Finally, in 2012, when Syria joined Iran in jamming over twenty-five radio and television international broadcasts, including the BBC, France 24, Deutsche Welle, the Voice of America, Nilesat and Arabsat, hundreds of millions of people from northwestern Europe to Afghanistan were affected.[149]

---

139. WRIGHT ET AL., *supra* note 102, at 112; CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 125, at 3.

140. WRIGHT ET AL., *supra* note 102, at 112.

141. Grego, *supra* note 34, at 8–9.

142. *Id.* at 9.

143. *Id.*

144. Anne Wainscott-Sargent, *Fighting Satellite Interference on All Fronts*, SATELLITE TODAY (Mar. 1, 2013), http://satellitetoday.com/via/features/40651.html.

145. Safa Haeri, *Cuba Blows the Whistle on Iranian Jamming*, ASIA TIMES (Aug. 22, 2003), http://www.atimes.com/atimes/Middle_East/EH22Ak03.html.

146. *Falun Gong Hijacks HK Satellite*, XINHUA NEWS AGENCY (Nov. 22, 2004), http://www.chinadaily.com.cn/english/doc/2004-11/22/content_393776.htm.

147. Luke Baker, *2-EU Ministers Warn Iran on Satellite Jamming*, REUTERS (Mar. 22, 2010), http://in.reuters.com/article/2010/03/22/eu-iran-sanctions-idUSLDE62L0VB20100322.

148. Housen-Couriel, *supra* note 2, at 440.

149. *See* Wainscott-Sargent, *supra* note 146.

The communications system is considered the heart of a satellite.[150] It is made of a transmitter, a receiver and antennae, and forms the radio link between all satellites, their Earth-based ground stations and possibly other satellites, depending on the specific mission of the satellite.[151] Radio links transmit, transfer and receive all satellite signals (radio frequencies carrying data) to and from Earth, as well as from other satellites.[152] Radio links are highly vulnerable to interference and when disrupted deny satellite communications,[153] making a satellite useless.[154]

Radio waves comprise part of the electromagnetic spectrum, the spectrum of all frequencies of electromagnetic radiation.[155] While the electromagnetic spectrum includes x-rays, gamma rays, ultraviolet light, visible light rays and radio waves, only visible light rays are detectable by humans.[156] Despite being invisible to the naked eye, radio waves used in satellite operations can be tracked and located relatively easily[157] because they travel via line-of-sight connections from the sending location to the receiving location.[158] Tracking is accomplished through antennas, which gather and track information to precisely locate the transmission signal and source of the signal in both time and space.[159]

Every satellite requires and utilizes radio links to and from Earth for communication purposes and for accurately monitoring satellite function and health. These radio links are known as telemetry, tracking and command (TT&C).[160] Telemetry refers to the data transfer process (containing specific details on the health and status of the satellite) from the satellite to the ground.[161] Tracking locates the satellite in time and space based on position, speed and range measurements.[162] Command is the method of commanding and controlling the satellite from the ground via the transmis-

150. JOSEPH N. PELTON, SATELLITE COMMUNICATIONS 19 (2012).

151. WRIGHT ET AL., *supra* note 102, at 112.

152. *Id.*

153. CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 125, at 13.

154. E.R.C. VAN BOGAERT, ASPECTS OF SPACE LAW 192 (1986).

155. Weedon, *supra* note 87.

156. *Id.*

157. While similar techniques and technologies are used to locate the sources of jamming attacks, this does not mean that it is always easy to directly pinpoint, track down or attribute the source of jamming to a certain location or entity.

158. WILSON, *supra* note 28, at III(C).

159. *Id.* at III(D).

160. WRIGHT ET AL., *supra* note 102, at 112.

161. CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 125, at 4.

162. *Id.*

sion of signals while the satellite is in line of sight of a ground station.[163] TT&C is essential and basically the same for all satellites, regardless of mission.[164]

Any interference with TT&C signals could cause significant damage. Without TT&C, operators could lose control of a satellite, resulting in an uncontrolled satellite colliding with other satellites. TT&C transmissions, however, are generally protected by way of encryption and encoding.[165] Therefore, TT&C transmissions are not the element of satellite communications that are most vulnerable to interference or disruptions,[166] and further discussions on TT&C will be intentionally limited. Regardless, technical aspects of satellite signal interference discussed herein would, generally speaking, apply in the same way to TT&C transmissions as they would to almost all satellite transmissions. However, because satellite signal interference is usually employed as a means to disrupt communications temporarily, rather than to cause physical damage, it is unlikely TT&C signals will be targeted unless physical destruction of a satellite is intended.

In addition to the elements described above, satellites also have attitude and control systems, and propulsion subsystems. Gyroscopes, accelerometers and guidance systems control the satellite and keep it positioned in the right direction for communications and data collection.[167] The propulsion system, comprised of engines and thrusters, maintains station keeping, control and maneuvering.[168] Any malfunction of or interference with these systems could endanger other satellites.[169] Therefore, satellite operators must monitor, control and communicate with satellites at all times through radio signals sent to satellites via Earth-based ground stations.

2. Ground Stations and Links

Satellite operators control, track, monitor and communicate with satellites via high-powered, high frequency radio signals emitted from ground-based stations using antennas.[170] Ground stations and antennas can be large,

163. *Id.*
164. *Id.*
165. WRIGHT ET AL., *supra* note 102, at 112.
166. *Id.* at 113.
167. *Id.* at 112.
168. *Id.* at 113.
169. *Id.* at 112–13.
170. *Id.* at 114.

small, stationary or mobile.[171] A satellite can communicate with a single ground station, such as a control station for TT&C purposes, or with hundreds of ground stations or antennas at the same time as it is transmitting or receiving data such as video or voice communications.[172] In addition to sending and receiving satellite signals, ground stations have inherent jamming capabilities.[173] The area receiving a radio signal of useful strength from the satellite is known as the satellite's coverage area or footprint.[174]

Pathways used to communicate with satellites are called links.[175] A radio signal transmitted from the ground station up to a satellite is the uplink;[176] the radio signal traveling down from the satellite to the ground station is the downlink;[177] crosslinks transmit signals between satellites.[178] Uplink and downlink radio signals are most vulnerable to interference or jamming because their signal strength is so low. By the time they reach the receiving antenna, the original signal can be easily overpowered by a stronger radio signal.[179] Crosslinks would be most vulnerable to space-based jammers.

B. The Technical Application of Intentional Interference

Jamming equipment is easy to make and/or buy.[180] Jamming is not complex or technically demanding.[181] It is also increasingly available to, and employed by, States, as well as non-State entities.[182] Thus, for a State or non-State entity engaged in a conflict with a country dependent on space-based technologies, disrupting satellite transmissions could be the principal determinant of victory. A July 2000 Chinese report noted, "[f]or countries

171. *Id.*

172. *Id.*

173. WILSON, *supra* note 28, at IV.

174. William Craig Cook, *How Do Satellites Work?*, http://www.williamcraigcook.com/satellite/work.html (last visited Feb. 11, 2014).

175. WRIGHT ET AL., *supra* note 102, at 114.

176. *Id.*

177. *Id.*

178. *Id.*

179. *Id.* at 115, 118.

180. For example, a jammer can be built using a satellite TV receiver or made from scratch using plans downloaded from the Internet. Commercial jammers are also openly marketed and sold. *See* John Brandon, *GPS Jammers Illegal, Dangerous, & Very Easy to Buy* (Fox News television broadcast Mar. 17, 2010), http://www.foxnews.com/tech/2010/03/17/gps-jammers-easily-accessible-potentially-dangerous-risk/.

181. Grego, *supra* note 34, at 15.

182. WRIGHT ET AL., *supra* note 102, at 118.

that could never win a war by using the method of tanks and planes, attacking the U.S. space system may be an irresistible and most tempting choice."[183] This has been recognized by the United States as a probable act.[184] In fact, the Gulf War might have turned out differently had Iraqi military forces been able to successfully disrupt satellite signals relied on so heavily by U.S. forces.[185]

1. Jamming and Spoofing

Jamming, the term most often associated with intentional disruption of satellite communications, refers to temporary interference of radio signals or communications between a satellite and its receiver or users on the ground.[186] The object is to render radio transmissions unintelligible by causing interference.[187] It is accomplished by overpowering signals emitting noise sent to and received by the satellite or using a second signal at the same frequency or higher power, preventing the receiver from collecting the real signal.[188] The jamming signal is often meaningless noise that drowns out the real signal[189] in the form of "harmful interference."[190]

There are two forms of satellite jamming: orbital jamming and terrestrial jamming.[191] Orbital jamming involves beaming a conflicting signal toward a satellite. The original signal is drowned out by the jamming signal so

183. Santoli, *supra* note 108.

184. In 2001, in reaction to the U.S. military's increasing dependence on satellite technology, the Commission to Assess U.S. National Security released a report stating that the United States needed to secure itself against a "Space Pearl Harbor." *See* COMMISSION TO ASSESS U.S. NATIONAL SECURITY SPACE MANAGEMENT & ORGANIZATION, REPORT OF THE COMMISSION TO ASSESS UNITED STATES NATIONAL SECURITY SPACE MANAGEMENT AND ORGANIZATION viii (2001), *available at* http://space.au.af.mil/space_commission/executive_summary.pdf; *see also* Jean-Michel Stoullig, *Rumsfeld Commission Warns Against 'Space Pearl Harbor,'* SPACE DAILY (Jan. 11, 2011), http://www.spacedaily.com/news/bmdo-01b.html.

185. Kanuck, *supra* note 55, at 284.

186. Grego, *supra* note 34, at 9, 15.

187. Michel Bourbonniére, *Law of Armed Conflict (LOAC) and the Neutralisation of Satellites or* Ius In Bello Satellitis, 9 JOURNAL OF CONFLICT & SECURITY LAW 43, 58 (2004) [hereinafter, Bourbonniére, *Law of Armed Conflict*].

188. WRIGHT ET AL., *supra* note 102, at 118.

189. WILSON, *supra* note 28.

190. International Telecommunication Union Radio Regulations art. 1.169 (2012) [hereinafter ITU Radio Regulations].

191. Satellite Jamming in Iran*, supra* note 25, at 22.

the original signal does not reach the satellite and cannot be rebroadcast to users. When this occurs, the original signal is overridden and disrupted for users everywhere,[192] which can impact a large number of users because satellites operate in groups of channels.[193] When one signal is disrupted, all signals in the same group can be affected, thereby cutting off services to all users in the satellite's footprint, which can cover multiple continents.[194] Captain Midnight used uplink orbital jamming to disrupt all HBO service, the impact of which was felt all over the eastern United States.

Terrestrial jamming occurs at a specific place on the Earth near the targeted receiving station and involves using equipment that is easy to purchase, use and conceal.[195] Rather than targeting the satellite, terrestrial jamming targets specific terrestrial users.[196] Thus, whereas orbital jamming effects can extend throughout a satellite's entire footprint, terrestrial jamming effects can be localized and limited to specific targets.[197]

Known as a type of electronic decoy, [198] spoofing is similar to jamming. Instead of drowning out the real signal, a usable but false signal is emitted that mimics the characteristics of a true signal so the user receives a fake (or spoofed) signal.[199] The goal of spoofing is to fool or mislead the end user by providing fake signals. The downing of the U.S. military drone in 2011 by Iran, discussed previously, is believed to have been caused by a spoofing attack.[200]

In the case of either jamming or spoofing, the jammer must operate in the same radio frequency bands as the system being jammed.[201] The jammer must locate via radar or signal tracking systems[202] the signals to be jammed, and produce a similar signal with sufficient intensity to overwhelm the targeted signal(s).[203] A jammer does not have to be located near the receiver to produce a signal nor need to know the location of the receiver to

192. *Id.*
193. *Id.*
194. *Id.*
195. *Id.* at 24.
196. *Id.*
197. *Id.*
198. WILSON, *supra* note 28.
199. WRIGHT ET AL., *supra* note 102, at 118.
200. Oliveri, *supra* note 22.
201. WILSON, *supra* note 28.
202. *Id.*
203. Grego, *supra* note 34, at 15.

be jammed.[204] The jammer must only be located within the satellite's footprint or broadcasting area and have the ability to direct its signal to the receiver.[205] Thus, as long as the jamming activity is within the footprint of the satellite, which can span multiple countries, the jammer will not necessarily physically violate the territorial integrity of another State to effectuate a disruption. While most interference takes place on Earth with ground-based jammers, jammers can be placed in orbit on a satellite.[206] Space-based jammers however, are impractical because, in order to be effective, a large number of orbiting jammers would be needed.[207]

2. The Ease of Intentional Interference

Technically speaking, interfering with a satellite is easy, inexpensive and can be accomplished by using commercially available equipment. Anyone with commercial satellite communications equipment can jam satellite communications.[208] For just a few thousand U.S. dollars, commercial companies are selling compact, well-disguised, weatherproofed jamming antennas that can disrupt satellite signals over a radius of five to twenty kilometers, depending on terrain.[209] Even hand-held jammers are now available and can deny radio signals up to eighty kilometers away.[210] Thus, not only have advancements in technologies made jamming easier and less expensive to employ, the mobile nature of equipment has made it more difficult for satellite operators to track and locate the origin of jamming activities. In fact, while some countries like the United States recently passed new laws prohibiting the marketing, sale and use of jamming devices,[211] jamming devices remain widely available in other countries and on-line.[212] An Internet search on the phrase "how to jam a signal" or "satellite signal jamming" results in pages of videos, tutorials, demonstrations and blogs detailing the ease in which one can obtain jamming equipment and disrupt almost any signal.

---

204. WRIGHT ET AL., *supra* note 102, at 119.

205. *Id.* at 118.

206. *Id.* at 119.

207. *Id.*

208. WILSON, *supra* note 28, at IV.

209. Satellite Jamming in Iran*, supra* note 25, at 26–27.

210. WILSON, *supra* note 28, at IV(F).

211. News Release, Federal Communications Commission, FCC Enforcement Bureau Takes Action Against Craigslist Sellers for Marketing Illegal Signal Jamming Devices (Oct. 15, 2012), http://transition.fcc.gov/eb/News_Releases/DOC-316796A1.html.

212. WILSON, *supra* note 28, at IV.

3. The Vulnerability of Commercial Communication Satellites and Signals

All military and commercial satellite communications systems are susceptible to intentional interference, uplink and downlink jamming and spoofing. Whereas military satellites encrypt and encode satellite signals before transmitting them, most commercial communication satellites do not. Consequently, commercial communication satellite signals are more susceptible to interference and jamming than military satellites and signals.[213]

Commercial communication satellites are susceptible to jamming for a number of reasons. First, the cost and weight of countermeasures is considered an unnecessary expense.[214] Second, commercial communication satellites are designed for ease of use and to send and receive signals over large areas.[215] Third, most commercial communication satellites are easy to locate because they remain "stationary" over a particular location above Earth's surface at all times.

Most commercial communication satellites are located in GEO.[216] The GEO orbit lies 35,786 kilometers/22,236 miles directly in the plane above the equator and remains fixed relative to Earth's surface so satellites located in the GEO orbit rotate at the same speed as Earth.[217] Thus, because satellites in GEO are essentially located in the same position relative to a point on Earth at the same time every day, they are relatively easy to track and locate,[218] and there is a large area from which it is possible to jam or spoof a signal.[219]

---

213. WRIGHT ET AL., *supra* note 102, at 121.

214. WILSON, *supra* note 28, at IV.

215. WRIGHT ET AL., *supra* note 102, at 121.

216. LYALL & LARSEN, *supra* note 43, at 246, 256.

217. *Id.* at 246.

218. WILSON, *supra* note 28. Additionally, while all satellites launched into space are supposed to be registered (including launch date, name, orbital parameters and purpose) with the United Nations and/or the ITU, some are not. That said, there are publically accessible databases that provide significant information about active satellites in orbit, such as those maintained by Space Track.org or the Union of Concerned Scientists. This information can be used to help locate and track satellites and satellite signals. While these publically available databases cannot necessarily pinpoint the exact location of a given satellite, they do include the orbital parameters of the satellite. *See* Union of Concerned Scientists, *The Nature of the UCS Database Information*, UNION OF CONCERNED SCIENTISTS, http://www.ucsusa.org/assets/documents/nwgs/common-misconceptions.pdf (last visited Feb. 11, 2014).

219. WRIGHT ET AL., *supra* note 102, at 121.

Some Russian commercial communication satellites operate in the Molniya Orbit, a highly elliptical orbit,[220] because much of Russia is too far north to fall within the footprint of a satellite located in GEO.[221] Other commercial communication satellites, such as the Globalstar satellite phone system, use a constellation of forty-eight satellites positioned in LEO.[222] Because LEO satellites are much closer to the Earth's surface than those in GEO (satellites in LEO are located between 65–310 miles/100–500 kilometers above the surface),[223] LEO satellites and their communications are very susceptible to jamming attacks and attacks from Earth-based kinetic weapons.[224]

C. Legal Frameworks Governing Satellites and Intentional Interference

1. International Telecommunications Law

The UN technical agency in charge of international coordination for information and telecommunications technologies is the International Telecommunications Union. The ITU defines telecommunications as, "[a]ny transmission, emission or reception of signs, signals, writings, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems."[225] Initially founded in 1865 as the International Telegraph Union, the ITU became a UN specialized agency in 1947.[226] Currently, 193 countries and over seven hundred private-sector entities and academic institutions are members.[227]

The ITU has numerous functions relating to satellites and telecommunications. Specifically, the ITU coordinates and allocates the global radio spectrum used by satellites for different services and parties, assigns orbital slots to satellites stationed in the GEO orbit and prohibits intentional interference with satellite signals on the basis of reciprocity.[228] The ITU also

220. LYALL & LARSEN, *supra* note 43, at 246.

221. Bourbonniére, *Law of Armed Conflict*, *supra* note 187, at 52.

222. *Id.*

223. LYALL & LARSEN, *supra* note 43, at 245–46.

224. Bourbonniére, *Law of Armed Conflict*, *supra* note 187, at 52.

225. ITU Constitution, *supra* note 23, annex 1012.

226. LYALL & LARSEN, *supra* note 43, at 200–05.

227. *About ITU: Membership*, ITU, http://www.itu.int/en/about/Pages/default.aspx (last visited Feb. 11, 2014). Despite being members of the ITU, these 700+ non-State entities do not have standing under international law to deal directly with the ITU.

228. ITU Radio Regulations, *supra* note 190, art. 8.5.

develops worldwide technical standards for the use, assignment and allocation of radio frequencies.[229] The allocations and technical standards are codified in the ITU Constitution, the ITU Convention and the ITU Radio Regulations. In short, the ITU is the single leading international entity that, through mutual cooperation, ensures global communications run smoothly by organizing, managing and coordinating radio signals used by different services and providers.

When the ITU assigns or allocates a specific radio signal, that signal assignment is recorded in a registry of radio frequency assignments under the Master International Frequency Register (MIFR).[230] Registering a signal on the MIFR gives the assigned user a right to "international recognition"[231] and protection against interference. If another user uses the same signal and thus interferes with the recognized holder of the allocated signal, the interfering user must, upon notification, immediately cease using that frequency if that use creates harmful interference with the signal that has international recognition.[232]

"Harmful interference" is defined by the ITU as interference with a radio signal that endangers the functioning of a radio service "or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with ITU Radio Regulations."[233] All ITU member States are obligated not to cause harmful interference, and enforce and respect the ITU regulatory regime.[234] To this effect, Article 6.1 of the ITU Constitution provides: "The Member States are bound to abide by the provisions of this Constitution, the Convention and the Administrative Regulations in all telecommunications office and stations established or operated by them which engage in international services or which are capable of causing harmful interference to radio services of other countries . . . ."[235]

Article 45 of the ITU Constitution also prohibits harmful interference. It states:

> All Stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States or of recognized operating agencies, or of other duly authorized operating agencies which carry on a

229. *About ITU: Membership*, *supra* note 227.
230. ITU Radio Regulations*, supra* note 190, art. 8.1.
231. *Id.*, art. 8.3.
232. *Id.*, art. 8.5.
233. *Id.*, art. 1.169.
234. Jakhu, *Satellites*, *supra* note 4, at 6.
235. ITU Constitution*, supra* note 23, art. 6(1).

> radio service, and which operate in accordance with the provisions of the Radio Regulations.

Similarly, ITU member States must not use an unnecessary transmission of power causing harmful interference. Specifically, Article 15 of the ITU Radio Regulations provides:

> All Stations are forbidden to carry out unnecessary transmissions, or the transmission of superfluous signals, or the transmission of false or misleading signals, or the transmission of signals without identification . . . .[236] Transmitting stations shall radiate only as much power as is necessary to ensure a satisfactory service.[237]

Accordingly, any interference with, or intentional jamming of, a signal is contrary to the ITU regulatory regime. Such an act not only violates the principle of international recognition under the ITU Radio Regulations, it also interferes with another user's right under Article 6 and Article 45 of the ITU Constitution, and represents an unnecessary transmission of power in violation of Article 15 of the ITU Constitution.

If satellite signal interference or jamming occurs, member States are obligated to comply with ITU provisions and cooperate with others to eliminate harmful interference[238] through bilateral negotiations.[239] If negotiations fail, the affected State may attempt arbitration as specified under Article 41 of the ITU Convention or seek dispute resolution pursuant to Article 56. However, neither Article 41 nor Article 56 has ever been used.[240]

Historically, compliance with ITU provisions, utmost goodwill and mutual cooperation resolved most interference issues.[241] States observed the ITU's rules and regulations voluntarily and out of self-interest. Voluntary compliance however, is increasingly proving to be insufficient. Jamming continues despite calls for its elimination by ITU member States and international organizations, and responsible member States often fail to acknowledge the interference. Not only is the problem of interference largely political,[242] but also there are no compulsory international dispute

---

236. ITU Radio Regulations*, supra* note 190, art. 15.1 §1.
237. *Id.,* art. 15.1 §2.
238. *Id.,* arts. 11.42, 11.42A, 15.21 §13; *see also* Jakhu, *Satellites*, *supra* note 4.
239. Jakhu & Singh, *supra* note 4, at 88.
240. Jakhu, *Regulatory Processes*, *supra* note 29, at 290.
241. ITU Radio Regulations, *supra* note 190, art. 15.22 §14.
242. SAVAGE, *supra* note 5, at 132–34.

resolution systems within the ITU legal regime to resolve interference problems.[243] Additionally, not all nations have ratified all of the ITU rules and regulations, and the ITU does not have any mechanism of enforcement power, nor does it have the authority to impose sanctions against those States violating the ITU regulatory regime.[244] Thus, despite the ITU's efforts to resolve the growing problem of interference, persuasion, negotiations and voluntary compliance have long been the only tools available to prevent intentional interference.[245]

Over the course of the past few years, however, the ITU has taken a stronger stance against satellite interference and jamming. For example, in 2010, the ITU issued its first public exhortation to a State (Iran) to stop jamming originating within its borders.[246] At the 2012 World Radiocommunication Conference (WRC),[247] the ITU took another public step in condemning intentional interference by amending portions of the ITU Constitution and Radio Regulations.[248] The changes, albeit insignificant, declare violations of Article 45 of the ITU Constitution and Article 15.1 of the Radio Regulations as acts requiring necessary actions by national administrations. Of the 193 member States, 165 approved the change to Article 45, which states: "If an administration has information of an infringement of the Constitution, the Convention or the Radio Regulations (in particular Article 45 of the Constitution and No. 15.1 of the Radio Regulations) committed by a station, under its jurisdiction, the administration shall ascertain the facts and take the necessary actions."[249]

---

243. Jakhu & Singh, *supra* note 4, at 88.

244. *Id.*

245. Peter B. de Selding, *ITU Implores Iran to Help Stop Jamming*, SPACE NEWS (Mar. 26, 2010), http://www.spacenews.com/article/itu-implores-iran-help-stop-jamming#.UdWkfhZsWR8.

246. Theresa Hitchens, *Multilateralism in Space: Opportunities and Challenges for Achieving Space Security*, 4 SPACE AND DEFENSE 3, 14 (2010).

247. The WRC is held every three to four years. The WRC has the authority to review, and when necessary, amend the ITU Radio Regulations, which constitute a treaty governing the use of the radio-frequency spectrum and satellite orbits. *See World Radiocommunication Conferences (WRC)*, ITU, http://www.itu.int/ITU-R/index.asp?category=conferences&rlink=wrc&lang=en (last visited Feb. 11, 2014).

248. Yvon Henri, Presentation delivered to The Brussels Space Policy Roundtable, Brussels, Belgium: The ITU Radio Regulations and Space Sustainability (Nov. 29, 2012), SECURE WORLD FOUNDATION, http://swfound.org/media/96609/2012_SSI_Yvon%20Henri.pdf.

249. ITU Radio Regulations, as modified by WRC-12, art. 15.21 §13.

Unfortunately, the change did not increase the ITU's authority nor did it contemplate any future action when member States fail to take "necessary actions." Article 45 merely rephrases the original regulation with some clarification as to the types of infringement contemplated. Consequently, many problems remain with respect to preventing interference.

Notwithstanding the general obligation of non-interference, Articles 34 and 35 of the ITU Constitution permit member States to suspend or prevent incoming and outgoing satellite communications within their own territory. Article 34 provides:

> Member States reserve the right to stop, in accordance with their national law, the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage . . . .[250] Member States also reserve the right to cut off, in accordance with their national law, any other private telecommunication which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency.[251]

Similarly, Article 35 states: "Each Member State reserves the right to suspend the international telecommunication service, either generally or only for certain relations and/or for certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other Member States . . . ."[252] This authority derives from every State's capacity as a sovereign to control information within its own territory, but does not permit States to interfere with communications beyond its borders.[253] In fact, under Article 38 of the ITU Constitution, member States are obligated to ensure the best technical conditions for rapid, uninterrupted international telecommunications and refrain from disrupting operations in other States.[254] Regardless, a properly executed disruption of satellite transmissions fitting within the Article 34 and 35 exemptions would not violate the ITU regulatory regime. However, because neither Article 34 nor Article 35 specifies the source or destination of stopped or "cut off" communications, there is some ambiguity as to the scope of the exemption. For example, it is un-

250. ITU Constitution*, supra* note 23, art. 34(1).
251. *Id.*, art. 34(2).
252. *Id.*, art. 35.
253. Housen-Couriel, *supra* note 2, at 445.
254. ITU Constitution*, supra* note 23, art. 38.

clear whether communications completely within a foreign country or between locations in two foreign countries would be included under these exemptions where a State could establish a basis for jurisdiction other than territoriality, such as communications to or from an embassy.[255]

Moreover, Article 48 of the ITU Constitution carves out an exception for the military. It provides, in part: "Member States retain their entire freedom with regard to military radio installations. Nevertheless, these installations must, so far as possible, observe statutory provision relative . . . to the measures to be taken to prevent harmful interference . . . ."[256] Article 48 exempts national defense services from ITU rules and regulations, but in doing so makes resolution of harmful interference incidents involving the military difficult. In fact, the words "so far as possible" appear only to require military installations to exercise "due regard." Article 48 also leaves open the question of whether military use of commercial satellites falls outside the ITU regulatory framework.[257] Regardless of how Article 48 impacts the use of commercial satellites, the terms "entire freedom" and "so far as possible" clearly suggest military exigency or necessity (such as measures taken in armed conflict) may supersede the obligation to prevent harmful interference.[258] In armed conflict, the ITU regime would not govern all acts of harmful interference. Measures involving interference would be governed by the *jus ad bellum* and *jus in bello* as discussed below.

The impact of the ITU regime on satellite signal interference during armed conflict, aside from Article 48 discussions above, will not be discussed in greater detail since historical practice suggests treaties inconsistent with a state of armed conflict are usually suspended[259] between belligerents during armed conflicts.[260] Regardless, ITU treaty obligations be-

255. Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL LAW REVIEW 57, 63–64 (1998).

256. ITU Constitution, *supra* note 23, art. 48.

257. Scott, *supra* note 255, at 63–64.

258. Jarman, *supra* note 60, at 41.

259. While treaty obligations between belligerents during armed conflict were historically suspended, the applicability and compatibility of some treaties to a state of armed conflict between belligerents is assessed on a case-by-case basis in order to determine whether the object and purpose of particular provisions are consistent with a state of hostilities. 1 DANIEL P. O'CONNELL, INTERNATIONAL LAW 268 (2d ed. 1970).

260. LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE 302 (H. Lauterpacht ed., 7th ed. 1952).

tween belligerents and non-belligerents (neutrals) would continue in armed conflict under the law of neutrality.[261]

As the above discussion demonstrates, there are exceptions and ambiguities regarding the application and scope of the ITU framework to harmful interference. The ITU framework has also had little ability to prevent intentional disruption of satellite communications and a failure to comply with ITU provisions may only constitute a breach of contractual obligations [262] giving rise to State responsibility.[263] While an exhaustive discussion on State responsibility is outside the scope of this article, it is important to emphasize that a breach of international obligation attributable to a State is an internationally wrongful act,[264] thereby triggering a secondary obligation to cease the unlawful conduct and re-establish the *status quo ante* by way of restitution,[265] compensation[266] or satisfaction.[267] Moreover, if the ensuing dispute cannot be resolved, an injured State can always bring the matter before the UN Security Council or the UN General Assembly for investigation.[268] As noted above, however, States have yet to pursue such courses of action. This lack of action could be because States want to avoid drawing attention to vulnerable systems or because States don't want to call out others for activities they too engage in against others.

2. International Space Law

In addition to the ITU framework, international space law also governs activities of satellites and satellite communications. Initiated in the 1950s, ISL was formally codified in the 1960s and 1970s as a result of the launch

261. For a thorough discussion on how the law of neutrality applies to satellites and outer space, see Jarman, *supra* note 60.

262. STEPHEN GOROVE, DEVELOPMENTS IN SPACE LAW: ISSUES AND POLICIES 49 (1991).

263. Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 2, Rep. of the Int'l L. Comm'n, 53d Sess., U.N. Doc. A/56/10, GAOR 56th Sess., Supp. No. 10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter State Responsibility].

264. *Id.*, art. 2.

265. *Id.*, art. 35.

266. *Id.*, art. 36.

267. *Id.*, art. 37.

268. U.N. Charter art. 35.

of Sputnik I,[269] the world's first artificial satellite.[270] Today, the fundamental norms applicable to outer space are found in five treaties[271] and several non-binding principles and declarations.[272] Together, these documents establish the primary principles, rules and legal system for all activities conducted in outer space.

---

269. *Sputnik* means, "fellow traveler." John N. Wilford, *With Fear and Wonder in Its Wake, Sputnik Lifted Us Into the Future*, NEW YORK TIMES (Sept. 25, 2007), http://www.nytimes.com/learning/teachers/featured_articles/20070925tuesday.html. Even though the Soviet Union notified the international community of its plan to launch a satellite prior to actually doing so, Sputnik I grabbed the attention of the world and caught Americans completely off-guard. It also shocked the U.S. government due to its military implications. With no function but to chirp at a predetermined frequency, Sputnik I revealed the Soviet Union not only had the ability to launch a rocket into outer space, but, more importantly, it demonstrated that the Soviets could advance that technology to produce a rocket with enough thrust to launch an inter-continental ballistic missile armed with a nuclear warhead at a target within the United States. In fact, Sputnik was even seen by some as a "Sword of Damocles" dangling overhead. *See Sputnik and The Dawn of the Space Age*, NASA, www.history.nasa.gov/sputnik (last visited Feb.11, 2014); *A Brief History of the National Aeronautics and Space Administration*, NASA, http://www.hq.nasa.gov /office/pao/History/40thann/factsheet.htm (last visited Feb. 11, 2014); Neil de Grasse Tyson, *The Case for Space: Why We Should Keep Reaching for the Stars*, FOREIGN AFFAIRS, Mar./Apr. 2012, at 22; JOHN W. MASON, THE COLD WAR, 1945–1991, at 29 (2009); MCDOUGAL, LASSWELL & VLASIC, *supra* note 18, at 283.

270. *Sputnik* was an aluminum sphere the size of a beach ball (twenty-two inches). It weighed 183.9 pounds and orbited Earth in approximately ninety-eight minutes. *Sputnik* had four spring-loaded whip antennae and carried a small radio beacon that chirped at regular intervals on a predetermined radio frequency. Its exact location over Earth's surface could be verified by means of telemetry. *Sputnik and The Dawn of the Space Age*, *supra* note 269.

271. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 19 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty]; The Agreement on the Rescue of Astronauts and the Return of Objects Launched in Outer Space, Apr. 22, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 119; Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 [hereinafter Liability Convention]; Convention on Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15 [hereinafter Registration Convention]; Agreement governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 18, 1979, 1363 U.N.T.S. 3.

272. Question of the Peaceful Use of Outer Space*,* G.A. Res. 1348 (XIII), U.N. Doc. A/RES/1348 (III) (Dec. 13, 1958); Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, G.A. Res 1962 (XVII), U.N. Doc. A/RES/1962 (XVII) (Dec. 13, 1963).

All major spacefaring nations are State parties to most of the ISL treaties, including the Outer Space Treaty, the Liability Convention, the Registration Convention, and the Return and Rescue Agreement. Participation in the Moon Agreement, however, remains low, with only fifteen State parties to date.[273] Because not all five treaties or provisions therein are relevant to satellite signal interference, this article will only address those treaties and provisions most relevant to satellites, satellite communications and satellite signal interference.

The Outer Space Treaty is one of the primary legal instruments governing space activities and represents the international community's first step in proscribing norms to an area without law.[274] Often referred to as the "Constitution," the "Bible" or "Magna Carta" of space law,[275] the Outer Space Treaty has been in force since October 10, 1967 and has been ratified by 102 States and signed by another twenty-six States.[276] It provides the basic framework for international space law, contains numerous principles that have passed into customary law[277] and applies to all activities conducted in outer space, regardless of actor. It also reaffirmed the duty of States to comply with international law[278] while conducting outer space activities.[279]

Article III of the Outer Space Treaty dictates that all State parties must undertake outer space activities "in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promotion international cooperation and understanding."[280] State parties engaged in any outer space activity are

273. *Status of International Agreements Relating to Activities in Outer Space*," UNITED NATIONS OFFICE FOR OUTER SPACE AFFAIRS, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/treatystatus/index.html (last visited Feb. 11, 2014).

274. Michael C. Mineiro, *FY-1C and USA-193 ASAT Intercepts: An Assessment of Legal Obligations under Article IX of the Outer Space Treaty*, 34 JOURNAL OF SPACE LAW 321, 325 (2008).

275. LYALL & LARSEN, *supra* note 43, at 53.

276. *Status of International Agreements Relating to Activities in Outer Space*, *supra* note 273.

277. LYALL & LARSEN, *supra* note 43, at 41.

278. Under Article 38 of the Statute of the ICJ, international law includes treaties and international conventions, international custom and general principles of law as recognized by civilized nations, as well as judicial decisions and the teachings of the most highly qualified publicists as subsidiary means for the determination of rules and law. Statute of the International Court of Justice, June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993 [hereinafter Statute of the ICJ].

279. Outer Space Treaty, *supra* note 271, art. III.

280. *Id.*

therefore obliged to respect not only the rights and obligations established by the Outer Space Treaty, but also the rights and obligations contained in the ITU and the UN Charter, as well as general principles of international law.

Article I of the Outer Space Treaty codifies one of the most significant and well recognized principles of international space law: the freedom of exploration and use of outer space by all States.[281] As it relates to this article, Article I allows States to utilize satellites and engage in satellite communications without prior authorization from other States.[282] Article I also establishes the "common interest" principle, which provides space shall be used for the benefit and in the interests of all mankind.[283] In full, Article I requires States to balance their outer space activities and national interests with the wider benefit and interest of the international community.

Although Article I requires States to contemplate the ramifications of their outer space activities and the impact of those actions on all countries, it does not explicitly prohibit anyone or any State from engaging in a specific space activity, including interfering with satellite signals. Thus, Article I does not answer the question of when jamming is permissible. One thing is clear, however, under the Outer Space Treaty, States bear international responsibility for actions committed contrary to international obligations.[284]

Article II of the Outer Space Treaty creates a borderless regime in outer space[285] by prohibiting States and private entities from making any claim of sovereignty over the moon, *any* celestial body and *any* expanse of outer space, including orbital slots occupied by satellites.[286] Article II provides, "[o]uter 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."[287] Thus, despite the freedom of exploration and use of outer space as codified within Article I of the Outer Space

281. *Id.*, art. I(2).

282. Schmitt, *Military Operations in Space*, *supra* note 51, at 101.

283. Outer Space Treaty, *supra* note 271, art. I(1).

284. Phosphates in Morocco (Italy v. Fr.), Preliminary Objections, 1938 P.C.I.J. (ser. A/B) No. 74, at 10, 28; *see also* S.S. Wimbleton (U.K. v. Ger.), 1923 P.C.I.J. (ser. A) No. 1, at 15, 30; Factory at Chorzow (Ger. v. Pol.), Jurisdiction, 1927 P.C.I.J. (ser. A) No. 9, at 21.

285. Michel Bourbonniére, *The Clausewitz Nebulae: The Legitimacy of Military Activities in Outer Space During Armed Conflicts*, 40 ISRAEL YEARBOOK ON HUMAN RIGHTS 243, 250 (2010) [hereinafter Bourbonniére, *Clausewitz Nebulae*].

286. *Id.* at 251–52.

287. Outer Space Treaty, *supra* note 271, art. II.

Treaty, Article II establishes that any exercise of that freedom, wherever located and in whatever form, may never create the basis of sovereignty and ownership.[288]

Bearing in mind the ITU provisions discussed above regarding the assignment of orbital positions and the allocation of radio frequencies, satellite activities may appear to contradict Article II of the Outer Space Treaty. For example, satellites occupy (and assert exclusive use and occupation of) specific orbits as assigned by the ITU. Additionally, satellite transmissions are provided protection against interference when registered with the ITU. These actions, however, do not give rise to claims of sovereignty or ownership. Satellite owners and operators are merely exercising specific rights extended to them under the ITU regime as agreed to and as respected by State parties of the ITU.[289] Satellite orbital slots are also sold,[290] traded and leased.[291] While such activities may again appear to contravene the non-appropriation principle as set forth in Article II of the Outer Space Treaty, in actuality they do not because the object at issue is the not the physical location in space where the satellite is positioned nor the specific radio frequency, but rather the right of use as determined under the ITU framework. Finally, even with Article II's prohibition of claims of sovereignty in outer space, States retain sovereignty and control over satellites and other objects they launch into space, including those launched by their nationals.[292]

Article II does not explicitly address the activities of private or non-State entities. However, the extension of the "non-appropriation principle" to non-State entities is "firmly established in space law,"[293] and is set forth in Article VI of the Outer Space Treaty, which provides:

---

288. For a good discussion on whether Article II also prohibits the creation of private property rights on celestial bodies, see Ricky J. Lee, A*rticle II of the Outer Space Treaty: Prohibition of State Sovereignty, Private Property Rights, or Both?*, 11 AUSTRALIAN INTERNATIONAL LAW JOURNAL 128 (2004).

289. Radio spectrum frequency and orbital positions are recognized as limited natural international resources that are to be used economically and efficiently so all States have equitable access to them. *See* ITU Constitution, *supra* note 23, art. 44(2).

290. *NBN Co Closes in on Satellite Slots*, TALK SATELLITE—ASIA PACIFIC (Apr. 8, 2013), http://www.talksatellite.com/Asia-A101283.htm.

291. SAMUEL BLACK, NO HARMFUL INTERFERENCE WITH SPACE OBJECTS: THE KEY TO CONFIDENCE BUILDING (2008), *available at* http://www.stimson.org/images/uploads/research-pdfs/NHI_Final.pdf.

292. Outer Space Treaty*, supra* note 271, art. VI.

293. Lee, *supra* note 288, at 129.

> 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.

Article VI requires the appropriate State to authorize and continually supervise space activities of State and non-State entities, making any act of appropriation taking place under the State's influence, supervision or direction a violation of Article II.[294] Article VI also holds States internationally responsible for space activities of both State and non-State entities, including all activities involving satellites and satellite communications. This means States not only have a duty to actively manage and supervise the satellite communications of both State and non-State entities, but also States must not allow such entities to act contrary to the rights of others States,[295] including engaging in satellite signal interference in violation of the ITU regime.

Insofar as supervision, authority and control are concerned, Article VIII of the Outer Space Treaty further ties activities of non-State entities to State parties. According to Article VIII, the State on whose registry an object is launched into space must retain jurisdiction and control over such object while in outer space.[296] Ownership of such an object is not changed by its presence in outer space.[297] Under the Registration Convention, which establishes the link between State and spacecraft,[298] a "launching State" (defined as the State that either launches or procures the launch of a space object, or a State from whose territory or facility an object is launched)[299] must register the object in its domestic registry and with the United Na-

---

294. *Id.*

295. Outer Space Treaty, *supra* note 271, art. VI; Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

296. Outer Space Treaty, *supra* note 271, art. VIII.

297. *Id.,* art. VIII.

298. I.H. Ph. Diederiks-Verschoor, *Registration of Spacecraft*, *in* NEW FRONTIERS IN SPACE LAW 125 (Edward McWhinney & Martin A Bradley eds., 1969).

299. Registration Convention, *supra* note 271, art. I.

tions.[300] Collectively, Article VIII of the Outer Space Treaty and the Registration Convention permanently tie the State of registry to a launched object, as well as establish the link between registration, legal responsibility and liability under Article VII of the Outer Space Treaty.

Article VII holds States financially liable for any damages caused by objects launched into space. Specifically, Article VII provides that States launching or procuring the launching of an object into space are "internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air space or in outer space, including the Moon and other celestial bodies."[301] Read in conjunction with Articles VI and VIII of the Outer Space Treaty, Article VII imposes financial liability on launching States whenever damage is caused on Earth, in airspace or in outer space by objects launched into outer space by State, non-State, private and commercial entities. Article VII, however, is limited in both scope and application; it applies only to *physical* damage[302] caused *by objects* launched *into* outer space. Article VII of the Outer Space Treaty does not apply to non-physical damage or to physical damage not *caused by* an "object," an object being "something that can be seen or touched."[303] Article VII would also not apply to objects never launched into space, such as terrestrial jammers.

Applying this analysis to satellite signal interference, Article VII may then only apply in situations where interference is generated by a satellite (or other object launched *into* outer space) *and* when those activities actually result in *physical* damage. As testimony before the 1967 U.S. Senate Foreign Relations Committee on the Outer Space Treaty reveals, the United States believed Article VII liability did not apply to "damages of an electronic nature in outer space with respect to radio and ray and various electronic

300. *Id.,* art. II.

301. Outer Space Treaty, *supra* note 271, art. VII.

302. In fact, U.S. Senate hearings on the Outer Space Treaty indicate that liability under Article VII, "has never been viewed by any state participating in [U.N.] discussions . . . [to go] beyond physical damage." *See Treaty of Outer Space, Hearings before S. Comm. on Foreign Relations*, 90th Cong., 1st Sess. 70–72 (1967) (testimony of U.S. Ambassador Arthur Goldberg).

303. *Object*, MERRIAM-WEBSTER ONLINE DICTIONARY, http://www.merriam-webster.com/dictionary/object. Applying an ordinary and plain meaning to the term "object" is the general rule for treaty interpretation. *See* Vienna Convention on the Law of Treaties art. 31(1), May 23, 1969, 1155 U.N.T.S. 331 [hereinafter VCLT] ("a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose").

communications."[304] While the U.S. opinion does not dictate what drafters of Article VII contemplated, it may indicate how the United States might frame responses to any claims made against it for damages involving satellite signal interference.

Article VII also fails to address causal links required between the object and resulting physical damage, i.e., whether indirect physical damages are covered under Article VII. For example, if satellite A were to jam satellite B causing satellite B to collide with satellite C, would the launching State of satellite A be liable for damages to the launching States of both B and C? Article VII fails to address such a scenario.

The Liability Convention, promulgated to elaborate on liability for damages caused by space objects as set forth in the Outer Space Treaty,[305] defines damage as "loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations."[306] The Liability Convention imposes liability only when damage is *physically caused* by a space object in a crash, explosion or other direct harm.[307] Assuming jamming effects and spoofing activities remain limited to temporary disruptions and/or indirect damages (such as "consequential" economic losses), the Liability Convention does not appear to apply to satellite signal interference. Additionally, because satellite signal interference and radio frequency spectrum are not "objects" or "space objects," an argument can also be made that the Liability Convention, like Article VII, is inapplicable when interference emits from Earth-based stations. However, because Article VII and the Liability Convention have never been asserted as a basis for damages resulting from satellite signal interference, it is difficult to discern the actual scope or extent of eithers' reach.[308]

Setting the above uncertainty aside, ISL does not completely supersede general principles of liability under international law. As previously noted, international law is explicitly referenced and incorporated into ISL under Article III of the Outer Space Treaty. Thus, even though the Outer Space

304. *See Treaty of Outer Space, Hearings before S. Comm. on Foreign Relations*, 90th Cong., 1st Sess. 71 (1967) (testimony of U.S. Senator Albert Gore).

305. Liability Convention, *supra* note 271, pmbl.

306. *Id.*, art. I.

307. CARL Q. CHRISTOL, SPACE LAW: PAST, PRESENT, AND FUTURE 219–20 (1991).

308. Under Article 31 (b) of the Vienna Convention on the Law of Treaties, treaty interpretation shall take into account, "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation." VCLT, *supra* note 303.

Treaty and the Liability Convention do not clearly address financial recovery for the full range of damages resulting from satellite signal interference, a State remains liable under international law if it breaches any international obligation.[309] As addressed above, all ITU member States are obligated not to cause harmful interference and to enforce and respect the ITU regulatory regime. Moreover, as recognized in the *Corfu Channel* and *Trail Smelter Arbitration Tribunal* decisions, a State has an obligation "not to allow its territory to be used for acts contrary to the rights of other States."[310] Finally, in the *Chorzow Factory* case, the Permanent Court of International Justice laid down the principle that a State committing an unlawful act must make reparation for the damage caused.[311] Thus, even though ISL may not cover liability for satellite signal interference, States retain the duty "to protect other States against injurious acts by individuals from within their jurisdiction."[312] A similar principle is found in Article IX of the Outer Space Treaty.

Article IX declares, "State Parties . . . shall be guided by the principle of cooperation and mutual assistance and shall conduct all their activities in outer space . . . with due regard to the corresponding interests of all other State Parties to the Treaty. . . ." Article IX further provides, in relevant part:

> 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 . . . would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space, . . . 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 . . . would cause potentially harmful interference with activities in the peaceful exploration and use of outer space, . . . may request consultation concerning the activity or experiment.

309. BIN CHENG, GENERAL PRINCIPLES OF INTERNATIONAL LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 226 (1953).

310. *Corfu Channel, supra* note 295, at 23; Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1907 (1938).

311. *Factory at Chorzow*, *supra* note 284, at 21.

312. *Trail Smelter*, *supra* note 310.

Interpreted in an ordinary and plain meaning and read in the context of the Outer Space Treaty,[313] Article IX is an obligation on States to consider legal rights of other States, both prior to and during any ongoing activities.[314] However, "States can disregard any anticipated impact on rights that do not correspond to peaceful use and exploration."[315] In placing an obligation on States to exercise "due regard," Article IX imposes a consultation requirement on a State party if that State believes its activity would cause interference that is potentially harmful.

To trigger the consultation requirement, three conditions must be satisfied: (1) an activity is planned by a State or its nationals; (2) the State has reason to believe the activity has the potential to cause interference that is harmful; and (3) the interference must potentially interfere with the activities of other States in their peaceful exploration and use of outer space.[316] The first condition reflects the link between a State and its nationals established by Articles VI and VIII of the Outer Space Treaty, as well as under the Registration Convention. Under the second condition, the responsibility and authority to determine whether the activity at issue may cause potentially harmful interference lies with the State planning the action. If a State "ha[s] knowledge that proves the assertion that a planned activity would cause potentially harmful interference,"[317] the second condition is satisfied. The second condition requires the State to "know" the effect of its activity on other States, as well as a determination by the State of whether the activity's effect qualifies as harmful interference as contemplated in Article IX and ISL.

While the phrase "harmful interference" is defined under the ITU,[318] it is not defined nor explicitly proscribed by the Outer Space Treaty. However, when Article IX was negotiated, one motivating factor was the U.S.'s

313. The standard method of treaty interpretation, as adopted by the International Court of Justice, is articulated in Article 31 of the Vienna Convention on the Law of Treaties. Article 31 states, "treaties shall be interpreted in good faith and in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose." VCLT, *supra* note 303.

314. Mineiro, *supra* note 274, at 334.

315. *Id.*

316. *Id.* at 334–35.

317. *Id.* at 336.

318. "Harmful interference" is defined as interference with a radio signal that endangers the functioning of a radio service or seriously degrades, obstructs, or repeatedly interrupts a radio communication service operating in accordance with ITU Radio Regulations. ITU Radio Regulations, *supra* note 190, art. 1.169.

Project West Ford, which studied the effects on global radio communications of dispersing a network of five hundred thousand tiny copper metal strips (dipoles) into a short-lived orbit.[319] When the project became public, a community of international scientists and astronomers protested, voicing concerns the project would interfere with their studies on optical and radio astronomy, especially if the dipoles remained in orbit beyond their one- to two-year life cycle.[320] The project was also condemned at the United Nations by the Soviet Union and several other States.[321]

In 1960, the Academy of Sciences studied the project effects and soon thereafter, the United States publically announced Project West Ford would be a short-term project. Specifically, the U.S. statement provided, in relevant part:

> No further launches of orbiting dipoles will be planned until after the results of the West Ford experiment have been analyzed and evaluated. . . . Any decision to place additional quantities of dipoles in orbit, subsequent to the West Ford experiment, will be contingent upon the results of the analysis and evaluation and the development of necessary safeguards against harmful interference with space activities or with any branch of science. Optical and radio astronomers throughout the world should be invited to cooperate in the West Ford experiment to ascertain the effects of the experimental belt in both the optical and the radio parts of the spectrum.[322]

The U.S. pledge, however, failed to quell the International Astronomical Union (IAU) concerns, which issued a resolution "to all governments … launching space experiments which could possibly affect astronomical research" to consult with the IAU before conducting such experiments.[323] In response to these concerns, as well as Soviet Union condemnation of Project West Ford, UN Ambassador Adlai E. Stevenson announced:

---

319. Mineiro, *supra* note 274, at 337; Irwin I. Shapiro, *Orbital Properties of the West Ford Dipole Belt*, IEEE XPLORE, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=& arnumber=1444922&isnumber=31060 (last visited Feb. 11, 2014).

320. DELBERT R. TERRILL JR., THE AIR FORCE ROLE IN DEVELOPING INTERNATIONAL OUTER SPACE LAW 63 (1999).

321. Kathleen Teltsch, *6 Soviet Space Failures Believed To Have Been Probes of Planets*, NEW YORK TIMES, June 16, 1963, at A2.

322. TERRILL, *supra* note 320, at 65.

323. *Id.* at 64–65

> The U.S. would conduct no more such experiments until the results of this one were fully analyzed, and in any case none without proper scientific safeguards; The results of the experiment would be disclosed to interested scientists of all nations; Prior consultations with scientists would precede any further activity of this nature; Advance notice of the launching of such experiments would be given in accordance with the procedure recommended by the General Assembly.[324]

It is this precedent created by the United States that provided the basis for Article IX.[325]

Today, harmful interference in outer space falls into three primary categories: (1) observational interference (terrestrial based astronomical observations or space based terrestrial observations); (2) radio frequency interference (as defined by the ITU); and (3) physical interference (interference with the freedom of movement and/or physical operations in outer space).[326] Under this classification, interference with satellite signals may in fact qualify as potentially harmful interference. However, because harmful interference is understood more broadly under the Outer Space Treaty than under the definition adopted by the ITU, States have wide latitude in determining when their activities constitute harmful interference under the Outer Space Treaty and whether their activities trigger the duty to consult. Moreover, there has never been any consultation under the auspices of Article IX despite the fact States have questioned others about outer space activities deemed dangerous or potentially hazardous,[327] and at least one State initiated international discussions despite declaring it had no Article

---

324. Norman Thorpe, *The Process of Space Law Development* 3 (unpublished paper delivered at Major Command Judge Advocate Conference, Bolling Air Force Base, Washington DC, Nov. 16, 1967), http://www.docstoc.com/docs/33978175/The-Air-Force-Role-in-Developing-International-Outer-Space-Law.

325. *Id.*

326. Mineiro, *supra* note 274, at 337.

327. The United States issued several demarches in response to China's 2007 kinetic shoot down of its aging weather satellite, Feng-Yun-1C. Jeff Foust, *WikiLeaks Cables on US-China ASAT Testing*, SPACE POLITICS (Feb. 3, 2011), http://www.spacepolitics.com/2011/02/03/wikileaks-cables-on-us-china-asat-testing/. The United Kingdom stated it was concerned about the creation of debris generated and China's lack of international consultation. *Britain Concerned by Chinese Satellite Shoot-Down*, SPACE WAR (Jan. 19, 2007), http://www.spacewar.com/reports/Britain_Concerned_By_Chinese_Satellite_Shoot_Down_999.html. Japan asked China for an explanation and stated nations "must use space peacefully." *Concern Over China's Missile Test*, BBC NEWS (Jan. 19, 2007), http://news.bbc.co.uk/2/hi/asia-pacific/6276543.stm.

IX obligation to do so.[328] The absence of implementation in situations where Article IX may otherwise seem to apply suggests a possible emergence of customary international law which could effectively amend the Outer Space Treaty by narrowly constraining the application of Article IX.[329] Arguably, State practice seems to reflect a general understanding that some type of notification is expected even when activities do not trigger Article IX obligations.

The third condition triggering a State's obligation to undertake Article IX consultations requires the proposed activity (assuming it satisfies the threshold for the first and second conditions set forth above) to interfere with activities of other States in their peaceful exploration and use of outer space. This requires a determination as to whether other States' activities meet the criteria for peaceful use and exploration.[330] If such States' activities are not peaceful, Article IX has not been triggered and there is no duty to undertake international consultations.[331]

The term "peaceful purposes" is not defined in the Outer Space Treaty, but is referenced in its preamble. While some legal scholars assert "peaceful" means "non-military,"[332] others suggest "peaceful" means "non-aggressive" or "non-hostile."[333] Despite a long and historical disagreement over the meaning of "peaceful purposes," most experts now agree the Outer Space Treaty does not prohibit military use of space.[334] State prac-

328. In 2008, prior to the U.S. shoot down of its satellite, USA-193, the United States openly declared it had no obligation under the Outer Space Treaty, Article IX, but nonetheless voluntarily notified other States of the planned action in the spirit of international cooperation. U.S. Department of Defense News Transcript, DoD News Briefing with Deputy National Security Advisor Jeffrey, General Cartwright and NASA Administrator Griffin (Feb. 14, 2008), http://www.defense.gov/transcripts/transcript.aspx?transcript id=4145.

329. VCLT*, supra* note 303, art. 31(b).

330. Mineiro, *supra* note 274, at 338.

331. *Id.*

332. BIN CHENG, STUDIES IN INTERNATIONAL SPACE LAW 520–22 (1997).

333. Schmitt, *Military Operations in Space*, *supra* note 51, at 101. In 1962, U.S. Senator Albert Gore Sr., in comments made at the United Nations, stated that the U.S. view was that "outer space should be used only for peaceful purposes—that is non-aggressive and beneficial purposes." *International Space Treaties Travaux Preparatoires,* U.N. GOAR, 17th Sess., 1289th Mtg, U.N. Doc. A/C.1/PV.1289 (1962).

334. Ivan A. Vlasic, *The Legal Aspects of Peaceful and Nonpeaceful Uses of Outer Space, in* PEACEFUL AND NON-PEACEFUL USES OF SPACE, PROBLEMS OF DEFINITION FOR THE PREVENTION OF AN ARMS RACE 45, 45–47 (Bhupendra Jasani ed., 1991).

tice[335] also supports the proposition that "peaceful" should be interpreted to mean "non-aggressive" or "non-hostile."[336] There has even been "consensus, within the United Nations that 'peaceful' equates to 'non-aggressive.'"[337] As will be further addressed below, the UN Resolution on the Definition of Aggression defines aggression as "the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the UN, as set out in this definition."[338]

In light of the above, "peaceful purposes" and "peaceful use and exploration" should mean a State's activity in outer space must not involve aggressive behavior. That is, if a State's activity amounts to aggression, an unlawful use of force or rises to the level of an armed attack, as contemplated under the UN Charter (and as will be explored in Section IV), there is no obligation on another State to undertake appropriate international consultations before interfering with that activity. In such a case, observational interference, radio frequency interference and physical interference affecting that non-peaceful activity would not violate ISL. Moreover, if Article IX was suspended between belligerents,[339] a belligerent State would only be required to conduct appropriate international consultations with neutral parties under the law of neutrality, when applicable.[340] However,

---

335. Pursuant to Article 31(3)(b) of the Vienna Convention on the Law of Treaties, treaty interpretation shall "take into account . . . any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation." VCLT*, supra* note 303.

336. Richard A. Morgan, *Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and "Peaceful Purposes,"* 60 JOURNAL OF AIR LAW AND COMMERCE 237, 303–9 (1994).

337. Walter D. Reed & Robert B. Norris, *Military Use of the Space Shuttle*, 13 AKRON LAW REVIEW 665, 678 (1979); CHRISTOL, *supra* note 307, at 16.

338. Definition of Aggression art. 1, G.A. Res. 3314 (XXIV), U.N. Doc. A/RES/3314 (XXIV) (Dec. 14, 1974).

339. OPPENHEIM'S INTERNATIONAL LAW 302 (Robert Jennings & Arthur Watts eds., 9th ed. 1992).

340. The law of neutrality was formally established in 1907 by Hague Convention (V). Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310. As Article I provides that the territory of neutral State is inviolable, it highlights a question as to whether satellites or signals can qualify as "territory" of a State. Assuming a satellite or signal is deemed "territory" of a State, the law of neutrality under Hague V would limit the type of actions that can be taken against a satellite or a signal of a neutral State. Hague V law did not contemplate satellites, satellite communications or even outer space activities. However, as several actions permitted under Hague V are analogous to these activities, specifically, Articles 8

because Article IX only imposes a duty to consult in good faith,[341] and does not mandate that parties reach a mutually agreeable solution,[342] consultations would solely depend on the nature and extent of the planned activity.[343] Thus, if a belligerent deemed its outer space activity would not cause harmful interference to a neutral party, Article IX consultations would not be triggered.

The final point of discussion on Article IX involves the meaning of "appropriate international consultations." The Outer Space Treaty does not identify any procedure for "appropriate international consultations" nor does it designate an agency or international body with which States should consult in evaluating their activities.[344] At a minimum, "appropriate international consultations" requires States to provide affected States sufficient information to take appropriate action to avoid potentially harmful interference and to mitigate effects.[345] It does not provide States any ability to limit, prevent or even prohibit another State from engaging in activities constituting harmful interference. Article IX only allows an affected State party the right to put forth a request for consultation, but the result of the consultation is not stipulated.[346]

Regardless of the obligation to undertake "appropriate international consultations," there have been no formal attempts by any State to hold another State responsible for a breach of that duty. Indeed, States have been vocal when it comes to outer space activities that have had the potential to be harmful, but States have rarely, if ever, gone so far as to declare such an activity is outright illegal. The reluctance to do so is likely tied to States' desire to preserve a full range of activities in outer space in peacetime, as well as during armed conflict.

The foregoing raises one additional provision under the Outer Space Treaty deserving brief discussion. Article IV relates to the militariza-

---

and 9 relate to telegraph, telephone and wireless telegraphy, given their role in global trade and their purpose of mitigating the spread of armed conflict, "it is almost inconceivable that the law of neutrality would not apply to satellite communications." *See* Jarman, *supra* note 60, at 85.

341. Mineiro, *supra* note 274, at 338–39.

342. Jarman *supra* note 60, at 39.

343. Brandon Hart, *Legal Implications Surrounding Recent Interception of Spy Satellite*, JOINT CENTER FOR OPERATIONAL ANALYSIS JOURNAL, June 2008, at 32.

344. Mineiro, *supra* note 274, at 338.

345. *Id.* at 339.

346. Li Juqian, *Legality and Legitimacy: China's ASAT Test*, 5 CHINA SECURITY 45, 48 (2009).

tion and weaponization of outer space. Specifically, Article IV provides as follows:

> States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner. The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. 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. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the Moon and other celestial bodies shall also not be prohibited.

While this article will not go into detail in discussing Article IV there are some important considerations. First, even though there have been many discussions on the term "peaceful purposes," the predominant opinion, as already mentioned, is "peaceful" means "non-aggressive."[347] Second, treaty drafters deliberately and intentionally excluded conventional weapons from the prohibition.[348] Third, Article IV creates only a partial demilitarization of space, which is specifically applicable only during peacetime.[349] This assumes ISL treaty obligations between belligerents would be suspended in a state of armed conflict. Finally, the Article IV ban focuses on nuclear weapons. Other weapons, such as conventional, biological, chemical and "exotic future weapons," including laser beams, can be deployed without violating Article IV unless they can be classified as a weapon of mass destruction.[350]

Jamming, which typically involves no direct physical damage, would not cause mass destruction in the same way as a nuclear weapon.[351] Even if it did, the weapon of mass destruction might not be in space.[352] For exam-

347. CARL Q. CHRISTOL, THE MODERN INTERNATIONAL LAW OF OUTER SPACE 5 (1982).

348. Michel Bourbonniére & Ricky J. Lee, *Legality of the Deployment of Conventional Weapons in Earth Orbit: Balancing Space Law and the Law of Armed Conflict*, 18 EUROPEAN JOURNAL OF INTERNATIONAL LAW 873, 882–86 (2007).

349. *Id.* at 877.

350. Maogoto & Freeland, *supra* note 54, at 1105–6, 1111.

351. GREENBERG ET AL., *supra* note 3, at 9.

352. *Id.*

ple, if a satellite is used to relay a jamming signal, the weapon of mass destruction (the initiator of the signal) may be located on Earth, and the satellite is only a tool used to carry out the attack, just as satellites used for navigation and guidance of intercontinental ballistic missiles would not be weapons of mass destruction.[353] In such a case, this act would not violate Article IV of the Outer Space Treaty.

As the above discussion reveals, in addition to the enforcement problems within the ITU regime, ISL too may not limit jamming, nor does it specifically protect States from intentional interference. Nevertheless, Article III of the Outer Space Treaty brings in the full force and effect of the UN Charter and international law. Thus, even though the ITU and ISL offer limited protection, intentional interference is not *non liquet*, or within a total legal vacuum.

Because the UN Charter stipulates obligations under it override obligations under any other international agreement,[354] the Outer Space Treaty is subject to the terms of the Charter and must be considered in the broader context of public international law.[355] Therefore, the Outer Space Treaty does not modify any right or obligation within the UN Charter. Since the Charter addresses a State's inherent right of self-defense,[356] as long as a State is acting in self-defense its actions would not violate the Outer Space Treaty, assuming they otherwise comply with IHL, other provisions within the UN Charter and general principles of international law.

D. The Principle of Non-Intervention

In addition to violating ITU and ISL frameworks, satellite signal interference may also constitute a breach of the non-intervention principle, an autonomous principle of customary law.[357] However, international law does not specifically address whether sovereignty exists in a satellite signal, and no State has ever claimed satellite signal interference violated its sovereignty.

---

353. *Id.*, citing Richard W. Aldrich, *The International Legal Implications of Information Warfare* 20 (U.S. Air Force Institute for National Security Strategic Studies, Research Paper, 1996).

354. U.N. Charter art. 103.

355. Bourbonniére & Lee, *supra* note 348, at 887.

356. U.N. Charter art. 51.

357. OPPENHEIM'S INTERNATIONAL LAW, *supra* note 339, at 429.

Non-intervention is the correlative of State sovereignty, a State's independence to exercise supreme authority over all people and things within its territory.[358] In *Corfu Channel,* the International Court of Justice (ICJ) noted, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[359] The principles of independence and non-intervention are also recognized in Article 2(7) of the UN Charter, which provides:

> Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.

The significance of State sovereignty and non-intervention is further emphasized in the UN Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States.[360] With a view towards maintaining international peace, the Declaration proclaims:

> No state . . . has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other state. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the state or against its political, economic and cultural elements, are in violation of international law.

Finally, in *Nicaragua* the ICJ noted the principle's customary status and scope by stating non-intervention, "forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States."[361] The Court also held:

> A prohibited intervention must . . . be one bearing on matters in which each State is permitted, by the principles of State Sovereignty, to decide

---

358. Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 JOURNAL OF CONFLICT & SECURITY LAW 211, 222 (2012).

359. *Corfu Channel, supra* note 295, at 35.

360. Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, G.A. Res 2625 (XXV), U.N. Doc. A/8082 (Oct. 24, 1970) [hereinafter Declaration on Friendly Relations].

361. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S), 1986 I.C.J. 14, ¶ 205 (June 27) [hereinafter *Nicaragua*].

> freely. One of these is the choice of political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones . . . the element of coercion . . . defines, and intended forms the very essence of prohibited intervention. [362]

An intervention is only wrongful when using methods of coercion.[363] Moreover, because the decisive test remains coercion,[364] some academics believe "interference pure and simple is not intervention."[365] It then follows from this assertion, if there is no coercive element, there is no per se violation of the non-intervention principle.[366]

In the context of satellite signal interference, a violation of the non-intervention principle would exist if a broadcast signal was jammed and spoofed with coercive political messages for effecting a regime change or an election.[367] Likewise, if jamming or spoofing were used to manipulate financial markets, it would constitute prohibited intervention. On the other hand, if jamming or spoofing was used to disrupt or prevent the broadcast of a television or news broadcast, but had no coercive element, the act may not violate the non-intervention principle.

E. International Humanitarian Law

Given the likelihood that satellite signal interference will assume a greater role in future armed conflicts, a question emerges as to whether the body of law regulating the conduct of armed conflict (*jus in bello)* or IHL[368] can adequately protect civilians and civilian property from this new technical and military reality. As discussed above, because the military is so dependent on unprotected commercial communication satellite systems, these dual-use objects have become increasingly vulnerable to disruptions by way of jamming and spoofing attacks. In addition, due to the interconnected nature of civilian and military communication systems, it is almost impossible to differentiate between purely civilian systems and purely military systems,

---

362. *Id.*

363. *Id.*

364. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 45 (Michael N. Schmitt ed., 2013).

365. OPPENHEIM'S INTERNATIONAL LAW, *supra* note 339, at 432.

366. TALLINN MANUAL, *supra* note 364, at 44.

367. *Id.*

368. WILLIAM H. BOOTHBY, THE LAW OF TARGETING 3 (2012).

or limit the effects of an attack to only military targets.[369] Thus, satellite signal interference aimed at military communications during armed conflict will likely have an impact, perhaps even a severe impact, on civilian communications that provide essential services to civilian, economic, State and other non-military entities. To illustrate an impact of satellite communication disruptions, one need only to consider the impacts of a 1996 incident involving a programming error with the GPS constellation. Six seconds after an erroneous time was accidentally entered into the system, over one hundred cellular networks were shutdown, taking hours and even days to recover.[370] Given the extensive dependence on GPS signals by military, civilian and economic users, it is not hard to imagine the extent of such a disruption today.

Even though there are no reported instances of intentional interference with commercial communication satellites during armed conflict causing devastating effects on civilian objects or the civilian population, it is possible. Indeed, most instances of satellite signal interference cause only temporary and annoying disruptions. However, potential catastrophic scenarios, such as disruptions of critical financial infrastructures, collisions between aircraft or even losing communication capabilities with remotely piloted aircraft carrying weapons could occur. For these reasons, it is important to examine how States may interpret IHL with regard to satellite signal interference and assess how IHL may be challenged by this emerging phenomenon. While a comprehensive discussion of IHL is well beyond the scope of this article, the basic sources of IHL and several primary principles will be briefly discussed to provide a basic understanding of implications emerging from interfering with commercial communication satellite signals during armed conflict.

The principles of IHL have developed as a result of international agreement that armed conflict is subject to specific legal constraints and must be conducted in accordance with minimum international standards.[371] Initially rooted in customary law, IHL is now codified within a variety of rules and treaties, including the Hague and Geneva Conventions and the Additional Protocols of 1977.[372] In simple terms, Hague treaties address the

369. Droege, *supra* note 112, at 7.

370. Bruce Carlson, *Protecting Global Utilities: Safeguarding the Next Millennium's Space Based Public Services*, AEROSPACE POWER JOURNAL, Summer 2000, at 37, 38.

371. Steven Freeland, *In Heaven as on Earth? The International Law Regulation of the Military Use of Outer Space*, 8 US-CHINA LAW REVIEW 272, 278 (2011).

372. *Id.* at 280.

behavior of belligerents and the means and methods of warfare, including the lawfulness of weapons and targeting,[373] whereas the Geneva Conventions focus on protecting personnel involved in international armed conflicts, and addressing such issues as prisoners of war, civilians and wounded combatants.[374]

Even though IHL frameworks do not specifically address satellite signal interference as a means or method of warfare, they do set forth legal boundaries with which all States are obliged to comply during any armed conflict.[375] The UN Security Council also demands strict compliance with IHL obligations during armed conflicts.[376] It is important to emphasize that it is only in the context of an armed conflict (an international armed conflict (IAC)[377] or a non-international armed conflict (NIAC)[378]) that IHL rules apply.[379]

While a discussion of the criteria for and rules specific to IACs and NIACs is beyond the scope this article,[380] classifying a conflict is necessary to determine the specific legal regime applicable to that conflict[381] and the

373. Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227, 2295.

374. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter API].

375. Legality of the Threat or Use of Nuclear Weapons*,* Advisory Opinion, 1996 I.C.J. 226, ¶ 79 (July 8) [hereinafter *Nuclear Weapons*].

376. Protection of Civilians in Armed Conflict, S.C. Res. 1674, ¶ 6, U.N. Doc. S/RES/1674 (Apr. 28, 2006).

377. An international armed conflict exists whenever there are hostilities, declared war or any other armed conflict between two or more States. *See, e.g.*, Convention Relative to the Treatment of Prisoners of War art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter POW Convention].

378. A non-international armed conflict exists whenever there are hostilities between governmental armed forces and dissident armed forces or other organized groups. Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts art. 1, June 8, 1977, 1125 U.N.T.S. 609. A NIAC also exists for conflicts that meet the Common Article 3 criteria of the 1949 Geneva Conventions. *See, e.g.*, POW Convention, *supra* note 377, art. 3.

379. Droege, *supra* note 112, at 7; BOOTHBY, *supra* note 368, at 388.

380. For a thorough discussion as to what rules apply to IACs and NIACs and in the spectrum of conflict, see BOOTHBY, *supra* note 368, at 43–54, 429–54.

381. Michael N. Schmitt, *Classification of Cyber Conflict*, 17 JOURNAL OF CONFLICT & SECURITY LAW 245 (2012); *see also* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICT (Elizabeth Wilmshurst ed., 2011).

rules governing targeting decisions.[382] Thus, if satellite signal interference is conducted in the context of an IAC, its use and application is subject to specific rules for IAC as set forth within the IHL normative framework. Likewise, if interference is utilized in a NIAC, the rules applicable to NIAC would apply.

However, if satellite signal interference were employed in operations outside armed conflict, IHL considerations need not be made, even if such operations were directed at civilians or civilian objects.[383] Additionally, IHL does not prohibit disseminating propaganda or economic sanctions deliberately targeting the military and civilian populations.[384] Thus, if satellite signal interference were employed against commercial communication satellites and their signals for such purposes, the targeting of civilians and these civilian objects would be permissible under IHL, regardless of the unlawfulness of the jamming and spoofing activities under the ITU or ISL frameworks.

Aside from the legality of a State's decision to use force (*jus ad bellum*), discussed in Section V, the law governing the means and methods of force application (*jus in bello*), or IHL, always applies. In other words, IHL must always be respected and followed during an armed conflict regardless of whether the decision to use force was legitimate and within legal norms. The overarching IHL considerations include: military necessity, discrimination and proportionality.

1. The Principle of Military Necessity

Military necessity is part of customary international law for armed conflict.[385] The principle of military necessity permits States to use only the degree and kind of force required to achieve the legitimate purpose of the conflict.[386] For a target to constitute a legitimate military objective, the responsible decision maker must determine, based on information reasonably available, that an object by its "nature, location and purpose or use make[s]

382. BOOTHBY, *supra* note 368, at 43.

383. Droege, *supra* note 112, at 27.

384. BOOTHBY, *supra* note 368, at 43.

385. Yoram Dinstein, *Legitimate Military Objectives under the Current* Jus in Bello, *in* LEGAL AND ETHICAL LESSONS OF NATO'S KOSOVO CAMPAIGN 139, 140 (Andru E. Wall ed., 2002) (Vol. 78, U.S. Naval War College International Law Studies).

386. INTERNATIONAL AND OPERATIONAL LAW DEPARTMENT, THE JUDGE ADVOCATE GENERAL'S LEGAL CENTER AND SCHOOL, LAW OF WAR DESKBOOK 139–40 (2001) [hereinafter LAW OF WAR DESKBOOK]; *see also* BOOTHBY, *supra* note 368, at 59.

an effective contribution to military action" and that its "total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[387] Attacks against civilian objects are prohibited.[388] Objects contributing to military action by their "nature" include all objects used by the military, including weapons, equipment, transport, buildings occupied by the military and communication centers.[389] Such objects must have an inherent attribute or character that contributes to military action.[390] Military objectives are not limited to military bases, units, equipment or forces, and may include other objects making an effective contribution to the opposing force's ability to conduct hostilities. Applied to commercial satellite communications, interference may occur, assuming both a reasonable possibility exists that the communications make an effective contribution to military activities and interfering with the communications would offer a military advantage.

A military's use of any satellite to provide instantaneous global service during peace and in war satisfies the nature criteria and makes them lawful military objectives. This would also include military satellites, commercial communication satellites and GPS satellites, as well as remote sensing satellites.[391] "Location" refers to "objects which by their very nature have no military function but which, by virtue of their location, make an effective contribution to military action."[392] For commercial communication satellites, this could be any satellite that is or can relay military communications or support military operations. In armed conflict, it would be important for one party to employ measures, such as jamming attacks against commercial communication satellites, to prevent the opposing force from using them.

The "purpose" of a military objective relates to intended future uses of an object, whereas "use" reflects the object's current function.[393] With commercial communication satellites, because such objects make an effective contribution to the military at all times, and especially in armed conflict

387. API*, supra* note 374*,* art. 52(2).

388. *Id.*, arts. 52(1), 52(3).

389. HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 185 (2012); LAW OF WAR DESKBOOK, *supra* note 386, at 141–42.

390. *Id.*

391. Jarman, *supra* note 60, at 50.

392. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 2021 (Yves Sandoz, Christophe Swinarski & Bruno Zimmerman eds., 1987).

393. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 89 (2d ed. 2010).

as demonstrated during the Iraq War, this means they are considered military objectives, valid military targets and susceptible to attack. Along those same lines, any object launching jamming and spoofing attacks during armed conflict would also become a valid military objective and thus liable to attack.

Given the military's reliance and dependence on commercial communication satellites, it is obvious these satellites and systems can and will be targeted during armed conflict. Not only would disrupting such satellites provide an opposing force a clear and direct military advantage over their enemy, their disruption or destruction would likely (and quickly) lead to that enemy's partial or complete submission. The use of satellite signal interference in warfare would also allow States to avoid the physical destruction of satellite system components and contamination of the outer space environment.

As the above discussion reveals, commercial communication satellites will often qualify as valid and lawful military targets under the principle of military necessity, and intentional interference as a means and method of warfare satisfies the degree of force requirement. The unavoidable fact is not only can civilian systems be lawfully targeted, but, when they are, military and civilians using these systems have little legal protection under the principle of military necessity.

2. The Principle of Discrimination

Another fundamental principle of customary international law and IHL is the principle of discrimination.[394] This principle, appearing first in 1868 in the preamble of the St. Petersburg Declaration,[395] is now codified in Article 48 of Protocol I to the Geneva Conventions of 1949, which dictates that civilians and civilian property must be protected from attacks. It provides: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian ob-

394. BOOTHBY, *supra* note 368, at 60.

395. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Nov. 29/Dec. 11, 1868, 18 Martens Nouveau Recueil (ser. 1) 474, *available at* http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=568842C2B90F4A29C12563CD0051547C.

jects and military objectives and accordingly shall direct their operations only against military objectives."[396]

According to Article 52 of Protocol I, civilian objects are defined as "all objects which are not military objectives."[397] Combatants must always distinguish themselves from civilians, and civilian objects must not be mistaken for military targets.[398] In other words, if an object is claimed to be civilian, it should be separated from military objects.

In practicing discrimination, "constant care" must be taken "to spare the civilian population, civilians and civilian objects."[399] Moreover, attacks against non-specific military targets or using methods that cannot be exclusively targeted or contained against solely military targets are prohibited; they violate the distinction principle.[400] However, as previously discussed above, these requirements would be virtually impossible to achieve with respect to dual-use commercial communication satellites. Because much of space is dual-use, complying with the distinction constraint requires a balancing of military necessity and civilian collateral effects.[401] Thus, when commercial satellite signals qualify as valid military targets, but collateral effects expected are excessive in relation to military necessity, a violation of IHL occurs.

Under Article 51(4) of Protocol I indiscriminate attacks are prohibited.[402] According to the International Committee of the Red Cross, this provision is an "application of the prohibition on directing attacks against civilians or against civilian objects."[403] With respect to satellite signal interference and discrimination, many technologies used and employed to jam satellite signals may not be very precise. Indeed, jamming is a sloppy application often resulting in the mass disruption of a wide range of adjacent signals. Thus, even if only one signal is targeted, other signals may also be disrupted. Despite this unintended impact on other signals, it does not necessarily change the military validity of the targeted signal.

---

396. API*, supra* note 374*,* art. 48.

397. *Id.,* art. 52(1).

398. *Id.,* art. 57. Prosecutor v. Kupreskic, IT-95-16-T, Trial Judgment, ¶ 521 (Int'l Crim. Trib. for the former Yugoslavia Jan. 14, 2000).

399. API*, supra* note 374, art. 57(1).

400. Bourbonniére, *Law of Armed Conflict*, *supra* note 187, at 48.

401. API*, supra* note 374, arts. 51(5)(b), 57(2)(a)–57(2)(b).

402. *Id.*, art. 51(4).

403. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 43 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2009).

Developed nations and sophisticated non-State actors may have methods and means to locate and target specific satellite signals, but groups of terrorists, individuals or unorganized groups may not. Thus, and as interference and jamming are increasingly employed during armed conflict by actors without the ability to precisely target specific signals, a wide range of State and non-State users may suffer disruptions. What is more, while in the midst of an intense armed conflict, it may be difficult for even the most technologically advanced State to pierce through the "fog of war"[404] and foresee all of the resulting harms before using interference as a means and method of warfare. To do so would require technical precision, verification and thorough consideration of second and third order effects; not to do so could taint the use interference with illegality thereby violating IHL. If intentional interference cannot distinguish legitimate from illegitimate targets, there may be an obligation to either forego the attack or use some other weapon with an ability to satisfy the discrimination requirement. Thus, while satellite signal interference may sometimes be an illegal means and method of warfare because it may not be able to adhere to the principle of discrimination, it may at other times be the only legal option.

3. The Principle of Proportionality

The principle of proportionality limits attack effects by requiring belligerents to establish a balance between military and humanitarian interests.[405] Proportionality prohibits States from carrying out attacks when loss of life, injury to civilians, damage to civilian objects or a combination thereof would be excessive in relation to the military advantage anticipated.[406] Proportionality requires a balancing of anticipated military advantage against anticipated damage caused.[407] Proportionality also requires military commanders to "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects," "take all feasible precautions" necessary to avoid or minimize incidental loss or damage and, when

404. The "fog of war" refers to the uncertainty in situational awareness that arises during war. CARL VON CLAUSEWITZ, ON WAR 20 (Michael Howard & Peter Paret eds. & trans., Princeton University Press 1976) (1832).

405. Bourbonniére, *Law of Armed Conflict*, *supra* note 187, at 47.

406. API*, supra* note 374, art. 51(5)(b).

407. *Id.*, art. 57(2). Robert A. Ramey, *Space Warfare and the Future Law of War* 58 (1999) (unpublished LL.M. thesis, McGill University Institute of Air and Space Law).

possible, choose objectives that will "cause the least danger to civilians."[408] This means if intentional interference with commercial communication satellites were reasonably expected to cause superfluous injury or unnecessary suffering, it would be prohibited under the principle of proportionality.[409] Even the ICJ noted uncertainty with respect to the type of weapons that could be used lawfully. Specifically, in the *Nuclear Weapons* advisory opinion the ICJ stated even though the threat or use of nuclear weapons should comply with IHL, to do so does not in all circumstances constitute a violation of international law.[410]

As can be seen, the nature of dual-use commercial communication satellites and the use of satellite signal interference in warfare significantly complicates the application and consideration of IHL principles. One of the most discussed examples of targeting dual-use objects in warfare is the bombing of the Iraqi power grid during the 1990–91 Gulf War. As noted by Professor Yoram Dinstein,

> Since the electrical grid in Iraq was totally integrated, attacks against it—and its installations—resulted not only in a tremendous military advantage (shutting down radar stations, military computers, etc.), but also extensive damage to civilians: hospitals stopped operating, water pumping and filtering facilities came to a standstill, etc. From a legal point of view, a "dual use" of Iraq's electrical grid did not alter its singular and unequivocal status as a military objective. There was, as usual with military objectives, the question of proportionality where collateral damage is concerned. But the extensive damage to civilians was not excessive in relation to the military advantage anticipated.[411]

The bombing of the Iraqi electrical grid clearly suggests commercial communication satellites will be targeted in future conflicts in lieu of kinetic attacks and that civilians will face consequences in the future as military and civilian systems become increasingly interconnected and as civilian objects become progressively dual-use. However, whereas the military objective in Iraq was accomplished through the kinetic bombing and physical destruction of the power grid, the future of warfare involving satellite sig-

---

408. API*, supra* note 374, art. 57(2).

409. *Id.,* arts. 35(1)–35(2), 85.

410. *See Nuclear Weapons, supra* note 375, ¶ 42; *see also* Freeland, *supra* note 371, at 281.

411. Yoram Dinstein, *Discussion*, *in* LEGAL AND ETHICAL LESSONS OF NATO'S KOSOVO CAMPAIGN, *supra* note 385, at 211, 219.

nal interference could cause less permanent damage and destruction. Thus, even though IHL clearly permits targeting commercial communication satellite and their supporting systems in armed conflict, when they are targeted, IHL may be able to ensure civilians are protected because IHL requires belligerents to consider the use of less destructive means to accomplish military objectives.

Assessing the potential direct and indirect damage to civilians and civilian objects will likely prove difficult as States consider targeting commercial communication satellites by engaging in satellite signal interference. States may also have difficulty balancing civilian damage, loss of life and injuries against anticipated "concrete and direct military advantage." The key to limiting unintended collateral effects will be the sophistication of the entity employing satellite signal interference, the technical ability to effectively limit intended effects to carefully vetted targets and due diligence in appropriately considering and applying the principles of IHL. How this will play out in future armed conflicts remains to be seen.

IV. SATELLITE SIGNAL INTERFERENCE UNDER THE UN CHARTER

As dependency on satellite technologies and communications increases globally, State and non-State actors are becoming increasingly vulnerable to the consequences of disrupted transmissions. This emerging phenomenon reveals existing norms are unable to address the growing problem of interference. Thus, as satellite signal interference becomes more prevalent and collateral consequences become more severe, States will need to know how to characterize such acts and under what circumstances self-defense is justified. With this understanding, this Section addresses the implications of satellite signal interference under the normative framework of the UN Charter and focuses on circumstances under which satellite signal interference can be characterized as an "armed attack" under Article 51 triggering the right of self-defense.

A. The Prohibition of the Threat or Use of Force

The UN Charter and its focus on peace is the result of the international community's desire "to save succeeding generations from the scourge of war, which twice in [their] lifetime [had] brought untold sorrow to man-

kind."[412] Despite its imperative for preserving international peace and security, the UN Charter does not ban all use of force. Rather, it outlaws aggressive use of force, and establishes the general principle that armed conflict is neither proper nor inevitable, irrespective of the political purposes or merits. To that end, the UN Charter restates customary norms related to the behavior of States with respect to the threat or use of force[413] and reaffirms the duty of States to resolve all international disputes through "peaceful means in such a manner that international peace and security . . . are not endangered."[414]

The principle prohibiting the "threat or use of force" by States is considered *jus cogens*[415] and is an obligation *erga omnes*.[416] The ICJ has opined that the principle is also binding on all States as a customary norm.[417] The prohibition against the "use of force," the scope of which remains hotly contested,[418] is also codified in Article 2(4) of the Charter. Article 2(4) is the key prescription in international law regarding the use of force.[419]

Article 2(4), described as "the cornerstone of peace"[420] and as "the heart of the United Nations Charter"[421] states: "All 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."[422]

This prohibition is complemented by the customary norm of non-intervention, which, as addressed above, dictates States must not directly or

---

412. U.N. Charter pmbl.

413. IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE 112–13 (1963). [hereinafter BROWNLIE, USE OF FORCE].

414. U.N. Charter art. 2(3).

415. *Jus cogens* is the legal term given to norms of general international law from which no derogation is allowed under any circumstances. IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 489 (6th ed. 2003).

416. *Erga omnes* obligations are owed to the international community as a whole. Barcelona Traction, Light and Power Co. (Belg. v. Spain), 1970 I.C.J. 3, 32 (Feb. 5).

417. *Nicaragua, supra* note 361, ¶ 190.

418. Maogoto & Freeland, *supra* note 54, at 1105.

419. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 900 (1999) [hereinafter Schmitt*, Computer Network Attack*].

420. CLAUD H.M. WALDOCK, THE REGULATION OF THE USE OF FORCE BY INDIVIDUAL STATES IN INTERNATIONAL LAW 492 (1952).

421. Louis Henkin, *The Reports of the Death of Article 2(4) are Greatly Exaggerated*, 65 AMERICAN JOURNAL OF INTERNATIONAL LAW 544 (1971).

422. U.N. Charter art. 2(4).

indirectly interfere with the internal affairs of other States.[423] When intervention takes the form of a use or threat of force, it breaches not only the norm of non-intervention, but also Article 2(4).[424]

Despite intense debate over the scope of Article 2(4), the prevailing view is that Article 2(4) is limited to the use of *armed* force and does not include economic or political coercion.[425] Some States, however, may be starting to favor a more expansive interpretation of Article 2(4) to include coercive activities, such as computer network attacks.[426] While such an expansion may emerge through State practice, the prevailing view is that Article 2(4) applies to any use of force not otherwise permitted by the terms of the Charter.[427]

Article 2(4) sets the threshold for when a "threat or use of force" breaches international law. That threshold, however, is subject to two exceptions: (1) actions and measures specifically authorized by the UN Security Council[428] and (2) actions taken in self-defense in response to an "armed attack."[429] Therefore, any use of force falling outside of these two exceptions would violate Article 2(4), whereas measures falling short of a use of force would not. Before addressing the two exceptions to Article 2(4), which will take place in Section V, the prohibition on the use of force must be clarified.

---

423. Manila Declaration on the Peaceful Settlement of International Disputes, G.A. Res. 37/10, U.N. Doc. A/RES/37/10 (1982); Declaration on Friendly Relations, *supra* note 360.

424. *Nicaragua, supra* note 361, ¶ 209.

425. THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 117–18 (Bruno Simma ed., 2d ed. 2002) [hereinafter CHARTER OF THE UNITED NATIONS].

426. WALTER G. SHARP, CYBER SPACE AND THE USE OF FORCE 130–33 (1999) (arguing that United States national policies indicate a wide range of cyber activities should fall within the prohibition of Article 2(4)).

427. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in* NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 151, 153 (2010) [hereinafter Schmitt, *Cyber Operations*].

428. U.N. Charter ch. 7.

429. *Id.*, art. 51.

1. Defining the Use of Force

Article 2(4) renders only specific uses of force wrongful.[430] While the notion of force is disputed,[431] some suggest the proper view is that "force" denotes "*armed force*,"[432] meaning a "resort to a violent weapon that inflicts human injury."[433] Consistent with this view, armed force also includes all activities related to military action, ranging from the transfer of soldiers and tanks to country borders to acts of war, including dropping bombs and firing artillery.[434] Even the Charter *travaux preparatoires* and the Declaration on Principles of International Law, Friendly Relations and Co-Operation among States support the view that only military force is the focus of the Article 2(4) prohibition on the use of force.[435]

Ultimately, international law perceives the unlawful recourse to the unlawful use of force as an act of "aggression."[436] While there is no legally binding definition of "aggression," UN General Assembly Resolution 3314 articulates specific acts which the international community believes to be "aggression" and thus illegitimate uses of force. Entitled, UN Resolution on the Definition of Aggression, Resolution 3314, which as a General Assembly resolution is non-binding, defines aggression as "the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the UN, as set out in this definition."[437] Article 3 of the Resolution presents a non-exhaustive list of conduct amounting to acts constituting aggression, all of which require the use of "armed force," such as inva-

430. Schmitt*, Computer Network Attack*, *supra* note 419, at 900.

431. *Id.* at 904; CHARTER OF THE UNITED NATIONS, *supra* note 425, at 117.

432. BROWNLIE, USE OF FORCE*, supra* note 413, at 362; YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 86 (4th ed. 2005) [hereinafter DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE]; Schmitt, *Computer Network Attack*, *supra* note 419, at 904 (emphasis added).

433. Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUROPEAN JOURNAL OF INTERNATIONAL LAW 825, 845 (2001).

434. Isavella M. Vasilogeorgi, *Military Uses of Outer Space: Legal Limitations, Contemporary Perspectives Laws* 17 (2011) (unpublished LL.M. thesis, McGill University Institute of Air and Space Law).

435. CHARTER OF THE UNITED NATIONS, *supra* note 425, at 118; Declaration on Friendly Relations*, supra* note 360.

436. Bourbonniére, *Clausewitz Nebulae*, *supra* note 285, at 245.

437. Definition of Aggression*, supra* note 338, art. 1.

sions, bombardments and naval blockades.[438] Under Article 4, however, Resolution 3314 does not limit acts of aggression to those only coming from uses of *armed* force.[439]

The use of indirect armed force, referring to the participation of one State in the use of force by another State, also falls within the ambit of Article 2(4) of the UN Charter.[440] This includes one State allowing its territory to be used for violent acts against a third State, as well as providing assistance to anti-government forces such as was found in the *Nicaragua* case.[441] In that case, the International Court of Justice (ICJ) drew somewhat of a line as to what constituted a wrongful use of force. It stated:

> [W]hile arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all assistance given by the United States Government. In particular . . . the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua . . . does not itself amount to a use of force.[442]

Even though the ICJ did little to clarify the scope of the prohibition on the use of force regarding assisting subversive activities,[443] the Court established the use of force includes actively and directly preparing and assisting others to apply armed force.[444]

2. Defining Armed Attacks

The term "armed attack" is not only linguistically different than other similar terms within the UN Charter, it has also been interpreted more narrowly.[445] In *Nicaragua,* the ICJ held to qualify as an armed attack sufficient to trigger a response under Article 51, attacks must constitute the "most grave

438. *Id.*, art. 3.

439. Noah Weisbord, *Conceptualizing Aggression*, 20 DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW 1, 37 (2009).

440. CHARTER OF THE UNITED NATIONS, *supra* note 425, at 119.

441. *Id.* at 119–20.

442. *Nicaragua*, *supra* note 361, ¶ 119.

443. CHARTER OF THE UNITED NATIONS, *supra* note 425, at 121.

444. Schmitt*, Computer Network Attack*, *supra* note 419, at 909.

445. Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 100–101 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies) [hereinafter Dinstein, *CNAs and Self-Defense*].

forms of the use of force."[446] Thus, there may be acts that violate the prohibition on the use or threat of force, but they may not rise to the level of an armed attack as they are not "most grave." For example, the ICJ held where a cross-border incursion is minor in "scale and effects," it is merely a "frontier incident" and not an "armed attack."[447] According to Professor Michael Schmitt, the phrase "scale and effects" is simple shorthand for the quantitative and qualitative factors considered when determining whether a certain action qualifies as a use of force.[448]

The ICJ noted the need to distinguish the most grave forms of the use of force (those which constitute an armed attack for purposes of Article 51) from those that are less grave.[449] It offered modest guidance in doing so, suggesting that it is the "scale and effects" of the consequences that differentiate acts qualifying as an "armed attack" from those that do not.[450] In 2003, the ICJ revisited *Nicaragua* in the *Oil Platforms* case and invoked *Nicaragua's* threshold test in order to characterize "the most grave forms of the use of force."[451] Beyond confirming the threshold test in *Nicaragua,* however, the Court did nothing to clarify the most grave forms of force from those less grave.[452] Accordingly, beyond the requirement that a use of force must be "grave," the parameters of the scale and effects criteria remain unsettled.[453]

Against this backdrop, the question at hand is thus: could a non-kinetic weapon such as satellite signal interference ever constitute a use of force or an armed attack? Fortunately, this point was previously addressed by the ICJ in the *Nuclear Weapons* advisory opinion*,* which held, "any use of force, regardless of weapons employed" is governed by the UN Charter.[454] In other words, the issue is not the type of weapon employed, but rather whether such use could constitute a use of force or an armed attack. Thus, just as non-kinetic chemical, biological, and radiological attacks are assessed

---

446. *Nicaragua*, *supra* note 361, ¶ 191.

447. *Id.,* ¶ 195.

448. Schmitt*, Computer Network Attack, supra* note 419, at 915.

449. *Nicaragua, supra* note 361, ¶ 191.

450. *Id.*, ¶ 195.

451. *Id.*, ¶ 191.

452. Andrew Garwood-Gowers, Case Note, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States): Did the ICJ Miss the Boat on the Law on the Use of Force?*, 5 MELBOURNE JOURNAL OF INTERNATIONAL LAW 241, 249–51 (2004).

453. TALLINN MANUAL, *supra* note 364, at 55.

454. *Nuclear Weapons*, *supra* note 375, ¶ 39.

under the use of force or armed attack threshold, so too should satellite signal interference.

Despite some ambiguity surrounding the scope of use of force or where the threshold lies for an act to rise to the level of an armed attack, several conclusions can easily be made. First, not all uses of force rise to the level of an armed attack. Second, any act rising to the level of an armed attack is also a use of force. Third, uses of force need not involve a State's direct use of armed forces. Fourth, it is the scale and effects and consequences of the act that matter,[455] more than whether the act is, in fact, armed, direct, indirect, kinetic or even non-kinetic.

Applying the parameters outlined above to satellite signal interference, one can make several observations. First, non-destructive activities such as spoofing a signal and broadcasting signals or messages intended to merely undermine confidence in a State's government or its economy would likely never qualify as a prohibited use of force. Second, neither funding a group conducting interference as part of an uprising nor providing an organized group with the training and equipment necessary to carry out satellite signal interference qualifies as an unlawful use of force, even though it may violate the customary norm of non-interference or the ITU regime. Third, satellite signal interference resulting in physical harm to people or damage to tangible property may equate to an unlawful use of force.[456]

Even though satellite signal interference may be unlawful under the ITU and ISL frameworks, that alone does not indicate the interference will constitute a use of force. Satellite signal interference may only violate the ITU and/or ISL, or it may constitute a violation on the prohibition against unlawful intervention. In such cases, a States' response is limited to only those permissible under the relevant ITU, ISL or non-intervention frameworks. Responses to such acts will be addressed in Section V.

B. Satellite Signal Interference as an Armed Attack

Because satellite signal interference does not resemble armed attacks traditionally regulated under the law of war framework, can existing norms be applied and adapted to cope with this emerging phenomenon? The answer rests within the scholarly debates and the body of law currently developing with regard to information operations, namely CNAs.

---

455. BROWNLIE, USE OF FORCE*, supra* note 413, at 362.

456. Schmitt, *Cyber Operations*, *supra* note 427, at 154; Joyner & Lotrionte, *supra* note 433, at 845.

1. Current Debates over the Application of the Jus ad Bellum

In academic debates over the characterization of CNAs as a use of force, three different views have emerged: an instrument-based approach, a target-based approach and an effects-based approach.[457] This author asserts the effects-based approach, which scrutinizes the consequences caused by an act, is the most practical and appropriate framework to apply to CNAs and to satellite signal interference.

Professor Duncan Hollis argues that, under an instrument-based approach, an operation such as CNA does not "qualify as armed force because it lacks the physical characteristics traditionally associated with military coercion."[458] Under his analysis, satellite signal interference would almost never qualify as a use of force despite its potential to cause crippling effects because the interference does not involve the use of traditional military weapons.[459] The instrument-based approach "seeks to regulate the conflicts of yesterday"[460] that were conducted in environments devoid of modern infrastructure, targets, weapons and capabilities, and is thus wholly inadequate in the modern world.[461]

With a target-based approach, acts are characterized as a use of force or an armed attack whenever they "penetrate 'critical national infrastructure' systems," even without "significant destruction or casualties."[462] According to Hollis, the target-based approach focuses on determining when a State may respond in self-defense.[463] Under this approach, the mere identity of a target can authorize forceful self-defense.[464] In the context of satellite signal interference, even a slight intrusion into, or disruption of, a critical system could then be argued to justify an armed military response. The target-based approach expands the right of self-defense significantly, and, in do-

457. Oona A. Hathaway et al., *The Law of Cyber Attack*, 100 CALIFORNIA LAW REVIEW 817, 845 (2012).

458. Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK LAW REVIEW 1023, 1041 (2007).

459. Kanuck, *supra* note 55, at 288–89.

460. *Id.* at 290.

461. Hollis, *supra* note 458, at 1041–42.

462. *Id.* at 1041.

463. *Id.*

464. *Id.*

ing so, could threaten international peace and security by making armed conflict more likely.[465]

The effects-based approach, the most compelling and widely accepted of the three, focuses on the consequences or effects of the act.[466] This approach assesses whether the act in question causes effects equivalent to those produced by military force (damage to property or death).[467] The effects-based approach also assumes States want to preserve their ability to take a wide range of action, as well as avoid the harmful consequences caused by others.[468]

The most well-known proponent of the effects-based approach is Professor Schmitt who states the effects and consequences of a CNA should be assessed according to seven factors to determine whether the CNA constitutes a use of force.[469] These factors, deriving from that which historically made military force special in international law,[470] include: (1) severity: scale, scope and duration of the harm or damage; (2) immediacy: how quickly the consequences manifest after the act; (3) directness: how directly tied the consequences are to the act; (4) measurability: the extent to which damage can be identified and quantified; (5) invasiveness: the extent to which the act penetrated or intruded into a targeted system; (6) presumptive legitimacy: determining whether the act is unlawful; and (7) responsibility: the extent to which a State is involved in an act.[471]

These factors have also been formally recognized by an International Group of Experts[472] in the *Tallinn Manual on the International Law Applicable to Cyber Warfare* as that which States will likely consider when characterizing

---

465. Hathaway et al., *supra* note 457, at 847.

466. *Id.*

467. Hollis, *supra* note 458, at 1041.

468. Schmitt, *Cyber Operations*, *supra* note 427, at 155.

469. Michael N. Schmitt, *The 'Use of Force' in Cyberspace: A Reply to Dr. Ziolkowski*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 311, 314 (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., 2012).

470. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 432 (2011).

471. Schmitt, *Computer Network Attack*, *supra* note 419, at 914–15; Schmitt, *Cyber Operations*, *supra* note 427, at 155–56.

472. At the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, the International Group of Experts was asked to produce a manual on the law governing cyber warfare. The Group of Experts included legal practitioners, academics and technical experts, each one specifically selected to ensure the Manual was legally sound, practically grounded and addressed key issues raised by actual or possible cyber operations. TALLINN MANUAL, *supra* note 364, at 1, 9.

whether a non-kinetic act (CNA) is a use of force.[473] The *Tallinn Manual*, released in October 2012, adopted the seven factors described above and added a final factor, military character. The specifics of the eight factors are more fully described below:

> Severity of the Damage: If physical harm is caused to people or property, the act will likely qualify as a use of force. If death does not result or if the damage is *de minimis*, it is less likely that the act will be viewed as a use of force. Acts resulting in nothing more than mere inconvenience, irritation or annoyance will never amount to a use of force.
>
> Immediacy of the Consequences: The sooner the effects of an act are seen (such as when a bomb explodes), the greater likelihood there is that a State will view such act as a use of force. If consequences are delayed or occur slowly over a long period of time, it is more likely that a State would view the act not as a use of force but as one to be dealt with via diplomacy.
>
> Directness: The more closely tied the consequences are to the act itself, the more likely it is that States will consider that act to be in violation of the prohibition on the use of force.
>
> Invasiveness: The more invasive an act is into the targeted State, the more likely it is that a State will consider it to be a use of force. In other words, the more protected a system is from an intrusion, the greater the concern is as to its penetration.
>
> Measurability of the Damage: If the consequences and effects of the act are identifiable and quantifiable, the easier it is for a State to assess whether the act rises to the level of a use of force.
>
> Presumptive Legitimacy: If an act is presumptively legal, that is, it is not specifically prohibited, the less likely it is that a State will consider that act to be a use of force.

473. *Id.* at 48.

> Military Character: If the act is employed by a State's military, the greater likelihood there is that the act will be characterized as a use of force.
>
> State Involvement: The clearer it is that a State is responsible for or involved with an act, the greater the likelihood is that such act will be characterized as a use of force.[474]

These eight factors provide States significant latitude in characterizing acts as a use of force, which could favor a finding of a use of force.[475] These factors also allow States to balance conflicting objectives of avoiding the harmful consequences caused by the actions of other States, while maintaining the ability to take a wide variety of actions in peacetime and war.

In applying these factors, States measure the consequences of the act in question, as well as the perpetrator's identity, to determine whether the act is outside the use of force boundary or is similar to the consequences most often resulting from armed force.[476] If the assessment reveals the consequences at issue fall outside the use of force boundary, then the act can never rise to the level of a use of force or an armed attack. On the other hand, if the assessment reveals the consequences resemble those resulting from armed force, then the use of force prohibition would apply.[477]

Admittedly, these factors were never set forth as a tool for assessing satellite signal interference, nor are they legally prescriptive. In fact, these factors are considerations in a political determination or decision rather than a legal one. Nonetheless, because there is no specific or conclusive definitional threshold for determining uses of force, nor is there any normative framework available for assessing satellite signal interference, this approach and these eight factors provide a persuasive means to assess interference in the context of international law. What is more, considering States are usually most concerned with the effects and consequences of actions, rather than weapons employed, the effects-based approach more appropriately assesses and addresses emerging intangible modern technologies and warfare. Finally, while satellite signal interference has never been publically declared to be an unlawful use of force or an armed attack by any

474. *Id.* at 48–51; *see also* HARRISON DINNISS, *supra* note 389, at 63–64.
475. Schmitt, *Cyber Operations*, *supra* note 427, at 157.
476. Schmitt*, Computer Network Attack*, *supra* note 419, at 915.
477. *Id.*

State, it is likely when or if it is, it will be assessed by the resulting consequences and effects.

2. Assessing Satellite Signal Interference under the Effects-Based Approach

With the effects-based approach in mind, we can assess several examples of satellite signal interference and determine where, if at all, they should lie in the use of force spectrum. At one end of the spectrum, satellite signal interference is mere annoyance or inconvenience, and temporarily denies or disrupts satellite communications. The severity is minimal, the duration is short, there is no physical damage and the ability to measure the scope and degree of consequences is neither definitive nor quantifiable. Such a scenario clearly falls outside the scale and effects of those typical of an armed force and thus falls outside the ambit of Article 2(4).

Now consider a situation where satellite signals directing commercial airliners are disrupted and two planes collide and crash within a heavily populated city. The death toll and property losses would be severe, just as if the planes had been hit by a missile. Assuming signals were protected by way of uplink and downlink encryptions, the act is arguably quite invasive. The damage and harm are clearly measurable in lives and property loss. Without question, this act constitutes a use of force and undoubtedly satisfies the requisite threshold of severity and gravity to qualify as an armed attack.

Similarly, if TT&C signals of a satellite are intentionally jammed and the satellite collides with other satellites in orbit, the act would likely be characterized as severe and also directly tied to jamming. The jamming resulted in substantial economic loss of the satellites, created a cloud of debris endangering other objects in space and violated the ITU and ISL frameworks. In this case, the act would likely qualify as a use of force and be of sufficient gravity to be considered an armed attack.

A more difficult case, however, is satellite signal interference causing massive disruptions within a State's critical infrastructure, but which results in no physical damage or human harm. This author asserts because most definitions of critical infrastructure include services such as security, water and food, transportation, finance, health, energy, and governmental and

public services,[478] such an act could constitute a use of force if it led to significant or long-term disruptions of a State's critical infrastructure and impacted a State's ability to provide essential services to its citizens. In fact, as a Russian official once stated, "[a]n attack against the telecommunications and electronic power industries of the United States would, by virtue of its catastrophic consequences, completely overlap with the use of weapons of mass destruction."[479] If true, such an attack might surpass the quantitative criterion of an armed attack. Thus, while loss of satellite television coverage of the National Football League's Super Bowl might seem catastrophic to football fans and result in financial losses for satellite providers and advertisers, it would likely never rise to the level of an armed attack. However, if the disruption led to food contamination, fatal transportation sector accidents, financial market collapse and nuclear reactor meltdowns, or prevented essential governmental functioning or access to public utilities such as water or emergency services, the act might very well be characterized as an armed attack. As can be seen, there is no clear bright line. The determining factor remains the severity of consequences.

No doubt, some acts of interference may more easily be considered a use of force, whereas others clearly would not. Additionally, given the requisite threshold required for armed attacks, intentional interference will only in exceptional cases trigger the right of self-defense. Considering current State practice, States seem unwilling to draw too much attention to interference incidents for what could be a number of reasons. Perhaps this is because States want to retain the ability to engage in such acts or because they wish to avoid an unnecessary escalation of tensions with States from which interference is sourced. Regardless, if one State characterizes an act of intentional interference as a use of force or as an armed attack, it will have to be prepared to accept a consistent characterization in comparable cases where a similar action is taken by that State against another State.

In the event of doubt as to whether interference rises to the level of a use of force, States would be cautious before characterizing such incidents as an armed attack. If not so characterized, a State might not be entitled to assert a right of armed self-defense under Article 51 of the Charter. In such circumstances, the State, to comply with the letter and intent of international law, would have to pursue resolution of the matter diplomatically through the ITU framework, engage in non-use of force countermeasures

478. Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 12 JOURNAL OF CONFLICT & SECURITY LAW 229, 231 (2012).

479. Joyner & Lotrionte, *supra* note 433, at 865.

or take the matter before the Security Council to determine if a "threat to the peace" occurred under Article 39 of the UN Charter. The State would also be able to make a diplomatic claim with the other State on the basis of a breach of international obligation.

C. Interference Conducted by Non-State Actors

Neither UN Charter Article 2(4) nor its customary norm equivalent apply to the acts of non-State actors, including individuals, organized groups, terrorist organizations and the like, unless attributable to a State pursuant to the rules set out within the Articles on Responsibility of States for Internationally Wrongful Acts.[480] This means, while intentional interference conducted by non-State actors may be unlawful under domestic law or international legal frameworks, by itself it is not a violation of the prohibition on the use of force. As noted in Section III, member States are obligated to comply with ITU provisions and cooperate with others in eliminating harmful interference.[481] Additionally, under ISL, States bear international responsibility for national activities in outer space.[482]

Since the ITU and ISL frameworks do little to enforce protections against acts of intentional interference, a question emerges: what can States do when acts amount to an armed attack and trigger the State's right of self-defense? In answering this question, it is important to locate the source of the attack and determine whether the act is attributable to a State. Despite the provisions of Article VI of the Outer Space Treaty under which all acts can always be attributed to States, the difficulty is establishing a sufficient link between the State and the non-State entity or actor committing the unlawful act.[483]

With regard to attributing an act to a State, "the problem is not . . . the legal process of imputing the act to a particular State . . . but the prior process of tracing material proof of the identity of the perpetrator."[484] Thus, even though satellite signal interference can be detected by using antennas to co-locate the source of the jamming signal, it may be challenging to pinpoint the precise source of the interference in a timely manner. What is

480. TALLINN MANUAL, *supra* note 364, at 43–44.

481. *See* ITU Radio Regulations, *supra* note 190, arts. 11.42, 11.42A, 15.21 §13; *see also* Jakhu, *Satellites*, *supra* note 4.

482. Outer Space Treaty*, supra* note 271, art. VI.

483. MALCOLM N. SHAW, INTERNATIONAL LAW 701 (5th ed. 2003).

484. *Nicaragua, supra* note 361, ¶¶ 119–20.

more, even if the location of the interference is discovered, it may still be difficult and time-consuming to identify the person who operated the jamming equipment or to "identify the real 'mastermind' behind the attack."[485]

The problem of attribution is not limited to acts of intentional interference; it is one of the biggest difficulties associated with CNAs.[486] Such a challenge also extends to conventional attacks carried out anonymously or by groups such as terrorist organizations claiming responsibility when it appears that such a group was incapable or did not have the resources to carry out such an attack.[487] There are also issues of attribution with State-sponsored terrorism activities when the State fails to take responsibility for its role.[488] Nevertheless, in every case, a victim State must establish attribution to a State.

While this article will not address this issue at greater length, there is a fair amount of disagreement on the issue of attribution regarding conventional attacks, as well as with CNAs.[489] Despite this disagreement, a State may not knowingly allow "its territory to be used for acts contrary to the rights of other states,"[490] nor can its territory be used for military acts against another State.[491] Additionally, a State must not knowingly allow armed bands or terrorists to use its territory as a sanctuary from which it levies attacks against military targets or civilian objects within another country.[492]

In the *Armed Activities* case, however, even though the ICJ recognized toleration by a State of non-State actors who subsequently carried out an attack on another State could trigger a right of self-defense, it nonetheless failed to find such a right in that case.[493] In the *Oil Platforms* case, however,

---

485. Tsagourias, *supra* note 478, at 233.

486. HARRISON DINNISS, *supra* note 389, at 99–100.

487. *Id.* at 100.

488. *Id.*

489. *Id.* at 101.

490. *Corfu Channel, supra* note 295, at 22.

491. The Alabama Claims (United States v. Great Britain) [1872], *reprinted in* 1 JOHN BASSETT MOORE, HISTORY AND DIGEST OF INTERNATIONAL ARBITRATIONS TO WHICH THE UNITED STATES HAS BEEN A PARTY 495 (1898).

492. Ian Brownlie, *International Law and the Activities of Armed Bands*, 7 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 712, 734 (1958), cited in HARRISON DINNISS, *supra* note 389, at 101.

493. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 301 (Dec. 19).

the ICJ effectively held the burden of proof rests on the State invoking the right of self-defense.[494] In the *Corfu Channel* case, the ICJ noted the difficulty of obtaining evidence of a perpetrator when the territory at issue is under the exclusive control of another State and allowed for "a more liberal recourse to inferences of fact and circumstantial evidence."[495] The Court endorsed circumstantial evidence as sufficient, as long as the proof derived from inferences of fact and those facts did not leave room for reasonable doubt.[496] Thus, "a State should not resort to self-defense on the basis of casual evidence or wild political inferences."[497]

Assuming there is sufficient evidence to implicate a State in an unlawful act, a victim State may only take action against another State if the act is attributable under international law. The general rule is the only acts attributable to a State are those conducted by persons acting under the direction of the State.[498] This would include all individuals or collective entities, making up the organization of the State and acting on its behalf,[499] such as the military or any other State entity.

A State, however, may only take action against another State in self-defense if attribution standards are also met[500] or with the agreement of the UN Security Council. Attacks can also be attributed to a State if they are conducted by State organs,[501] controlled by the State,[502] or due to the State's intentional failure to prevent the attack.[503] If the attack cannot be attributed to the State, the non-State actor committing the attack can become the direct target of the self-defense action.[504] In the *Nicaragua* case, the ICJ attributed acts committed by organs of the United States to the United States, but also noted there was insufficient evidence the United States had actual control "in all fields [activities] as to justify treating the *contras* as act-

494. Oil Platforms (Iran v. U. S.), 2003 I.C.J. 161, ¶¶ 57, 61 (Nov. 6).

495. *Corfu Channel, supra* note 295, at 18.

496. *Id.*

497. Tsagourias, *supra* note 478, at 235.

498. THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY, INTRODUCTION, TEXT AND COMMENTARIES 81–85 (James Crawford ed., 2001) [hereinafter STATE RESPONSIBILITY COMMENTARIES].

499. *Id.*

500. Tsagourias, *supra* note 478, at 236.

501. State Responsibility, *supra* note 263, art. 4.

502. *Id.,* art. 8.

503. Tsagourias, *supra* note 478, at 236.

504. *Id.*

ing on its behalf."[505] The ICJ also noted, even though some activities conducted by the *contras* forces were highly dependent on the United States, they nonetheless did not constitute de facto control by the United States. [506] The ICJ reached a similar conclusion in the Bosnia *Genocide* case.[507]

Additionally, in the *Tehran* hostage's case, the ICJ held to attribute the occupation of the U.S. Embassy by militants to the State of Iran, the United States had to establish the militants acted on behalf of the State or were directed by an organ of the State to carry out a specific operation.[508] Without launching into the intricacies of these decisions, for attacks to be attributed to a State under international law, the State had to have issued specific instructions or directed or controlled the operation.[509] Then, in the *Tadić* case, the International Criminal Tribunal for the former Yugoslavia went further, noting it is enough the State authorities exercised "overall control" over an organized and hierarchical structured group without a need for specific control or direction over individual conduct.[510] Additionally, in the *Tadić* Appeals Chamber Judgment, it was noted that courts have not considered overall control or general control to be sufficient with respect to individuals or groups not organized into military structures.[511] In a subsequent decision, the ICJ distinguished the overall control test from that conducted for the purpose of establishing State responsibility.[512]

Applying this understanding to satellite signal interference, an attack carried out by non-State actors may be attributed to a State only if the act was carried out by an organ of the State; by those acting under its direction, instructions, control or direct influence prior to the act; or by non-State actors tolerated by a State.[513] If the interference attack cannot be attributed to a State, but is carried out by a non-State actor, the non-State actor can

505. *Nicaragua, supra* note 361, ¶ 109.

506. *Id.,* ¶ 111.

507. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montengro.), 2007 I.C.J. 43, ¶¶ 399–401 (Feb. 26) [hereinafter *Crime of Genocide*].

508. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran) 1980 I.C.J. 3, ¶ 58 (May 24).

509. State Responsibility, *supra* note 263, art. 8.

510. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 120 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999).

511. *Id.*, ¶ 132.

512. *Crime of Genocide*, *supra* note 507, ¶¶ 403–5.

513. Tsagourias, *supra* note 478, at 244; STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 81–85.

become the target of the victim State's self-defense action.[514] Nevertheless, all responses to attacks, whether individual or collective, warrant only those measures both "proportional to the armed attack and necessary to respond to it."[515]

V. LAWFUL RESPONSES TO SATELLITE SIGNAL INTERFERENCE

Having discussed satellite signal interference as an unlawful act under the ITU and ISL frameworks, as an unlawful intervention, as a prohibited use of force under Article 2(4) of the UN Charter and as an armed attack under Article 51 of the Charter, this Section looks to the spectrum of permissible parameters of lawful responses to such acts. It briefly discusses some of the remedies and responses available to States under international law when unlawful satellite signal interference falls outside the scope of the Charter. Finally, this Section addresses responses available to States under the Charter framework, namely actions and measures authorized by the Security Council and forcible actions taken in self-defense in response to armed attacks.

A. Remedies for Internationally Wrongful Acts under State Responsibility

In any case of State responsibility for an internationally unlawful act, victim States are entitled to reparations as set forth in the Articles on Responsibility of States for Internationally Wrongful Acts.[516] Reparations can take the form of restitution, compensation or satisfaction, either singly or in combination.[517] With respect to satellite signal interference, if no material harm is caused, reparations by the injuring State, such as cessation of the interference, may be sufficient to remedy the situation. If a victim State suffers material damage, however, such as physical damage or financial losses, compensation could be claimed by the injured State to wipe out all the consequences of the wrongful act.[518] An injured State may also take responsive measures neither amounting to a use of force nor breaching any existing

514. Tsagourias, *supra* note 478, at 244.

515. *Nicaragua, supra* note 361, ¶¶ 176, 196; *Nuclear Weapons*, *supra* note 375, ¶ 41; *Oil Platforms, supra* note 494, ¶ 74.

516. State Responsibility, *supra* note 263, art. 31.

517. *Id.*, art. 34.

518. STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 211–12.

treaty or customary law obligation,[519] such as stopping or suspending international telecommunications pursuant to Articles 34 and 35 of the ITU Constitution. An injured State could also respond with retorsions,[520] including severing diplomatic relations, imposing trade embargos and closing their borders to the offending State, as well as engaging in countermeasures.

B. Countermeasures

Countermeasures regulate how States may respond to violations of international law, including, but not limited to, those acts not rising to the level of armed attack justifying self-defense. Considered a form of self-help, countermeasures respond to the position of an injured State when due process of law is not yet guaranteed or when the responsible State is not cooperating in a legal process.[521]

Formerly known as reprisals,[522] countermeasures are otherwise wrongful acts not involving the use of force used by States in response to an internationally unlawful act "to procure its cessation and to achieve reparation for the injury."[523] In other words, countermeasures are peaceful measures falling outside the scope of accepted exceptions to Article 2(4) of the UN Charter used to enforce international law.[524] The purpose of countermeasures is to induce a wrongdoing State to comply with its international obligations,[525] not to create new non-rectifiable situations.[526]

According to the ICJ in the *Gabcikovo-Nagymaros* case, specific prerequisites and conditions apply for countermeasures to be justified and lawful.[527] Specifically, countermeasures must be in response to a prior wrongful act taken by another State and must be directed against the State committing the wrongful act.[528] Additionally, the injured State must have called upon

519. Schmitt, *Cyber Operations*, *supra* note 427, at 159.

520. Retorsions are lawful unfriendly acts made in response to violations of international law. STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 281–82.

521. *Id.*

522. SHAW, *supra* note 483, at 708.

523. STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 168–69.

524. ELENA K. PROUKAKI, THE PROBLEM OF ENFORCEMENT IN INTERNATIONAL LAW 68 (2010).

525. STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 284–87.

526. *Id.*

527. Gabcikovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, 55–57 (Sept. 25).

528. *Id.* at 55.

the offending State to make reparation for it.[529] Countermeasures must also be proportionate to the act and reversible.[530] Finally, countermeasures must be terminated as soon as the responsible State complies with its obligations.[531]

Not all otherwise wrongful acts are considered to be valid countermeasures. Acts violating the obligation to refrain from the threat or use of force as embodied in the UN Charter are unlawful, as are acts that violate fundamental human rights.[532] Other unlawful acts include those violating other preemptory norms of international law and those violating humanitarian obligations of a State.[533] Additionally, countermeasures are not to be used as a form of punishment.[534] They are only to be used to vindicate injured States' rights and restore the legal relationship with the responsible State to normalcy.[535]

The international law of countermeasures does not define satellite signal interference as unlawful. The law of countermeasures simply specifies that whenever any State commits an internationally wrongful act, an injured State may respond with a countermeasure.[536] Thus, whenever satellite signal interference is unlawful, a victim State may respond by employing countermeasures.

As previously concluded, satellite signal interference can constitute a breach of international obligations under the ITU and ISL even when not rising to the level of a use of force or an armed attack. Satellite signal interference may also be considered in violation of the customary international law principle of non-intervention[537] as a wrongful interference with State sovereignty. Finally, satellite signal interference may be a breach of a State's obligation "not to knowingly allow its territory to be used for action contrary to the rights of other States."[538] In each of these instances, satellite signal interference qualifies as an internationally unlawful act justifying a

529. *Id.* at 55–57.

530. *Id.*

531. STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 286.

532. State Responsibility, *supra* note 263, art. 50(1)(a–b).

533. *Id.*, art. 50(1)(c–d).

534. STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 281–87.

535. *Id.*

536. State Responsibility, *supra* note 263, art. 49.

537. The non-intervention principle prohibits the use of coercion to impact a State's political, economic and/or social systems in violation of its sovereignty. *Nicaragua, supra* note 361, ¶ 108.

538. *Corfu Channel, supra* note 295, at 22.

State's use of countermeasures, regardless of whether the acts of interference were carried out, facilitated by or not prevented by State officials. This makes countermeasures an especially valuable tool in situations where satellite signal interference is being employed by non-State entities, because an injured State does not have to attribute the act of jamming itself to a State before it can respond with countermeasures. In other words, the initial threshold requirement of an internationally wrongful act by a State may be established if the State where the interference originated failed to prevent the unlawful act despite its duty to do so. Thus, when a State suspects an act can be attributed to another State, but cannot prove it, the injured State can still utilize countermeasures to vindicate its rights.

Once the initial threshold is established, the primary constraints on how countermeasures may be exercised require they be both necessary and proportional.[539] The principle of necessity reflects the corrective function to achieve compliance,[540] as well as the purpose of preserving the rights of the injured State.[541] Necessity also dictates that, before countermeasures are taken, the injured State must call upon the responsible State to cease its wrongful conduct and offer to negotiate a settlement.[542] Additionally, countermeasures must be reversible and may not be taken if the wrongful act has ceased or if the dispute is pending before a court or tribunal.[543] In some situations, however, an injured State "may take such urgent countermeasures as are necessary to preserve its rights"[544] without notifying the wrongdoing State of its intention to do so.[545]

Under the ITU, an urgent countermeasure would be permissible in cases where the offending State has repeatedly failed to stop harmful interference from within its borders or from satellites under its jurisdiction and control. An urgent countermeasure would also likely be permissible if harmful interference caused a blackout in communications or led to a loss of critical State services. In either case, a State may resort to an urgent countermeasure to prevent further harm or injury. This would not only qualify as a reasonable use of an urgent countermeasure, but would also prevent the incident from escalating into a situation, if left unaddressed,

539. STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 294–96.
540. *Id.* at 288–93.
541. *Id.*
542. State Responsibility, *supra* note 263, art. 52(1).
543. *Id.*, art. 52(2).
544. *Id.*
545. STATE RESPONSIBILITY COMMENTARIES, *supra* note 498, at 298–99.

that could ultimately lead to an armed attack and a full blown armed conflict.

Under countermeasures, the principle of proportionality is assessed in quantitative and qualitative terms.[546] Proportionality requires countermeasures be "commensurate with the injury suffered taking into account the gravity of the internationally wrongful act and the rights in question."[547] While countermeasures need not necessarily be reciprocal, countermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or closely related obligation.[548]

In responding to satellite signal interference, a victim State could, but is not required to, employ interference as a reciprocal countermeasure.[549] For example, if satellite jamming disrupts a State's television broadcasting signals, reciprocal countermeasures could be in the form of defensive jamming directed back at the intruding signals or jamming other television broadcasting signals of the offending State.

There is, however, no certainty these reciprocal acts would produce similar and reciprocal effects, because fashioning a countermeasure only injuring the actor that perpetuated the wrongful act may be difficult given the interconnectedness of satellite systems and imprecise nature of applying satellite signal interference. Reciprocal jamming could also have an unintended and unrealized effect by harming those who have nothing to do with the initial unlawful act. This could also result in a situation that spirals out of control and creates a new breach of international law.[550] For example, if a State unlawfully employs a countermeasure, it could incur responsibility for its own wrongful conduct and/or find itself subject to countermeasures or some other more severe responsive measure as well.

Because countermeasures need not be reciprocal, but only necessary and proportional, an injured State could engage in any other countermeasure meeting the requirements of necessity and proportionality. For instance, since intentional interference with satellite signals is a breach of treaty obligations under the ITU, an injured State could respond by suspending performance of its obligations under another treaty or a duty owed under customary international law. An injured State could also employ

546. *Id.* at 294–96.
547. State Responsibility, *supra* note 263, art. 51.
548. STATE RESPONSIBILITY COMMENTARIES*, supra* note 498, at 282–83.
549. *Id.*
550. *Id.* at 286.

countermeasures such as restricting trade or censoring satellite transmissions of the offending State.

Even though the law of countermeasures could be viewed as a limited answer to the problem of satellite signal interference, it nonetheless provides States a means to react quickly to breaches of international law. The law of countermeasures also offers injured States a valuable tool for addressing a wide array of incidents.

C. The International Court of Justice

The International Court of Justice has jurisdiction over all cases referred to it and over all matters specifically provided for in the UN Charter or in treaties in force.[551] The Court also issues advisory opinions to legal questions.[552] These opinions, while not binding per se, are not without legal effect. The Court, a principal organ of the UN, follows the same procedure and rules as relied on in binding cases and the legal reasoning therein reflects the Court's authoritative views on important issues of international law.[553] Moreover, such a decision can prove to be authoritative despite its "advisory" nature. For example, the *Legality of the Threat or Use of Nuclear Weapons* advisory opinion has become an authoritative opinion concerning the legality under international law of the use or the threatened use of nuclear weapons. However, as there is no clause within the ITU and ISL frameworks granting the ICJ compulsory jurisdiction to adjudicate matters arising thereunder, the ICJ may not exercise jurisdiction unless both parties consent.[554] It is therefore unlikely a State engaging in satellite signal interference would ever submit to the ICJ's jurisdiction or that the ICJ would be able to resolve a dispute involving satellite signal interference.

D. Responses under the UN Charter

As previously addressed, under Article 2(4) States are prohibited from using force or threatening to do so in the course of their international rela-

551. Statute of the ICJ, *supra* note 278, art. 36.

552. *Id.*, art. 65.

553. Pieter H.F. Bekker, *The UN General Assembly Requests a World Court Advisory Opinion on Israel's Separation Barrier*, AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS (Dec. 2003), http://www.pchrgaza.org/Library/pieter.htm.

554. Monetary Gold Removed from Rome in 1943 (It. v. Fr., U.K. & U.S.), Preliminary Question, 1954 I.C.J. 19, 32 (June 15).

tions. The only accepted exceptions explicitly permitted by the Charter are measures authorized by the Security Council[555] and actions taken in self-defense.[556]

1. Measures Authorized by the UN Security Council

Pursuant to Article 24 of the Charter, the Security Council has primary responsibility for maintaining international peace and security. While collective measures specifically authorized by the Security Council are set forth in Chapters VI, VII, VIII and XII, only those authorized under Chapter VII (Articles 39–51) fall within the permissible exceptions to the general prohibition on the use or threat of force under Article 2(4).[557] On the legal basis of Chapter VII, the UN Security Council authorized armed action in Korea in 1950,[558] Iraq in 1990,[559] Darfur in 2006,[560] Libya in 2011[561] and Mali in 2012.[562]

However, before the Security Council can adopt any enforcement measure, armed or otherwise, it must, under Article 39 "determine the existence of any threat to the peace, breach of the peace, or act of aggression and make recommendations, or decide what measures shall be taken . . . to maintain or restore international peace and security."[563] The range of incidents the Security Council has determined as giving rise to "threats to the peace" or "a breach to the peace" is extensive, and has involved country-specific situations such as inter-State[564] and intra-State conflicts,[565] terror-

555. U.N. Charter ch. 7.
556. *Id.*, art.. 51.
557. *Id.*, ch. 7.
558. S.C. Res. 83, U.N. Doc. S/1511 (June 27, 1950).
559. S.C. Res. 678, U.N. Doc. S/RES/678 (Nov. 29, 1990).
560. S.C. Res. 1706, U.N. Doc. S/RES/1706 (Aug. 31, 2006).
561. S.C. Res. 1973, U.N. Doc. S/RES/1973 (Mar. 17, 2011).
562. S.C. Res. 2085, U.N. Doc. S/RES/2085 Dec. 20, 2012).
563. U.N. Charter art. 39.
564. By Resolution 1291, in 2000 the Security Council noted its concern over the illegal exploitation of natural resources in the Democratic Republic of the Congo and the potential consequences of those actions on the conflict, and reiterated its prior call for the withdrawal of foreign forces. S.C. Res. 1291, U.N. Doc. S/RES/1291 (Feb. 24, 2000). In 2003, by Resolutions 1497 and 1509, the Security Council determined that the situation in Liberia constituted "a threat to international peace and security," to "stability in West Africa" and "to the peace process for Liberia." S.C. Res. 1497, U.N. Doc. S/RES/1497 (Aug. 1, 2003); S.C. Res. 1509, U.N. Doc. S/RES/1509 (Sept. 19, 2003).

ists' acts,[566] the proliferation of weapons of mass destruction[567] and internal conflicts with a regional dimension.[568]

When Article 39 determinations are made, the Security Council "shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."[569] Security Council decisions made under Article 39 are binding upon UN member States through the combined application of Article 25 and Article 103.

Despite little clarity as to the meaning and scope of the phrase "threats to the peace," other than such threats must be distinguishable from activities constituting threats of the use of force as prohibited under Article 2(4),[570] a breach of the peace is often characterized by hostilities between the armed units of States.[571] However, the Council has also found deliberate targeting of civilian populations, as well as systematic, flagrant and widespread violations of international humanitarian and human rights law, to be threats to international peace and security.[572]

---

565. By Resolution 660, the Security Council determined that there existed "a breach of international peace and security with regards to the Iraqi invasion of Kuwait." S.C. Res. 660, U.N. Doc. S/RES/660 (Aug. 2, 1990).

566. In October 2005, by Resolution 1636, the Security Council determined that the terrorist act that killed the former Prime Minister of Lebanon Rafiq Hariri, as well as the act's implications, constituted a threat to international peace and security. S.C. Res. 1636, U.N. Doc. S/RES/1636 (Oct. 31, 2005).

567. By Resolution 1718, the Council determined that the test of a nuclear weapon supposedly carried out by the Democratic People's Republic of Korea constituted a "clear threat to international peace and security." S.C. Res. 1718, U.N. Doc. S/RES/1718 (Oct. 14, 2006).

568. *Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII)*, REPERTOIRE OF THE PRACTICE OF THE SECURITY COUNCIL, http://www.un.org/en/sc/repertoire/actions.shtml (last visited Feb. 26, 2014). By Resolution 1295, the Council determined that the continuing conflict in Angola constituted "a threat to international peace and security in the region." S.C. Res. 1295, U.N. Doc. S/RES/1295 (Apr. 18, 2000).

569. U.N. Charter art. 39.

570. Schmitt, *Cyber Operations*, *supra* note 427, at 161.

571. CHARTER OF THE UNITED NATIONS, *supra* note 425, at 721.

572. For example, by Resolution 1769, in 2007 the Council reiterated its deep concern for the security of humanitarian aid workers and their access to populations in need, and reaffirmed its concern that the ongoing violence in Darfur might further negatively affect the rest of the Sudan, as well as the region. The Council determined that the situation in Darfur continued to constitute "a threat to international peace and security." S.C. Res. 1769, U.N. Doc. S/RES/1769 (July 31, 2007). Additionally, by Resolution 1778, the Council expressed the gravest concern that the situation in the region of the border be-

It is uncertain as to when the Security Council might declare satellite signal interference a threat or breach of the peace. More likely than not, satellite signal interference resulting in death or damage to property would qualify as a breach of the peace. However, whether acts short of death or damage would be so qualified is unknown because the Security Council enjoys considerable discretion when making determinations.[573] As noted by Professor Schmitt, a threat to the peace is a political decision, not a legal one.[574] In other words, it is whatever the Security Council decides it to be.[575]

With this understanding, the question becomes, under what circumstances might the Security Council consider satellite signal interference to be a threat to the peace, breach of the peace, or an act of aggression, and authorize responsive measures. The answer depends solely on the circumstances of the case, as well as the relationship of the five permanent members of the Council to the issue under consideration.[576] For instance, if any one of the five permanent members has an interest in the act under consideration and exercises their right to veto pursuant to Article 27, it would block all but procedural resolutions of the Council.[577]

However, because the use of force, aggressions and acts of violence always presume a breach of the peace,[578] any satellite signal interference constituting aggression or a use of force should result in Security Council resolutions, recommendations or measures taken in accordance with Articles 41 and 42. Despite this, and given the selective actions of the Security Council, such a result seems highly speculative. Nevertheless, should the Security Council determine a situation caused by satellite signal interference is of greater gravity than merely endangering the maintenance of international peace and security,[579] a threat to the peace determination could be made.

---

tween the Sudan, Chad and the Central African Republic constituted "a threat to international peace and security." S.C. Res. 1778, U.N. Doc. S/RES/1778 (2007). By Resolution 1078, the Council particularly expressed concern at the humanitarian situation and the large scale movements of refugees and internally displaced persons, and determined that the magnitude of the humanitarian crisis in eastern Zaire constituted a threat to peace and security in the region. S.C. Res. 1078, U.N. Doc. S/RES/1078 (Nov. 9, 1996).

573. *Tadić, supra* note 510, at 28.

574. Schmitt, *Cyber Operations*, *supra* note 430, at 161.

575. *Id.*

576. SHAW, *supra* note 483, at 1120.

577. U.N. Charter art. 27.

578. CHARTER OF THE UNITED NATIONS, *supra* note 425, at 721.

579. U.N. Charter art. 41.

If the Security Council determines peace is threatened, that alone is sufficient to take action as necessary under Articles 41 and 42. Such measures may even be preceded by provisional action taken under Article 40 to prevent aggravation of the situation and induce negotiations. Regardless, once the Security Council decides an incident constitutes a threat to international peace and security, breach of the peace or an act of aggression, the Security Council can respond by either non-forcible measures under Article 41 or forcible measures under Article 42.

Pursuant to Article 41, non-forcible measures include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations." What is interesting to note, however, is that "interruption of . . . communication[s]" is considered as "measures not involving the use of armed force." Under this characterization, one could argue that satellite signal interference may never constitute a use of force. This author asserts such an interpretation is far too overreaching because drafters of the Charter never contemplated satellite signal interference would be used to cause physical damage and human injury.[580] Regardless, the Security Council may authorize any measure under Article 41 deemed necessary to respond to the act at issue to maintain or restore international peace and security, including an authorization to employ satellite signal interference.

Where the Security Council feels measures prescribed under Article 41 are unsuccessful or would be inadequate, it may, pursuant to Article 42, "take action by air, sea, or land forces as may be necessary to maintain or restore international peace and security." Such action extends to demonstrations, blockades, and other armed operations by air, sea or land forces of members of the United Nations. Despite this authority to resort to forcible means, this author believes it is highly unlikely the Security Council would ever authorize force against satellite signal interference. Where satellite signal interference is ongoing or cannot be otherwise stopped, however, forcible means are certainly within the Security Council's purview. In this case, the only factors limiting the Security Council's actions are norms within international law, including the IHL prohibition on attacking the civilian population and civilian objects, as well as the principles of necessity and proportionality.

580. Relying on Schmitt, *Computer Network Attack, supra* note 419, at 912.

2. The Right of Self-Defense

The second exception to the UN Charter's prohibition of the use of force is the right of self-defense embodied in Article 51. In the *Nicaragua* case, the ICJ recognized the right of self-defense in Article 51 refers to pre-existing customary law.[581] Article 51 provides:

> Nothing in the present 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. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

While States have the inherent right of self-defense, States are only permitted to exercise that right by way of a forcible response in the event an armed attack occurs and only until the Security Council takes measures necessary to maintain international peace and security. Thus, the right to self-defense cannot be asserted against acts falling short of armed attacks.[582] This means satellite signal interference must rise to the level of an armed attack for a State to respond lawfully under Article 51. As noted previously, however, armed attacks constitute the "most grave forms of the use of force."[583] Thus, if this threshold is not reached, a State's response is limited to non-forceful means, lawful countermeasures or recourse to the Security Council. If the armed attack threshold is reached, however, Security Council authorization is not required before a State can take defensive action.

Additionally, satellite signal interference employed as a component of an ongoing or broader military action otherwise constituting an armed attack does not alter the nature of the attack. For example, satellite signal interference may be employed against an enemy's air defense system or military communication infrastructure as part of a larger military operation. In this case, a State would be able to respond forcefully to this interference because it is an element of the overall military action. Likewise, satellite sig-

581. *Nicaragua, supra* note 361, ¶ 176.
582. CHARTER OF THE UNITED NATIONS, *supra* note 425, at 793.
583. *Nicaragua, supra* note 361, ¶ 191.

nal inference employed as a component of a lawful military response to an armed attack may be permissible so long as its use complies with IHL prohibitions against attacking civilians and civilian objects in addition to the principles of necessity and proportionality.

E. Legal Criteria for Engaging Self-Defense

As held by the ICJ in *Nicaragua*, all actions taken in self-defense, whether individual or collective, must comply with the principles of necessity and proportionality.[584] The ICJ has also repeatedly recognized self-defense warrants only those measures "proportional to the armed attack and necessary to respond to it" as a "rule well established" in customary law.[585] The principle of necessity requires measures taken in self-defense must have been necessary for that purpose, "leaving no room for any 'measure of discretion.'"[586] That is, the force used must be timely,[587] necessary to halt and repel the attack,[588] and non-forcible measures must be either futile or have been exhausted in an unsatisfactory manner.[589] The principle of proportionality addresses the issue of how much force is permissible.[590] It requires the scale, scope, duration and intensity of a defensive response be limited to that which is necessary to neutralize or repel an attack underway.[591] Additionally, the principle of proportionality does not restrict the defending State to use the same weapons or amount of force as the attacking State, nor is it limited to action within its own territory.[592]

The principles of necessity and proportionality make a response to satellite signal interference particularly challenging because a State may be required to employ a wide array of passive measures prior to resorting to any forcible course of action. For instance, if non-forcible measures are sufficient to stop the attack, a State may not engage in forcible measures. If, however, non-forcible measures are inadequate, forcible measures includ-

584. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 120–21 (2000).

585. *Nicaragua, supra* note 361, ¶ 176; *Nuclear Weapons, supra* note 375, ¶ 41; *Oil Platforms, supra* note 494, ¶ 74.

586. *Oil Platforms, supra* note 494, ¶ 73.

587. DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE, *supra* note 432, at 210.

588. GRAY, *supra* note 584, at 121.

589. Dinstein, *CNAs and Self-Defense*, *supra* note 445, at 109.

590. Schmitt, *Cyber Operations*, *supra* note 427, at 167.

591. *Id.*

592. HARRISON DINNISS, *supra* note 389, at 104.

ing kinetic operations may be employed, assuming they also conform to the applicable legal constraints of IHL.

F. Jus in Bello and Satellite Signal Interference

As discussed in Section III, intentional interference with commercial communication satellites in the context of armed conflict poses serious challenges to IHL. Not only can almost every civilian satellite be used for civilian and military purposes simultaneously, but also it may be impossible to avoid causing harm to civilians and civilian objects when satellite signals are targeted and interrupted. In addition, because military communications are increasingly flowing through civilian satellite systems, it is becoming more and more difficult to isolate, attack and disrupt only military communications. Moreover, due to the interconnectedness of satellite infrastructure, it is practically impossible to foresee the effects military action can have on the civilian population. Thus, even though IHL requires States to consider the collateral consequences of satellite signal interference to the maximum extent possible before any military action is taken, the practical application is unclear regarding the impact satellite signal interference will have on the civilian population and what foreseen and unforeseen consequences will follow.

Despite this, with proper consideration and anticipatory planning, satellite signal interference could become the preferred tool in warfare because it has the potential to limit human suffering when compared to traditional means of kinetic warfare. As discussed in Section III, the purpose of most satellite signal interference is to temporarily disrupt communications, not to cause physical destruction. Moreover, as soon as the military advantage is achieved, the purpose of the attack dissolves. Thus, satellite signal interference persists only temporarily and with reversible effects, thereby providing a distinct advantage not offered by conventional weapons. Accordingly, despite some effects resulting during an armed conflict, satellite signal interference also appears consistent with the goals of IHL. Satellite signal interference can result in less loss of life, does not require physical destruction of the objective, seeks only to disable or disrupt a target for a limited amount of time and is reversible.

Given the unique nature of intentional interference, every effort must be made to apply the existing principles of IHL as directly and thoroughly as possible to dual-use commercial communication satellites. While this suggests States should, at all times, be obligated to segregate their military

communications from civilian communications and use only military satellites, in practice, there is no ability to do so. Regardless, compliance with IHL principles and rules is not only required to the maximum extent possible, but also vital to ensuring the protection of all humanity and future generations from the frightening consequences of future wars.

VI. CONCLUSION

Commercial communication satellites are integrated into almost every aspect of modern day life. These satellites, however, lack sufficient protections against interference and jamming. As a result, commercial communication satellites are becoming increasingly vulnerable to the consequences of disruptions. The ITU framework, ISL and general international law contain provisions prohibiting satellite signal interference. Legal norms also obligate States to take the requisite steps necessary to stop any interference originating within their territories. These existing norms, however, have proven ineffective in containing and constraining intentional interference. Nevertheless, States are unwilling to vest regulatory authorities with enforcement powers, often fail to report incidents of satellite signal interference and do not pursue reparations under international law. While the basis for such inaction is uncertain, it appears many States are unwilling to call negative attention to activities they too enjoy and wish to preserve. Nevertheless, if satellite transmission disruptions become increasingly widespread and lead to significant physical damages, severe economic losses or substantial human injuries, States will look to the UN Charter to form a legal basis to respond to such acts.

As demonstrated, the prohibition on the use of force under Article 2(4) is adaptable to the emerging realities of satellite signal interference, and States will likely look to accepted criteria to identify those instances in which satellite signal interference results in unacceptable and prohibited consequences. States are also always permitted to respond with self-help measures to breaches of international law that both do and do not rise to a use of force. As noted above, this could include severing diplomatic relations, imposing trade embargos, closing borders to the offending State and even engaging in countermeasures as appropriate and as guided by international law.

For satellite signal interference to rise to the level of an armed attack and trigger a States' right to respond in self-defense, however, only those instances that constitute the most grave forms of force will qualify. Thus,

while few instances of satellite signal interference are likely to ever trigger the right of self-defense, it is a possibility States cannot afford to ignore. This is especially true for those States employing satellite signal interference and/or permitting such acts within their territories. In any case, State responses, regardless of weapons employed, are limited to those contained in international law and must conform to the principles within IHL.

To the extent satellite signal interference is employed as a means of warfare, IHL undoubtedly requires it be necessary, proportional and discriminate, as well as humane. While the availability of satellite signal interference as a means and method of warfare serves to increase the options available to States for minimizing collateral damage and incidental injury to civilians, whether IHL can protect the civilian population from the effects of interference remains to be seen. It will depend on how States interpret IHL with regard to satellite signal interference, and to what extent States exercise restraint and the utmost due care when targeting satellite signals. Even then, the reality is civilians will become victims of modern warfare, because as civilian infrastructures increasingly become dual-use and thus valid military objectives, they can and will be subjected to targeting and attack.