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

by

Sarah M. Mountin

A thesis submitted to McGill University
in partial fulfillment of the requirements of
the degree of **MASTER OF LAWS (LL.M)**

Institute of Air and Space Law
McGill University
Montreal, Quebec
August 2013

Unless otherwise noted, the conclusions expressed herein are solely those of the author writing in her personal capacity. They are not intended and should not be thought to represent official ideas, attitudes, or policies of any agency of the United States Government. The author has used only information available to the public in the researching and presentation of her work.

Acknowledgements

I express sincere gratitude to the United States Air Force and The Judge Advocate General for giving me the opportunity to study at the Institute of Air and Space Law at McGill University.

I would also like to thank my husband Chad, and our children, Madison and Henry, for their love, constant support, understanding, patience and encouragement throughout this past year and always. I thank them for viewing everything we have done and everywhere we have lived as another adventure full of new opportunities, new friendships and new experiences. Moving so frequently can be challenging and I thank them for doing so each time with excitement and open minds. I also thank Ms. Rachel Bowline for helping our family throughout this entire year.

Appreciation must also be extended to Major Matt Burris. Major Burris suggested the topic of this thesis, forwarded relevant materials to me and was extremely helpful in suggesting resources. Gratitude is also due Professor Ram Jakhu, who always found time to respond my questions and who forwarded valuable documents related to satellite signal interference. I must also thank Ms. Kathleen VanderNoot for providing me with a quiet, bright space in the Gelber Law Library.

I thank Mr. Michel Bourbonniére, legal counsel for the Canadian Space Agency, for his recommendations, for forwarding research materials and articles and for sharing his enthusiasm for and knowledge of outer space and the law of armed conflict. I thank Mr. Denis Couillard, Director of Innovations at Ultra Electronics TCS for the time he spent explaining the technical aspects of satellites and satellite signal interference.

I am also grateful to all of my fellow classmates, whom I am honored to call lifelong friends and with whom I will share great memories. I thank Isavella Vasilogeori, Mr. Kuzivakwashe Charamba and Mr. Charles Stotler for their guidance, advice and suggestions throughout the drafting of this thesis. I also thank Mr. Louis-Axel Batiste who provided the French translation for the abstract. I also owe deep and heartfelt thanks to Major Erik Mudrinich, Mr. James Rendleman, Col Andrew Williams and Dr. Barbara Mandleco for the time they spent reviewing this thesis and for providing feedback and recommendations.

Finally, I wish to express gratitude to Professor René Provost, my thesis advisor, for devoting his time, energy and patience to the supervision of this thesis and for providing me with his invaluable insight, guidance and support. I cannot thank him enough for his advice, recommendations, and instruction, all of which were all instrumental in the preparation, scope and path of this thesis. He always expressed interest and encouragement as well as shared thought provoking ideas with respect to facts and the law, for which I am truly grateful.

Abstract

Over the past few decades, commercial communication satellites have improved the lives of people all over the world. They have fundamentally transformed the way people communicate, how business is conducted, and the manner in which militaries operate, fight and win wars. This dependence, however, has revealed that commercial communication satellites are increasingly vulnerable to disruptions, but also that these disruptions can pose significant risks to users everywhere. Such risks are especially concerning given the likelihood that satellite signal interference will be employed during future armed conflicts to disrupt the communications of adversaries. The implications of this new political, technical and military reality challenge the normative frameworks under international telecommunications law, international space law and international humanitarian law.

This thesis addresses these and related issues in four chapters. Chapter One explores the extent to which satellite signal interference is becoming a serious threat to global users. Chapter Two discusses the technical application of interference and the normative regimes governing or relating to satellite transmissions and satellite communications. Chapter Three examines circumstances under which satellite signal interference can constitute an unlawful use of force or amount to an armed attack pursuant to the UN Charter. Chapter Four outlines the range of responses available to States suffering the effects of satellite signal interference.

Résumé

Au cours des dernières décennies, les satellites de télécommunication ont amélioré la qualité de vie de millions d'humains, et ont profondément transformé leur manière de communiquer. De la même manière, le monde des affaires et les armées ont considérablement changé leur manière d'opérer. Cependant, cette nouvelle dépendance a mis en évidence la vulnérabilité croissante des satellites de télécommunications aux incidents et les risques que ces derniers présentent aux usagers de toute la planète. De tels risques sont préoccupants, étant donnée la probabilité que de futurs belligérants provoquent des interférences avec les signaux satellitaires lors de conflits armés. L'existence de cette nouvelle réalité politique, technique et militaire remet en cause le cadre normatif formé par le droit international des télécommunications, le droit spatial et le droit humanitaire.

La présente thèse aborde ces difficultés et les problèmes adjacents. Le premier chapitre explore la portée de la menace réelle que représentent les interférences avec les signaux satellitaires pour les usagers du monde entier. Le deuxième chapitre étudie les applications techniques de ces interférences, ainsi que les normes qui régissent les transmissions par satellite. Le troisième chapitre examine les conditions dans lesquelles les interférences sont constitutives d'un usage illégal de la force ou s'apparentent à une agression armée au sens de la Charte des Nations Unies. Le dernier chapitre s'attarde sur les moyens dont disposent les Etats contre les interférences avec les signaux satellitaires.

Acronyms and Abbreviations

ASAT	Anti-Satellite Weapon
CAN	Computer Network Attack
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
GEO	Geosynchronous Orbit
GPS	Global Positioning System
HBO	Home Box Office
IAC	International Armed Conflict
ICJ	International Court of Justice
IHL	International Humanitarian Law
ITU	International Telecommunications Union
ISL	International Space Law
LEO	Low Earth Orbit
MIFR	Master International Frequency Register
NAFTA	North American Free Trade Agreement
NIAC	Non-International Armed Conflict
PNT	Precision Navigation and Timing
SWIFT	Society for World Interbank Financial Telecommunications
TT&C	Telemetry, Tracking and Command
US	United States
UN	United Nations
WRC	World Radiocommunication Conference

Table of Contents

Introduction

Commercial communication satellite systems have become essential and ubiquitous elements to 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, 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 vulnerable. 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]

---

[1] David A. Koplow, "ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons" (2009) 30 Mich J Int'l L 1187 at 1190.

[2] Deborah Housen-Couriel, "Disruption of Satellite Transmissions *ad Bellum* and *in Bello*: Launching a New Paradigm of Convergence" (2012) 45:3 Isr LR 431.

[3] Lawrence T. Greenberg, et al, *Information Warfare and International Law* (National Defense University Press, 1998) at 1; Housen-Couriel, *supra* note 2 at 437.

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

More ominously, as this paper 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 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 on high capacity satellite communications,[10] the

---

[5] James G. Savage, *The Politics of International Telecommunications Regulation* (Boulder, San Francisco & London: Westview Press, 1989) at 134.

[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" *The Washington Post* (9 July 2002), online: The Washington Post < 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* (Royal Holloway, United Kingdom, 2006).

[8] Savage, *supra* note 5 at 134.

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

[10] Ronald C. Wilgenbusch & Alan Heisig, "Command and Control Vulnerabilities to Communications Jamming," (2013) 69:2 Joint Force Quarterly 56 at 57, online: National Defense University <http://www.ndu.edu/press/lib/pdf/jfq-69/JFQ-69_toc.pdf>.

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] the frequency of such events is accelerating, as is the range of actors capable of exploiting signal vulnerabilities.

As this thesis 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 % 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 % of its

---

[11] *Ibid* 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* (5 March 2012), online: The Space Review <http://www.thespacereview.com/article/2038/1>.

[15] Mohammad Ghazai, "Satellite Channel Jamming Rose Sharply After Arab Spring" *The Jordan Times* (15 May 2013), online: The Jordan Times <http://jordantimes.com/satellite-channel-jamming-rose-sharply-after-arab-spring>.

[16] Jakhu, "Satellites," *supra* note 4.

satellite communications needs.[17] Jamming also poses challenges for States when the effects are generated within their borders or by its citizens. As this thesis 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 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 1,000 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 act also underscores a serious concern for the global

---

[17] Loren B. Thompson, "Lack of Protected Satellite Communications Could Mean Defeat for Joint Force in Future War" *Lexington Institute Early Warning Blog* (14 April 2010), online: Lexington Institute < http://www.lexingtoninstitute.org/lack-of-protected-satellite-communications-could-mean-defeat-for-joint-force-in-future-war>.

[18] Myres S. McDougal, Harold D. Lasswell, & Ivan A. Vlasic, *Law and Public Order in Space* (New Haven & London: Yale University Press, 1963) at 284.

[19] Gruss, *supra* note 4.

[20] Choe Sang-Hun, "Seoul Says North Korea Tries to Disrupt Air Navigation" *The New York Times* (2 May 2012), online: The New York Times <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* (30 May 2013), online: <http://www.reuters.com/article/2013/05/30/shipping-navigation-gps-idUSL5N0E926V20130530>.

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

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 originating from within their borders.[25] For example, the Iranian government was called upon several times between 2010-2012 by the International Campaign for Human Rights in Iran, the International Telecommunication Union (ITU), the European Union, the governments of the United Kingdom, U.S. and France, and the Broadcasting Board of Governors to put

---

[22] Frank Oliveri, "The Pentagon's GPS Problem" *Congressional Quarterly* (9 February 2013), online: <http://public.cq.com/docs/weeklyreport/weeklyreport-000004218242.html>.

[23] *Constitution of the International Telecommunication Union,* cited in *Collection of the basic texts of the International Telecommunication Union adopted by the Plenipotentiary Conference,* 2011 ed. (Geneva: ITU 2011), art 45 [*ITU Constitution*].

[24] Jakhu, "Satellites," *supra* note 4.

[25] "Satellite Jamming in Iran: A War Over Airways, Media Report" (November 2012), online: PBS <http://www.pbs.org/wgbh/pages/frontline/tehranbureau?satelliteJammingInIranSmallMedia.pdf>

an end to interference and cease jamming of satellite broadcasts.[26] Iranian officials however, have yet to take any visible efforts to comply with any of these requests.[27]

Further complicating the problem of satellite signal interference is 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 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, but also finds interference occurs within an evolved political and technological reality that now calls for a reexamination of that framework.

---

[26] *Ibid.*

[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. *Ibid.*

[28] Many countries such as the United States, Russia, China, Iran, Cuba, Iraq and North Korea have military jamming capabilities. See Tom Wilson, "Threats to United States Space Capabilities" (Paper prepared for the Commission to Assess United States National Security Space Management and Organization), online: <http://www.fas.org/spp/eprint/article05.html>.

[29] Ram Jakhu, "Regulatory Processes for Communications Satellite Radio Frequencies" in Joseph N. Pelton, Scott Madry & Sergio Camacho Lara, eds, *The Handbook of Satellite Applications* (New York: Springer Science & Business Media, 2013) 271 at 287 [Jakhu, "Regulatory Processes"].

Accordingly, this thesis addresses some of the rules applicable to satellite signal interference in peacetime as well as during armed conflict. In doing so, this thesis 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 thesis 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 UN 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) of the UN Charter 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]

Chapter One explores the emergence of satellite technology and the growing dependence on satellite communications by civilian, economic and military users. It also examines the extent to which satellite signal interference is becoming a serious threat to global users. Finally, it considers the potential impacts and effects resulting from intermingling civilian and military activities through "dual-use" satellite systems.

Chapter Two examines the technical characteristics of satellites and explores how interference is employed to disrupt satellite communications. It briefly discusses some of the specific vulnerabilities of commercial communication satellites. Chapter Two also addresses existing normative regimes governing satellite transmissions under the ITU and International Space Law as well as the implications of interference under International Humanitarian Law. Chapter Two reveals that not only does satellite signal interference challenge the adequacy of existing legal regimes but also that these regimes will not adequately address rapidly emerging technologies and modern warfare.

[30] Housen-Couriel, *supra* note 2 at 434-435.

Chapter Three examines the applicability of the normative framework of the UN Charter to satellite signal interference. It explores circumstances under which satellite signal interference could constitute a use of force under Article 2(4). It also addresses the possibility that satellite signal interference can, and may someday, be viewed by States as an act amounting to an armed attack under Article 51 thereby triggering a State's right to act in self-defense.

Chapter Four outlines some of the responses available to States suffering from the effects and consequences of satellite signal interference. It discusses some of the remedies available under general international law as well as permissible parameters of self-defense when triggered by Article 51 of the UN Charter.

Chapter One: 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 of America, and satellites are more useful now than 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 (U.S.) and the Soviet Union for maintaining peace and security through reconnaissance, and

---

[31] Manfred Lachs, *The Law of Outer Space: An Experience in Contemporary Law Making* (Netherlands: Sijthoff Leiden, 1972) at 1.

[32] Jakhu & Singh, *supra* note 3 at 74.

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

intelligence-gathering purposes; arms control monitoring and compliance; missile warning weapons detection; survivable strategic, global, and regional communications; meteorology; and precision navigation and timing (PNT) systems.[34] Now, satellites-based technologies are indispensable to a variety of civilian, space, science and commercial applications to include communications, meteorology, and remote sensing. For example, of the 1046 satellites currently orbiting Earth, approximately 59% are used for communication purposes, 9% for remote sensing, 8% for navigation, 7% for military surveillance, 5% for space science and 4% for meteorology.[35] Additionally, the U.S. Air Force's Global Positioning System (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, 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 difference financial and economic systems."[36] Commercial satellites relay hundreds of

---

[34] Laura Grego, "A History of Anti-Satellite Programs" (January 2012), online: Union of Concerned Scientists < 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* (LL.M. Thesis, McGill University Institute of Air and Space Law, 2003) at 5.

[35] Union of Concerned Scientists, UCS Satellite Database, online: Union of Concerned Scientists <http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html>. See also Koplow, *supra* note 1 at 1190.

[36] Steven J. Lambakis, *On the Edge of Earth: The Future of American Space Power* (Lexington, Kentucky: The University Press of Kentucky, 2001) at 15.

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] which is integrated into smart phones, law enforcement operations, the navigation and positioning of cars, airplanes, ships, as well as in the fleet management of trucks[43] and many aspects of the economy and commerce, [44] e.g., the Society for World Interbank Financial Telecommunication

---

[37] John E. Oberright, NASA Artificial Satellites, online: <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" online: <http://www.esoa.net/upload/files/news/Why%20Satellites%20Matter%20-%20Full%20Report.pdf>.

[39] *Ibid.*

[40] *Ibid.*

[41] Ryan McClure, "International Adjudication Options in Response to State-Sponsored Cyber-Attacks Against Outer Space Satellites" (2012) 18 New Eng J Int'l & Comp L Ann 431 at 433.

[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* (Surrey, England: Ashgate, 2009) at 389-390.

[44] Oliveri, *supra* note 22.

(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 time-stamp contractual agreements and financial transactions.[46] The shipping industry relies on satellite navigation services to avoid underwater hazards and stay within shipping channels and commercial communications systems, 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, 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 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

---

[45] Joy Gordon, "The U.S. Embargo against Cuba and the Diplomatic Challenges to Extraterritoriality" (2012) 36 Fletcher Financial World Aff 63 at 70.

[46] Lyall & Larsen, *supra* note 43 at 390; Acker, Potscher & Lefort, *supra* note 38.

[47] Paul W. Gydesen, *What it the Impact to National Security Without Commercial Space Applications* (Research Project, Air War College, Maxwell Air Force Base, Alabama, 2006) at 9, online: Air University <http://www.au.af.mil/au/awc/awcgate/awc/gydesen.pdf>.

[48] *Ibid*.

[49] Wilson, *supra* note 28 at IV(B); Norman Martello, "Where in the World?" (March 1999) 24 Electric Perspective 14 at 17.

weapons; (precision-guided munitions and unmanned aerial 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 U.S. 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 U.S. military communications element alone consisted of 118 mobile ground stations and 12 commercial satellite terminals which provided 329 voice and 30 message circuits that handled approximately

[50] Greenberg et al, *supra* note 3 at 1.

[51] Michael N. Schmitt, "International Law and Military Operations in Space" (2006) 10 Max Planck Yearbook of United Nations Law 89 at 90 [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 N. Jasentuliyana ed, *Perspectives on International Law* (The Netherlands: Kluwer Law & Business, 1995) 385 at 388.

[54] Jackson Nyamuya Maogoto & Steven Freeland, "Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist" (2007) 41 Int'l L 1091 at 1104.

700,000 telephone calls and 152,000 messages daily.[55] The U.S. military also used more than 35,000 tactical radio frequencies.[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 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

---

[55] Sean P. Kanuck, "Information Warfare: New Challenges for Public International Law" (1996) 37 Harv Int'l L J 272 at 282, citing Alvin Toffler & Heidi Toffler, *War and Anti-War: Making Sense of Today's Global Chaos* (New York: Warner Books, 1993) at 79.

[56] *Ibid* at 282, citing Toffler at 69-70.

[57] Waldrop, *supra* note 34 at 1, 17-18.

[58] *Ibid* at 6-9.

[59] Paul B. Stares, "Space and U.S. National Security" in William Durch, ed, *National Interests and the Military Use of Space* (Cambridge, Mass.: Ballinger, 1984) at 41.

[60] Robert W. Jarman, *The Law of Neutrality in Outer Space* (LL.M. Thesis, McGill University Institute of Air and Space Law, 2008) at 6-7.

[61] Matthew Burris, "U.S. Space Security: History, Law & Policy" (Presentation delivered online U.S. Air Force JAG Corps, 25 April 2013), [unpublished].

directing civilians to gas stations and supermarkets, are tied into ATMs, the power grid, and cellular phone systems, and are used by over 800,000 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% 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 U.S. has recently signed a one-year, $10 million dollar lease with the Chinese controlled satellite, Apstar-7.[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: "[e]very new drone feed and every new soldier with a satellite radio creates

---

[62] *Ibid.*

[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, naval forces as well as weapons. Stares, *supra* note 59 at 35.

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

[67] Noah Shachtman, "Pentagon Paying China – Yes, China – To Carry Data" *Wired.com* (29 April 2013), online: <http://www.wired.com/dangerroom/2013/04/china-pentagon-satellite/>.

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…. We 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 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, 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.

---

[68] *Ibid*.

[69] Kate Rust, "Kehler: 'The Future of Space is Now'" (7 December 2007), online: Air Force Space Command <http://www.afspc.af.mil/news/story.asp?id=123078666>.

[70] U.S., President of the United States, *U.S. National Space Policy* (28 June 2010) at 10.

[71] Greenberg et al, *supra* note 3 at 1.

B. Emerging Threats to Commercial Communication Satellites

1. Kinetic Weapons and the Problem of Space Debris

Space faring nations will likely pursue non-kinetic measures that are both temporary and reversible within outer space in future conflicts due to the 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 an anti-satellite weapon (ASAT),[73] "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.

---

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

[73] *Ibid*.

[74] U.S., United States Air Force, Counterspace Operations, Air Force Doctrine Document 2-2.1 (2 August 2004) at 33.

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

[76] *Ibid*.

[77] *Ibid*.

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 km) 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 approximately 22,000 miles (35,400 km),[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 can, amongst sufficiently large objects and satellites, produce hundreds of thousands of fragments,[84] which, depending on the orbit, can trigger other collisions thereby causing a cascade of

---

[78] Lyall & Larson, *supra* note 43 at 96.

[79] *Ibid* at 96-97.

[80] *Ibid* at 245-246.

[81] *Ibid* at 96.

[82] *Ibid* at 246.

[83] Theresa Hitchens, "Debris, Traffic Management, and Weaponization: Opportunities for and Challenges to Cooperation in Space" (2007) 14 Brown J World Affairs 173 at 175 [Hitchens, "Debris"].

[84] Lyall & Larson, *supra* note 43 at 305.

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 11 January 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 2 million pieces measuring between 1 mm and 1 cm, over 40,000 pieces of debris between 1 cm and 10 cm (slightly larger than a baseball)[88] and over 900 pieces of trackable debris measuring over 10 cm.[89] The smaller pieces cannot be tracked. A piece larger than 1cm can destroy a satellite, damage the space shuttle and ruin an Astronaut's day.[90]

---

[85] *Ibid*.

[86] David Finkleman, et. al., "Space Debris Birth to Death Analysis from Concern to Consequences" Center for Space Standards and Innovation Analytical Graphics, Inc., online: <http://www.amostech.com/TechnicalPapers/2008/Orbital_Debris/Finkleman.pdf>.

[87] Brian Weedon, "2007 Chinese Anti-Satellite Test Fact Sheet" *Secure World Foundation* (23 November 2010), online: Secure World Foundation < http://swfound.org/media/9550/2007%20chinese%20asat%20test%20factsheet.pdf>; 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" *The Huffington Post* (18 January 2007), online: The Huffington Post < http://www.huffingtonpost.com/noah-shachtman/china-space-attack-unstop_b_38999.html>.

[90] John Kelly, "Debris is Shuttle's Biggest Threat" *Space.com* (5 March 2005), online: <http://www.space.com/792-debris-shuttle-biggest-threat.html>; Tariq Malik, "Station Astronauts Take Shelter from Space Debris" *Space.com* (12 March 2009), online: < http://www.space.com/6410-station-astronauts-shelter-space-debris.html>.

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 (17 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 100 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 a lot of attention is Computer Network Attacks (CNAs).[98]

---

[91] Weedon, *supra* note 87.

[92] *Ibid*.

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

[94] Weedon, *supra* note 87.

[95] *Ibid*.

[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 revealed themselves as growing global threats similarly. Thus, while the current analysis mainly focuses on intentional interference with satellite signals, and not CNAs, the

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 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

---

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.

[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 (IV) Respecting the Laws and Customs of War on Land*, 18 October 1907, (1908 Supp.), 36 Stat. 2295, 2 A. J.I.L. 90, arts 8 & 9. See also *International Convention for the Protection of Submarine Telegraph Cables*, 14 March 1884, online: <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* (Cambridge, MA: American Academy of Arts and Sciences, 2005) at 121.

[103] Jakhu & Singh, *supra* note 4 at 84; Greg Berlocher, "Interference: Operators Making Advances in Flight" *Satellite Today* (1 June 2008), online: Satellite Today <http://www.satellitetoday.com/via/featires/23237.html>.

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 30-minute text message was transmitted to all HBO customers in the eastern half of the U.S.[105] Even though "Captain Midnight's" actions only achieved a temporary disruption to HBO connection with its customers, it nonetheless demonstrated how quickly and easily jamming can be employed to disrupt satellite communications and how far reaching 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

---

[104] Wilson, *supra* note 28 at IV(F).

[105] "The Story of Captain Midnight," online: Signal to Noise <http://web.archive.org/web/20070128101239/http://www.signaltonoise.net/library/captmidn.htm>.

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

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

asymmetric advantages to 21st 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 armed conflict may unintentionally disrupt civilian transmissions, which may be fundamental for civilian or commercial services such as financial transactions, emergency notification networks, and commercial air traffic control systems. Results

[108] Al Santoli, "Beijing Describes How to Defeat U.S. in High-Tech War" *China Reform Monitor* (10 October 2000).

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

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

could include economic chaos, 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 International Humanitarian Law,[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 been from a jamming attack causing the pilot to accidentally land the plane in Iran, believing it 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 significant 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

[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" (2013) 94 Int'l Rev Red Cross 1 at 7.

[113] See Wright, et al, *supra* note 102.

[114] Oliveri, *supra* note 22.

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 jet airline terrorist attacks on New York City 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, somewhere," 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 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

[115] "9/11 Terrorists Made Millions on the Stock Market" Charles Sturt University, online: <http://news.csu.edu.au/director/features.cfm?itemID=4C5F5C13C6A538CCE83C67E0784596AA>.

[116] *Ibid*.

[117] Hugh McDermott, "How Financial Markets Finance Terrorism" *Law, Crime, Politics* (8 July 2011), online: Law, Crime, Politics < http://lawcrimepolitics.com/how-financial-markets-finance-terrorism>.

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

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 other 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 September 11, 2001 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 U.S. 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.

Finally, whereas the International Telecommunications Union (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

[119] *Ibid*.

[120] *Ibid*.

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 while at the same time expanding both their peace time 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 normative framework applicable to satellite communications, the emerging trends, and their implications.

[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] Gansler & Binnendijk, *supra* note 118.

[123] *Ibid*.

Chapter Two: The Technical and Legal Aspects of Satellites and Satellite Signal Interference

This chapter 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.

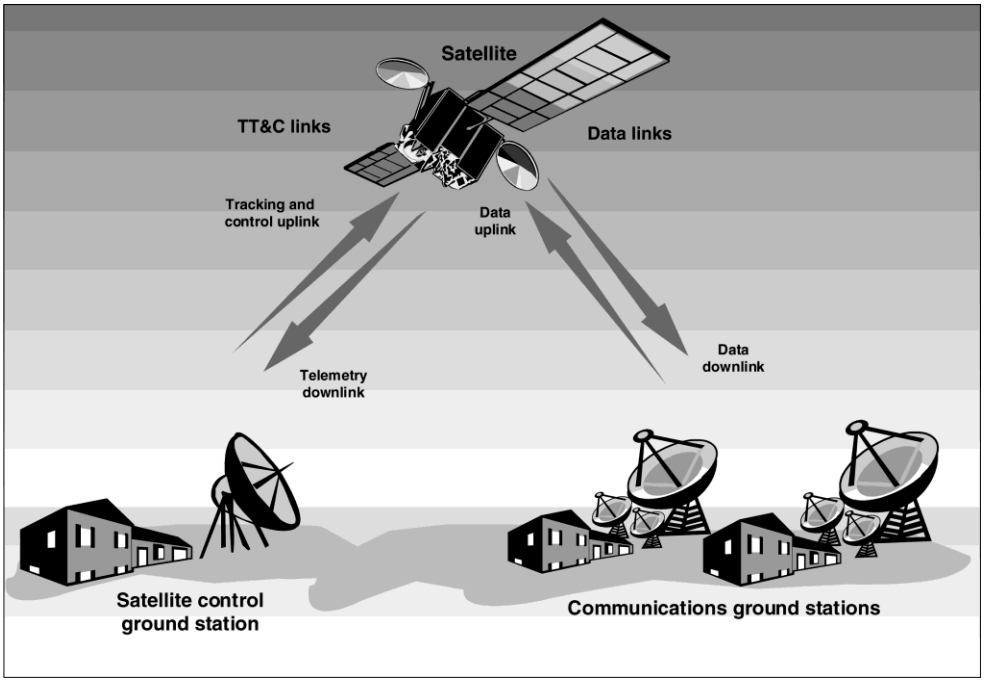
This chapter also examines the legal norms applicable to satellite transmissions under the International Telecommunications Union (ITU) and International Space Law (ISL). This section concludes existing norms are not equipped to handle the range of impacts emerging as more and more State and non-State actors engage in satellite signal interference. Finally, implications of satellite signal interference under International Humanitarian Law (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 harms 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] *See* Figure 1.

[124] Wright, et al, *supra* note 102 at 109.

Figure 1. Components of a Basic Satellite System. [125]



All satellite components are susceptible to physical attacks and/or sabotage.[126] However, some components are more susceptible to non-kinetic attacks, such as intentional interference or jamming.[127] 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.[128] *See* Figure 2.

---

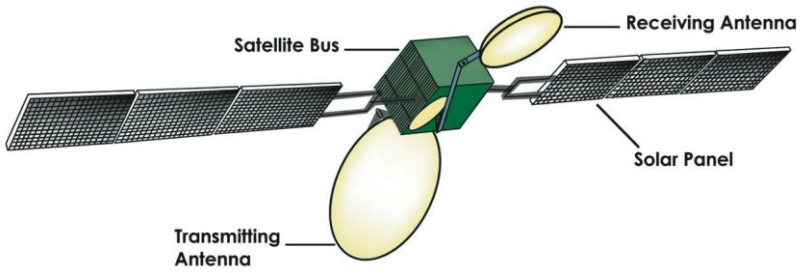
[125] U.S., General Accounting Office, *Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed* (GAO-02-781) (Washington, DC, US General Accounting Office, August 2002) at 8 [GAO, *Critical Infrastructure Protection*].

[126] *Ibid* at 12.

[127] Wright, et al, *supra* note 102 at 109.

[128] *Ibid* at 110.

Figure 2. Graphic illustration of a basic satellite comprised of a satellite bus, the solar panels and the communication system, the transmitting and receiving antennas.[129]



The satellite bus is the central metal structure or body to which other components are attached.[130] The bus carries the payload(s) and is comprised of subsystems including the power supply, antennas, and mechanical and thermal control subsystems.[131] The bus is durable enough to sustain launch stresses and designed to protect components within from threats such as solar heat and some laser attacks.[132] The solar panels, attached to the satellite bus, are the main power source.[133] Electricity generated by the solar panels is stored in rechargeable batteries.[134] 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.

---

[129] *Ibid*.

[130] *Ibid*.

[131] GAO, *Critical Infrastructure Protection, supra* note 125 at 3.

[132] Wright, et al, *supra* note 102 at 110.

[133] *Ibid*.

[134] *Ibid*.

If a satellite or its components are damaged, they cannot be repaired.[135] A fatally damaged satellite has to either be de-orbited and returned to Earth or propelled further up into outer space and into a "graveyard," "disposal," or "junkyard" orbit.[136] 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.[137] For example, the payload for a communications satellite includes radio receivers, transmitters and transponders[138] for collecting, relaying or rebroadcasting television or telephone signals.[139] 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.[140] 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.

---

[135] *Ibid*.

[136] 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 radio-active materials) to de-orbit. Lyall & Larson, *supra* note 43 at 246.

[137] GAO, *Critical Infrastructure Protection, supra* note 125 at 3.

[138] 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.

[139] GAO, *Critical Infrastructure Protection, supra* note 125 at 3.

[140] Stephen Clark, "Reconnaissance Satellites Launched by H-2A Rocket" *Spaceflight Now* (27 January 2013), online: Space Flight Now < 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.[141] In some specialized or highly protected satellites like military satellites, the on-board computer may also utilize anti-jamming computer software.[142] Most non-military, commercial satellites and their on-board computers are relatively unprotected from jamming attacks.[143] This is because they are designed for cheap and easy access and not equipped to protect against interference.[144] As a result, commercial satellites fall victim to an increasing number of jamming attacks.[145] For example, in November 2012, Eutelsat reported deliberate jamming increased dramatically, going from 54 cases in 2010 to over 340.[146]

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.[147] In 2004, the non-State entity, Falun Gong, jammed a Hong Kong based satellite and instead broadcast its own message.[148] From 2009-2010, Iran jammed Intelsat satellite broadcasts into Iran.[149]

---

[141] Wright, et al, *supra* note 102 at 112; GAO, *Critical Infrastructure Protection, supra* note 125 at 3.

[142] Wright, et al, *supra* note 102 at 112.

[143] Grego, *supra* note 34 at 8-9.

[144] *Ibid* at 9.

[145] *Ibid*.

[146] Anne Wainscott-Sargent, "Fighting Satellite Interference on All Fronts" *Satellite Today* (1 March 2013), online: Satellite Today.com <http://satellitetoday.com/via/features/40651.html>.

[147] Safa Haeri, "Cuba Blows the Whistle on Iranian Jamming," *Asia Times* (22 August 2003).

[148] "Falun Gong Hijacks HK Satellite," *Xinhua News Agency* (22 November 2004).

[149] Luke Baker, "2-EU Ministers Warn Iran on Satellite Jamming", *Reuters* (22 March 2010).

Then, in 2010, Brazilian hackers disrupted the U.S. Navy's satellite, FLTSAT-8.[150] Finally, in 2012, when Syria joined Iran in jamming over 25 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.[151]

The communications system is considered the heart of a satellite.[152] 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.[153] Radio links transmit, transfer and receive all satellite signals (radio frequencies carrying data) to and from Earth as well as from other satellites.[154] Radio links are highly vulnerable to interference and when disrupted, deny satellite communications[155] making a satellite useless.[156]

Radio waves comprise part of the electromagnetic spectrum, the spectrum of all frequencies of electromagnetic radiation.[157] While the electromagnetic spectrum includes x-rays, gamma rays, ultraviolet light, visible light rays and radio waves, only visible light

---

[150] Housen-Couriel, *supra* note 2 at 440.

[151] See Wainscott-Sargent, *supra* note 146.

[152] Joseph N. Pelton, *Satellite Communications* (New York: Springer Science & Business Media, 2012) at 19.

[153] Wright, et al, *supra* note 102 at 112.

[154] *Ibid*.

[155] GAO, *Critical Infrastructure Protection, supra* note 125 at 13.

[156] E.R.C. van Bogaert, *Aspects of Space Law* (The Netherlands: Kluwer Law & Taxation Publishers, 1986) at 192.

[157] Weedon, *supra* note 87.

rays are detectable by humans.[158] Despite being invisible to the naked eye, radio waves used in satellite operations can be tracked and located relatively easily[159] because they travel via line-of-sight connections from the sending location to the receiving location.[160] 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.[161]

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).[162] Telemetry refers to the data transfer process (containing specific details on the health and status of the satellite) from the satellite to the ground.[163] Tracking locates the satellite in time and space based on position, speed and range measurements.[164] Command is the method of commanding and controlling the satellite from the ground via the transmission of signals while the satellite is in line of sight of a ground station.[165] TT&C is essential and basically the same for all satellites, regardless of mission.[166]

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

[158] *Ibid*.

[159] 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.

[160] Wilson, *supra* note 28 at III(C).

[161] *Ibid* at III (D).

[162] Wright, et al, *supra* note 102 at 112.

[163] GAO, *Critical Infrastructure Protection, supra* note 125 at 4.

[164] *Ibid*.

[165] *Ibid*.

[166] *Ibid*.

colliding with other satellites. TT&C transmissions, however, are generally protected by way of encryption and encoding.[167] Therefore, TT&C transmissions are not the most vulnerable element of satellite communications to interference or disruptions,[168] 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 elements described above, satellites also have attitude and control systems, and propulsion subsystems. Gyroscopes, accelerometers and guidance systems control satellite and keep it positioned in the right direction for communications and data collection.[169] The propulsion system, comprised of engines and thrusters, maintains station keeping, control and maneuvering.[170] Any malfunction of or interference with these systems could endanger other satellites.[171] Therefore, satellite operators must monitor, control, and communicate with satellites at all times, accomplished through radio signals sent to satellites via Earth-based ground stations.

---

[167] Wright, et al, *supra* note 102 at 112.

[168] *Ibid* at 113.

[169] *Ibid* at 112.

[170] *Ibid* at 113.

[171] *Ibid* at 112-113.

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.[172] Ground stations and antennas can be large, small, stationary or mobile.[173] 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 transmitting or receiving data such as video or voice communications.[174] In addition to sending and receiving satellite signals, ground stations have inherent jamming capabilities.[175]

The area receiving a radio signal of useful strength from the satellite is known as the satellite's coverage area or footprint.[176] *See* Figure 3.

[172] *Ibid* at 114.

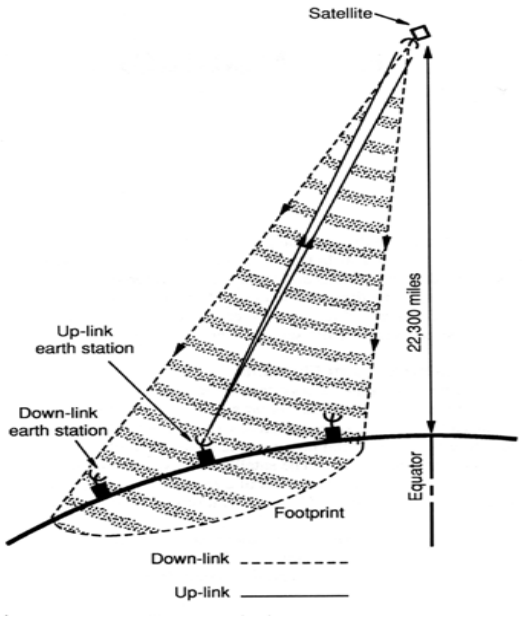
[173] *Ibid*.

[174] *Ibid*.

[175] Wilson, *supra* note 28 at IV.

[176] William Craig Cook, "How Do Satellites Work?" online: <http://www.williamcraigcook.com/satellite/work.html>.

Figure 3 Graphic illustration of a satellite's footprint as well as uplink and downlink satellite communications. [177]



Pathways used to communicate with satellites are called links.[178] A radio signal transmitted from the ground station up to a satellite is the uplink;[179] the radio signal traveling down from the satellite to the ground station is the downlink;[180] crosslinks transmit signals between satellites.[181] 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.[182] Crosslinks would be most vulnerable to space-based jammers.

---

[177] *Ibid*.

[178] Wright, et al, *supra* note 102 at 114.

[179] *Ibid*.

[180] *Ibid*.

[181] *Ibid*.

[182] *Ibid* at 115, 118.

B. The Technical Application of Intentional Interference

Jamming equipment is easy to make and / or buy.[183] Jamming is not complex or technically demanding.[184] It is also increasingly available to and employed by State as well as non-State entities.[185] 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 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…."[186] This has been recognized by the U.S. as a probable act.[187] 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.[188]

---

[183] For example, a jammer can be built using a satellite TV receiver or from 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* (17 March 2010), online: Fox News < http://www.foxnews.com/tech/2010/03/17/gps-jammers-easily-accessible-potentially-dangerous-risk/>.

[184] Grego, *supra* note 34 at 15.

[185] Wright, et al, *supra* note 102 at 118

[186] Santoli, *supra* note 108.

[187] 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 U.S. needed to secure itself against a "Space Pearl Harbor." See U.S., 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), online: Air University <http://space.au.af.mil/space_commission/executive_summary.pdf>; See also Jean-Michel Stoullig, "Rumsfeld Commission Warns Against 'Space Pearl Harbor'" *Space Daily* (11 January 2011), online: Space Daily < http://www.spacedaily.com/news/bmdo-01b.html>.

[188] Kanuck, *supra* note 55 at 284.

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.[189] The object is to render radio transmissions unintelligible by causing interference.[190] It is accomplished by overpowering signals sent to and received by the satellite by emitting noise or using a second signal at the same frequency or higher power, preventing the receiver from collecting the real signal.[191] The jamming signal is often meaningless noise that drowns out the real signal[192] in the form of "harmful interference."[193]

There are two forms of satellite jamming: orbital jamming and terrestrial jamming.[194] Orbital jamming involves beaming a conflicting signal toward a satellite. The original signal is drowned out by the jamming signal so 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,[195] which can impact a large number of users because satellites operate in groups of channels.[196] When one signal is disrupted, all signals in the same group can be affected, thereby cutting off services to all

---

[189] Grego, *supra* note 34 at 9, 15.

[190] Michel Bourbonniére, "Law of Armed Conflict (LOAC) and the Neutralisation of Satellites or *Ius In Bello Satellitis*" (2004) 9:1 J Confl & Sec L 43 at 58 [Bourbonniére, "Law of Armed Conflict"].

[191] Wright, et al, *supra* note 102 at 118.

[192] Wilson, *supra* note 28.

[193] *International Telecommunication Union Radio Regulations,* (Geneva: ITU, 2011) art 1.169 [*ITU Radio Regulations*].

[194] Satellite Jamming in Iran*, supra* note 25 at 22.

[195] *Ibid*.

[196] *Ibid*.

users in the satellite's footprint, which can cover multiple continents.[197] 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.[198] Rather than targeting the satellite, terrestrial jamming targets specific terrestrial users.[199] Thus, whereas orbital jamming effects can extend throughout a satellite's entire footprint, terrestrial jamming effects can be localized and limited to specific targets.[200]

Known as a type of electronic decoy,[201] spoofing is similar to jamming. Instead of drowning out the real signal, a usable but false signal is emitted, mimicking the characteristics of a true signal so the user receives a fake (or spoofed) signal.[202] 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.[203]

In the case of either jamming or spoofing, the jammer must operate in the same radio frequency bands as the system being jammed.[204] The jammer must locate, via radar

---

[197] *Ibid*.

[198] *Ibid* at 24.

[199] *Ibid*.

[200] *Ibid*.

[201] Wilson, *supra* note 28.

[202] Wright, et al, *supra* note 102 at 118.

[203] Oliveri, *supra* note 22.

[204] Wilson, *supra* note 28.

or signal tracking systems,[205] the signals to be jammed, and produce a similar signal with sufficient intensity to overwhelm the targeted signal(s).[206] 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 be jammed.[207] 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.[208] Thus, as long as the jamming activity is within the footprint of the satellite, which can span over 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.[209] Space-based jammers however, are impractical because, in order to be effective, a large number of orbiting jammers would be needed.[210]

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.[211] 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 5-20

---

[205] *Ibid*.

[206] Grego, *supra* note 34 at 15.

[207] Wright, et al, *supra* note 102 at 119.

[208] *Ibid* at 118.

[209] *Ibid* at 119.

[210] *Ibid*.

[211] Wilson, *supra* note 28 at IV.

km, depending on terrain.[212] Even hand-held jammers are now available and can deny radio signals up to 80 km away.[213] 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 U.S. recently passed new laws prohibiting the marketing, sale and use of jamming devices,[214] jamming devices remain widely available in other countries and on-line.[215] 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.

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.[216]

---

[212] Satellite Jamming in Iran*, supra* note 25 at 26-27.

[213] Wilson, *supra* note 28 at IV(F).

[214] U.S., Federal Communications Commission, "FCC Enforcement Bureau Takes Action Against Craigslist Sellers for Marketing Illegal Signal Jamming Devices" Commission Document 15 October 2012, online: FCC <http://transition.fcc.gov/eb/News_Releases/DOC-316796A1.html>.

[215] Wilson, *supra* note 28 at IV.

[216] Wright, et al, *supra* note 102 at 121.

Commercial communication satellites are susceptible to jamming for a number of reasons. First, the cost and weight of countermeasures is considered an unnecessary expense.[217] Second, commercial communication satellites are designed for ease of use and to send and receive signals over large areas.[218] 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 the geosynchronous (GEO) orbit.[219] The GEO orbit lies 35,786 km / 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.[220] 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,[221] and there is a large area from which it is possible to jam or spoof a signal.[222]

---

[217] Wilson, *supra* note 28 at IV.

[218] Wright, et al, *supra* note 102 at 121.

[219] Lyall & Larson, *supra* note 43 at 246, 256.

[220] *Ibid* at 246.

[221] 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 UN 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," online: Union of Concerned Scientists <http://www.ucsusa.org/assets/documents/nwgs/common-misconceptions.pdf>.

[222] Wright, et al, *supra* note 102 at 121.

Some Russian commercial communication satellites operate in the Molniya Orbit, a highly elliptical orbit,[223] because much of Russia is too far north to fall within the footprint of a satellite located in GEO.[224] Other commercial communication satellites, such as Globalstar satellite phone system, use a constellation of 48 satellites positioned in LEO.[225] Because LEO satellites are much closer to Earth's surface than those in GEO (satellites in LEO are located between 65-310 miles / 100-500 km above Earth's surface whereas GEO satellites are located 22,236 miles / 35,785 km above Earth's surface),[226] LEO satellites and their communications are very susceptible to jamming attacks and attacks from Earth-based kinetic weapons.[227]

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 (ITU). 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."[228] Initially founded in 1865 as the International Telegraph Union, the ITU became a UN specialized agency in 1947.[229]

---

[223] Lyall & Larson, *supra* note 43 at 246.

[224] Bourbonniére, "Law of Armed Conflict," *supra* note 190 at 52.

[225] *Ibid*.

[226] Lyall & Larson, *supra* note 43 at 245-246.

[227] Bourbonniére, "Law of Armed Conflict," *supra* note 190 at 52.

[228] *ITU Constitution*, *supra* note 23 at annex 1012.

[229] Lyall & Larson, *supra* note 43 at 200-205.

Currently, 193 countries and over 700 private-sector entities and academic institutions are members.[230]

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.[231] The ITU also develops worldwide technical standards for the use, assignment and allocation of radio frequencies.[232] 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).[233] Registering a signal on the MIFR gives the assigned user a right to "international recognition"[234] 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

---

[230] "About ITU Membership," online: International Telecommunications Union < http://www.itu.int/en/about/Pages/default.aspx>. Despite being members of the ITU however, these 700+ non-State entities do not have standing under international law to deal directly with the ITU.

[231] *ITU Radio Regulations, supra* note 193, art 8.5.

[232] *About ITU*, *supra* note 230.

[233] *ITU Radio Regulations, supra* note 193, art 8.1.

[234] *Ibid*, art 8.3.

frequency if that use creates "harmful interference" with the signal that has international recognition.[235]

"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.[236] All ITU Member States are obligated not to cause harmful interference and enforce and respect the ITU regulatory regime.[237] 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.[238]

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 radio service, and which operate in accordance with the provisions of the Radio Regulations. [239]

---

[235] *Ibid*, art 8.5.

[236] *Ibid*, art 1.169.

[237] Jakhu, "Satellites," *supra* note 4 at 6.

[238] *ITU Constitution, supra* note 23, art 6.1.

[239] *Ibid*, art 45.

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.[240] …Transmitting stations shall radiate only as much power as is necessary to ensure a satisfactory service.[241]

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[242] through bilateral negotiations.[243] 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 of the ITU Constitution. However, neither Article 41 nor Article 56 has ever been used.[244]

---

[240] *ITU Radio Regulations, supra* note 193, art 15.1§1.

[241] *Ibid,* art 15.1§2

[242] *Ibid,* arts 11.42, 11.42A, 15.21 §13; See also Jakhu, "Satellites," *supra* note 4.

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

[244] Jakhu, "Regulatory Processes," *supra* note 29 at 290.

Historically, compliance with ITU provisions, utmost goodwill and mutual cooperation resolved most interference issues.[245] 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,[246] but also there are no compulsory international dispute resolution systems within the ITU legal regime to resolve interference problems.[247] Additionally, not all nations have ratified all of the ITU rules and regulations, 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.[248] 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.[249]

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

---

[245] *ITU Radio Regulations*, *supra* note 193, art.15.22 §14

[246] Savage, *supra* note 5 at 132-134.

[247] Jakhu & Singh, *supra* note 4 at 88.

[248] *Ibid*.

[249] Peter B. de Selding, "ITU Implores Iran to Help Stop Jamming" *Space News* (26 March 2010), online: Space News <http://www.spacenews.com/article/itu-implores-iran-help-stop-jamming#.UdWkfhZsWR8>.

borders.[250] At the 2012 World Radiocommunication Conference (WRC),[251] the ITU took another public step in condemning intentional interference by amending portions of the ITU Constitution and Radio Regulations.[252] 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.[253]

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.

---

[250] Theresa Hitchens, "Multilateralism in Space: Opportunities and Challenges for Achieving Space Security" (2010) 4 Space & Defense 3, 14.

[251] 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 "About ITU: Conferences and Meetings: WRC," online: International Telecommunications Union < http://www.itu.int/ITU-R/index.asp?category=conferences&rlink=wrc&lang=en>.

[252] Yvon Henri, "The ITU Radio Regulations and Space Sustainability" (Presentation delivered to The Brussels Space Policy Roundtable, Brussels, Belgium, 29 November 2012), online: Secure World Foundation <http://swfound.org/media/96609/2012_SSI_Yvon%20Henri.pdf>.

[253] *ITU Radio Regulations*, as modified by WRC-12, at art.15.21 §13.

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….[254] 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.[255]

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….[256]

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.[257] 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.[258] Regardless, a properly executed disruption of satellite transmissions fitting within the Article 34 and 35 exemptions would not violate the ITU

---

[254] *ITU Constitution, supra* note 23, art. 34.1.

[255] *Ibid*, art. 34.2.

[256] *Ibid*, art. 35.

[257] Housen-Couriel, *supra* note 2 at 445.

[258] *ITU Constitution, supra* note 23, art. 38.

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 unclear 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.[259]

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…[260]

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.[261] 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.[262] In armed conflict, the ITU regime would not govern all

---

[259] Roger D. Scott, "Legal Aspects of Information Warfare: Military Disruption of Telecommunications" (1998) 45 Nav L Rev 57 at 63-64.

[260] *ITU Constitution, supra* note 23, art. 48

[261] Scott, *supra* note 259 at 63-64.

[262] Jarman, *supra* note 60 at 41.

acts of "harmful interference." Measures involving interference would be governed by *lex specialis*, specifically, the law of armed conflict (*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[263] between belligerents during armed conflicts.[264] Regardless, ITU treaty obligations between belligerents and non-belligerents (neutrals) would continue in armed conflict under the Law of Neutrality.[265]

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[266] giving rise to state responsibility.[267] While an exhaustive discussion on state responsibility is outside the scope of this thesis, it is

---

[263] While treaty obligations between belligerents during armed conflict were historically suspended between them, 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. Daniel Patrick O'Connell, *International Law, Vol. 1* 2d ed (London: Stevens, 1970) at 268.

[264] *Oppenheim's International Law: A Treatise* 7th ed (H. Lauterpacht, ed, London: Longmans, 1952) at 302.

[265] For a thorough discussion on how the Law of Neutrality applies to satellites as well as outer space, see Jarman *supra* note 60.

[266] Stephen Gorove, *Developments in Space Law: Issues and Policies* (The Netherlands: Kluwer Academic Publishers, 1991) at 49.

[267] International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, UNGAOR, 53d Sess, UN Doc A/56/83 (2001) art 2 [*ASR*].

important to emphasize that a breach of international obligation attributable to a State is an internationally wrongful act[268] thereby triggering a secondary obligation to cease the unlawful conduct and re-establish the *status quo ante* by way of restitution,[269] compensation[270] or satisfaction.[271] 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.[272] 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 (ISL) also governs activities of satellites and satellite communications. Initiated in the 1950's, ISL was formally codified in the 1960's and 1970's as a result of the launch of Sputnik I,[273] the

---

[268] *Ibid*, art 2.

[269] *Ibid*, art 35.

[270] *Ibid*, art 36.

[271] *Ibid*, art 37.

[272] *Charter of the United Nations*, 26 June 1945, Can TS 1945 No 7, art 35 [*UN Charter*].

[273] *Sputnik* means, "fellow traveler." "The Beep Heard 'Round the World," online: <http://memagazine.asme.org/Web/Beep_Heard_Round_World.cfm>. 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 the American completely off-guard. It also shocked the US 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 (ICBM) 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," online: NASA

world's first artificial satellite.[274] Today, the fundamental norms applicable to outer space are found in five treaties[275] and several non-binding principles and declarations.[276] Together, these documents establish the primary principles, rules and legal system for all activities conducted in outer space.

All major space-faring nations are State Parties to most of the ISL treaties including the Outer Space Treaty, the Liability Convention, the Registration Convention, the Return and Rescue Agreement. Participation in the Moon Agreement, however,

---

<www.history.nasa.gov/sputnik>; "A Brief History of the National Aeronautics and Space Administration," online: NASA <http://www.hq.nasa.gov/office/pao/History/40thann/factsheet.htm>; Neil de Grasse Tyson, "The Case for Space: Why We Should Keep Reaching for the Stars" (March/April 2012), 91 Foreign Affairs 22; John W. Mason, *The Cold War, 1945-1991* (London: Routledge, 2009) at 29; McDougal, Lasswell and Vlasic, *supra* note 18 at 283.

[274] *Sputnik* was an aluminum sphere the size of a beach ball (22 inches). It weighed 183.9 pounds and orbited Earth in approximately 98 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 273.

[275] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 19 UST 2410, 610 U.N.T.S. 205 (entered into force on 10 October 1967) [*The Outer Space Treaty*]; *The Agreement on the Rescue of Astronauts and the Return of Objects Launched in Outer Space*, 22 April 1968, 19 UST 7570, 672 U.N.T.S. 119 (entered into force on 3 December 1968) [*The Return & Rescue Agreement*]; *Convention on International Liability for Damage Caused by Space Objects*, 29 March 1972, 961 U.N.T.S. 187, 24 UST 2389 (entered into force 1 September 1972) [*The Liability Convention*]; *Convention on Registration of Objects Launched into Outer Space*, 14 January 1975, 28 UST 695, 1023 U.N.T.S. 15 (entered into force on 15 September 1976) [*The Registration Convention*]; *Agreement governing the Activities of States on the Moon and Other Celestial Bodies*, 18 December 1979, 1363 U.N.T.S. 3 (entered into force on 11 July 1984) [*The Moon Agreement*].

[276] *Question of the Peaceful Use of Outer Space,* GA Res 1348 (XIII), UN GAOR, 13th Sess, (1958); *Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space*, GA Res 1962 (XVII), UN GAOR, 18th Sess, Supp No. 15, UN Doc A/5515 (1963).

remains low with only 15 State Parties to date.[277] Because not all five treaties or provisions therein are relevant to satellite signal interference, this thesis 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.[278] Often referred to as the "Constitution," the "Bible" or "Magna Carta" of Space Law,[279] the Outer Space Treaty has been in force since 10 October 1967, ratified by 102 States and signed by another 26 States.[280] It provides the basic framework for international space law, contains numerous principles passed into customary law,[281] and applies to all activities conducted in outer space, regardless of actor. It also reaffirmed the duty of States to comply with international law[282] while conducting outer space activities.[283]

---

[277] "Status of International Agreements Relating to Activities in Outer Space" United Nations Office for Outer Space Affairs, online: United Nations Office for Outer Space Affairs < http://www.oosa.unvienna.org/oosa/en/SpaceLaw/treatystatus/index.html>.

[278] Michael C. Mineiro, "FY-1C and USA-193 ASAT Intercepts: An Assessment of Legal Obligations Under Article IX of the Outer Space Treaty" (2008) 34 J Space L 321 at 325.

[279] Lyall & Larson, *supra* note 43 at 53.

[280] "Status of International Agreements Relating to Activities in Outer Space, *supra* note 277.

[281] Lyall & Larson, *supra* note 43 at 41.

[282] Under Article 38 of the Statute of the ICJ, international law includes, treaties and international conventions, international custom, 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*, 3 Bevans 1179, 59 Stat. 1031 [*Statute of the ICJ*].

[283] *Outer Space Treaty*, *supra* note 275, art III.

Article III of the Outer Space Treaty dictates that all State Parties must carry on 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."[284] State Parties engaged in any outer space activity are 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, 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.[285] As it relates to this thesis, Article I allows States to utilize satellites and engage in satellite communications without any prior authorization from other States.[286] Article I also establishes the "common interest" principle, which provides space shall be used for the benefit and in the interests of all mankind.[287] In full, Article I requires States 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 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,

---

[284] *Ibid.*

[285] *Ibid,* art I, para 2,

[286] Schmitt, "Military Operations in Space," *supra* note 51 at 101.

[287] *Outer Space Treaty*, *supra* note 275 art I, para 1.

States bear international responsibility for actions committed contrary to international obligations.[288]

Article II of the Outer Space Treaty creates a borderless regime in outer space[289] 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.[290] Article II provides, "Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."[291] Thus, despite the freedom of exploration and use of outer space as codified within Article I of the Outer Space 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.[292]

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 over) specific orbits as assigned by the ITU. Additionally,

---

[288] *Phosphates in Morocco, Preliminary Objections (Italy v. France)* (1938), PCIJ (Ser A/B) No 74, 10 at 28. See also *S.S. Wimbleton (United Kingdom v. Germany)* (1923), PCIJ (Ser A) No 1, 15 at 30; *Factory at Chorzow, Jurisdiction (Germany v. Poland)* (1927) PCIJ (Ser A) No 9 at 21.

[289] Michel Bourbonniére. "The Clausewitz Nebule: The Legitimacy of Military Activities in Outer Space During Armed Conflicts" (2010) 40 Isr YB Hum Rts 243 at 250. [Bourbonniére, "Clausewitz Nebulae"].

[290] *Ibid* at 251-252.

[291] *Outer Space Treaty, supra* note 275, art II.

[292] For a good discussion on whether Article II also prohibits the creation of private property rights on celestial bodies, See Ricky J. Lee, "Article II of the Outer Space Treaty: Prohibition of State Sovereignty, Private Property Rights, or Both?" (2004) 11 Aust. Int'l LJ 128.

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.[293] Satellite orbital slots are also sold,[294] traded and leased.[295] 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 against 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.[296]

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,"[297] and is set forth by Article VI of the Outer Space Treaty. Article VI provides:

---

[293] 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).

[294] "NBN Co Closes in on Satellite Slots" (8 April 2013), online: <http://www.talksatellite.com/Asia-A101283.htm>.

[295] Samuel Black, "No Harmful Interference with Space Objects: The Key to Confidence Building" *Stimson Center* (July 2008), online: <http://www.stimson.org/images/uploads/research-pdfs/NHI_Final.pdf >.

[296] *Outer Space Treaty, supra* note 275, art VI.

[297] Lee, *supra* note 292 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.[298]

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.[299] 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,[300] 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 is carried must retain jurisdiction and control over such object while in outer space.[301] Ownership

---

[298] *Outer Space Treaty*, *supra* note 275 art VI.

[299] Lee, *supra* note 292 at 129.

[300] *Outer Space Treaty*, *supra* note 275, art VI. *Corfu Channel Case (United Kingdom v. Albania),* Merits [1949] ICJ Rep 4 at 22 [*Corfu Channel*].

[301] *Outer Space Treaty*, *supra* note 275, art VIII.

of such an object is not changed by their presence in outer space.[302] Under the Registration Convention, which establishes the link between State and spacecraft,[303] 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)[304] must register the object in its domestic registry and with the UN.[305] 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 procureing 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.[306]

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 air space 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

---

[302] *Ibid,* art VIII.

[303] I.H. Ph. Diederiks-Verschoor, "Registration of Spacecraft" in Edward McWhinney & Martin A Bradley, eds, *New Frontiers in Space Law* (The Netherlands: Kluwer Law, 1969) 125.

[304] *Registration Convention*, supra note 275 art I.

[305] *Ibid,* art II.

[306] *Outer Space Treaty*, supra note 275 art VII.

application; it applies only to *physical* damage[307] 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."[308] 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 from the 1967 U.S. Senate Foreign Relations Committee on the Outer Space Treaty reveals, the U.S. 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 communications..."[309] While the U.S. opinion does not dictate what drafters of Article VII contemplated, it may indicate how the U.S. 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

---

[307] 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 Testimony of U.S. Ambassador Arthur Goldberg in Treaty of Outer Space, Hearings before Senate For. Relations Comm, 90th Cong., 1st Sess. 70-72 (1967).

[308] "Merriam-Webster Online Dictionary," online <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,* 23 May 1969, art 31 (1), 1155 U.N.T.S. 331 [*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."

[309] See Testimony of U.S. Senator Gore in Treaty of Outer Space, Hearings before Senate For. Relations Comm, 90th Cong., 1st Sess. 71 (1967).

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,[310] 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."[311] The Liability Convention imposes liability only when damage is *physically caused* by a space object in a crash, explosion or other direct harm.[312] 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.[313]

---

[310] *Liability Convention*, supra note 275 preamble.

[311] *Liability Convention*, supra note 275 art I.

[312] Carl Q. Christol, *Space Law: Past, Present, and Future* (New York: Springer, 1991) at 219-220.

[313] 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 tis interpretation." *VCLT, supra* note 308, art 31(b).

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 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.[314] As addressed above, all ITU Member States are obligated not to cause harmful interference and enforce and respect the ITU regulatory regime. Moreover, as recognized in the decisions of the *Corfu Channel Case* and the *Trail Smelter Arbitration Tribunal*, a State has an obligation "not to allow its territory to be used for acts contrary to the rights of other States."[315] 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 damaged caused.[316] 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."[317] 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

---

[314] Bin Cheng, *General Principles of International Law as Applied by International Courts and Tribunals* (Oxford: Cambridge, 1953) at 226.

[315] *Corfu Channel, supra* note 300 at 23; *Trail Smelter Arbitration* (*United States v. Canada*), 1938 3 RIAA 1907.

[316] *Chorzow Factory Case*, *supra* note 288 at 21.

[317] *Trail Smelter Arbitration*, *supra* note 315.

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.[318]

Interpreted in an ordinary and plain meaning and read in the context of the Outer Space Treaty,[319] Article IX is an obligation on States to consider legal rights of other States, both prior to and during any ongoing activities.[320] However, "States can disregard any anticipated impact on rights that do not correspond to peaceful use and exploration."[321] In imposing 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) activity is planned by a State or its nationals; (2) the State has reason to believe the

---

[318] *Outer Space Treaty*, *supra* note 275 art VII.

[319] 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 1969. 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 308, art 31.

[320] Mineiro, *supra* note 278 at 334.

[321] *Ibid.*

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.[322] 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,"[323] 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,[324] 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 Project West Ford, which studied the effects of dispersing a network of 500,000 tiny copper metal strips (dipoles) into short-lived orbit on global radio communications.[325] When the project became public, a

---

[322] *Ibid* at 334-335.

[323] *Ibid* at 336.

[324] "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 193, art 1.169.

[325] Mineiro, *supra* note 278 at 337; Irwin I. Shapiro, "Orbital Properties of the West Ford Dipole Belt," online: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1444922&isnumber=31060>.

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.[326] The project was also condemned at the UN by the Soviet Union and several other States.[327]

In 1960, the Academy of Sciences studied the project effects and soon thereafter, the U.S. publically announced Project West Ford would be a short-term project.[328] 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….

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 [329] In response to these concerns, as well as Soviet

---

[326] Delbert R. Terrill, Jr., "The Air Force Role in Developing International Outer Space Law" (Air University Press, May 1999) at 63.

[327] Kathleen Teltsch, "6 Soviet Space Failures Believed To Have Been Probes of Planets" *The New York Times* (16 June 1963).

[328] Terrill, *supra* note 326 at 64.

[329] *Ibid.* at 64-65

Union condemnation over Project West Ford, UN Ambassador Adlai E. Stevenson announced:

> 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.[330]

It is this precedent created by the U.S. that provided the basis for Article IX.[331]

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).[332] Under this classification, interference with satellite signals undoubtedly qualifies 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

---

[330] Maj Norman Thorpe, "The Process of Space Law Development" *International Law Division, USAF, Office of Judge Advocate General,* Paper delivered at Major Command Judge Advocate Conference, Bolling AFB*, D.C.*, 16 November 1967 at 3. online: <http://www.docstoc.com/docs/33978175/The-Air-Force-Role-in-Developing-International-Outer-Space-Law>.

[331] *Ibid.*

[332] Mineiro, *supra* note 278 at 337.

space activities deemed dangerous or potentially hazardous,[333] and at least one State initiated international discussions despite declaring it had no Article IX obligation to do so.[334] 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.[335] 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.[336] If

---

[333] The U.S. 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" (3 Feb 2011), online: <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. Dragon Space, "Britain Concerned by Chinese Satellite Shoot-Down" (19 Jan 2007), online: <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* (19 January 2007), online:< http://news.bbc.co.uk/2/hi/asia-pacific/6276543.stm>.

[334] In 2008, prior to the U.S. shootdown of its satellite, USA-193, the U.S. 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," 14 Feb 2008.

[335] *VCLT, supra* note 308, art 31(b).

[336] Mineiro, *supra* note 278 at 338.

such States' activities are not peaceful, Article IX has not been triggered and there is no duty to undertake international consultations.[337]

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,"[338] others suggest "peaceful" means "non-aggressive" or "non-hostile."[339] 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.[340] State practice[341] also supports the proposition that "peaceful" should be interpreted to mean "non-aggressive" or "non-hostile."[342] There has even been "consensus, within the United Nations that 'peaceful' equates to 'non-aggressive.'"[343] As will be further addressed below, the "UN Resolution on the Definition of Aggression," defines

---

[337] *Ibid.*

[338] Bin Cheng, *Studies in International Space Law* (Oxford: Clarendon Press, 1997) at 520-522.

[339] Schmitt, "Military Operations in Space," *supra* note 51 at 101. In 1962, U.S. Senator Albert Gore, Sr., in comments made to the UN, 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,* UN GOAR, 17th Sess., 1289th Mtg, UN Doc A/C.1/PV.1289 (1962).

[340] Ivan A. Vlasic, "The Legal Aspects of Peaceful and Nonpeaceful Uses of Outer Space" in Bhupendra Jasani ed, *Peaceful and Non-Peaceful Uses of Space, Problems for the Prevention of an Arms Race* (The Netherlands, Kluwer, 1991) 45, 47.

[341] 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 308, art 31(3)(b).

[342] Richard A. Morgan, "Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and "Peaceful Purposes" 60 J Air L & Comm (1994) 237, 303-309.

[343] Walter D. Reed & Robert B. Norris, "Military Use of the Space Shuttle" (1979) 13 Akron L Rev 665 at 678; Christol, *supra* note 312 at 16.

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."[344]

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 Chapter 3), 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,[345] a belligerent State would only be required to conduct "appropriate international consultations" with neutral parties under the Law of Neutrality, when applicable.[346] However, because Article IX only imposes a duty to consult in good

---

[344] *Resolution of the Definition of Aggression*, art 1, GA Res. 3314 (XXIV) UN GAOR, 29th Sess., Supp No 31, UN Doc A/9890 (1974) [*Definition of Aggression*].

[345] Robert Jennings & Arthur Watts, eds, *Oppenheim's International Law* 9th ed (Essex England: Longman Group, 1992) at 302.

[346] The Law of Neutrality was formally established in 1907 by Hague Convention (V). *Hague Convention (V), Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land,* 18 October 1907, 1 Bevans 654. As Article I provides that the territory of neutral State is inviolable, it highlights a question as to whether satellites or signal 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. The Law of Neutrality 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 and 9 relate to telegraph, telephone and wireless telegraphy, 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.

faith,[347] and not a mandate that parties reach a mutually agreeable solution,[348] consultations would solely depend on the nature and extent of the planned activity.[349] 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 to which States should consult in evaluating their activities.[350] 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.[351] 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.[352]

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

[347] Mineiro, *supra* note 278 at 338-339

[348] Jarman *supra* note 60 at 39.

[349] Brandon Hart, "Legal Implications Surrounding Recent Interception of Spy Satellite," Joint Center for Operational Analysis J. 24 (June 2008).

[350] Mineiro, *supra* note 278 at 338.

[351] *Ibid.* at 339.

[352] Li Juqian, "Legality & Legitimacy of China's ASAT Test" (2009) 5:1 China Sec 45 at 48.

ever, gone so far as to declare such an activity 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 military armed conflict.

The foregoing raises one additional provision under the Outer Space Treaty deserving brief discussion. Article IV relates to the militarization 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 thesis will not go into detail 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 discussed, is "peaceful" means "non-aggressive." [353] Second, treaty drafters deliberately and intentionally excluded conventional weapons from the prohibition.[354] Third, Article IV creates only a partial demilitarization of space specifically applicable only during peacetime.[355] This

---

[353] Carl Q. Christol, *The Modern International Law of Outer Space* (New York: Pergamon Press, 1982) at 5.

[354] Michel Bourbonniére & Ricky J. Lee, "Legality of the Deployment of Conventional Weapons in Earth Orbit: Balancing Space Law & the Law of Armed Conflict" (2007) 18:5 EJIL 873 at 882-886.

[355] *Ibid* at 877.

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.[356]

Jamming, which typically involves no direct physical damage, would not cause mass destruction in the same way as a nuclear weapon.[357] Even if it did, the "weapon of mass destruction" might not be in space.[358] For example, 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."[359] 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 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.

---

[356] Maogoto & Freeland, *supra* note 54 at 1105-1106, 1111.

[357] Greenburg, et al, *supra* note 13 at 9.

[358] *Ibid*.

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

Because the UN Charter stipulates obligations under it override obligations under any other international agreement,[360] the Outer Space Treaty is subject to the terms of the UN Charter and must be considered in the broader context of public international law.[361] Therefore, the Outer Space Treaty does not modify any right or obligation within the UN Charter; and since the UN Charter discusses a State's inherent right to self-defense,[362] as long as a State is acting in self-defense, such acts would not violate the Outer Space Treaty, assuming they otherwise complies with the Law of Armed Conflict, 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.[363] However, international law does not specifically address whether sovereignty exists in a satellite signal and no State ever claimed satellite signal interference violated its sovereignty.

Non-intervention is the correlative of state sovereignty, a State's independence to exercise supreme authority over all people and things within its territory.[364] In *Corfu Channel,* the ICJ noted, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[365] The principles of independence

---

[360] *UN Charter*, *supra* note 272, art 103.

[361] Bourbonniére & Lee, *supra* note 354 at 887.

[362] *UN Charter*, *supra* note 272, art. 51.

[363] Jennings & Watt, *supra* note 345 at 429.

[364] Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" (2012) 17:2 J Conflict & Sec L 211 at 222.

[365] *Corfu Channel, supra* note 300 at 35.

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.[366] With a view towards maintaining international peace, the Declaration proclaims:

> [n]o 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."[367] 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 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

---

[366] *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations,* GA Res 2625(XXV), UN GAOR, 25th Sess, Supp No. 18, UN Doc A/8082 (1970) [*Declaration on Friendly Relations*].

[367] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States),* [1986] ICJ Rep 14 at 205 [*Nicaragua*].

> ones…the element of coercion…defines, and intended forms the very essence of prohibited intervention. [368]

An intervention is only wrongful when using methods of coercion.[369] Moreover, because the decisive test remains coercion[370] some academics believe "interference pure and simple is not intervention."[371] It then follows from this assertion, if there is no coercive element, there is no *per se* violation of the non-intervention principle.[372]

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.[373] Likewise, if jamming or spoofing were used to manipulate financial markets, it would constitute prohibited intervention. On the other hand, if jamming or spoofing were 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 International Humanitarian Law (IHL)[374] can

---

[368] *Ibid,* para 205.

[369] *Ibid.*

[370] Schmitt, Michael N. ed, *Tallin Manual on the International Law Applicable to Cyber Warfare* (Cambridge: University Press, 2012) at 45 [*Tallin Manual*].

[371] Jennings & Watts, *supra* note 345 at 432.

[372] *Tallinn Manual, supra* note 370 at 44.

[373] *Ibid.*

[374] William H. Boothby, *The Law of Targeting* (Oxford: University Press, 2012) at 3.

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 or limit the effects of an attack to only military targets.[375] Thus, satellite signal interference aimed at military communications during armed conflict will likely have an impact, perhaps even a severe impact, on civilian communications, which 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 100 cellular networks were shutdown, taking hours and even days to recover.[376] 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,

[375] Droege, *supra* note 112 at 7.

[376] Bruce Carlson, "Protecting Global Utilities: Safeguarding the Next Millennium's Space Based Public Services" (2000) Aerospace Power J 37 at 38.

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 thesis, the basic sources of IHL and several primary principles will be briefly discussed to provide a basic understanding of implications emerging due to using intentional interference 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.[377] 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.[378] In simple terms, Hague treaties address the behavior of belligerents and the means and methods of warfare including the lawfulness of weapons and targeting,[379] 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.[380]

---

[377] Steven Freeland, "In Heaven as on Earth – The International Law Regulation of the Military Use of Outer Space" (March 2011) 8 US-China L Rev 272 at 278.

[378] *Ibid* at 280.

[379] *Regulations respecting the Laws and Customs of War on Land, Annex to Hague Convention (IV),* 18 October 1907, 36 Stat. 2295.

[380] *Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Conflicts (Protocol I*), 8 June 1977, 1125 U.N.T.S. 3, [*API*].

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 within any armed conflict.[381] The UN Security Council also demands strict compliance with IHL obligations during armed conflicts.[382] It is important to emphasize that it is only in the context of an armed conflict (an international armed conflict (IAC)[383] or a non-international armed conflict (NIAC)[384]) that IHL rules apply.[385]

While a discussion of the criteria for and rules specific to IACs and NIACs is beyond the scope this thesis,[386] classifying a conflict is necessary to determine the specific legal regime applicable to that conflict[387] and the rules governing targeting decisions.[388] 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 an NIAC, the rules applicable to NIAC would apply.

---

[381] *Legality of the Threat or Use of Nuclear Weapons Case,* Advisory Opinion, [1996] ICJ Rep 226 at 79 [*Nuclear Weapons*].

[382] *Protection of Civilians in Armed Conflict,* SC Res 1674, UN SCOR, 2006, 5430th Mtg, UN Doc S/RES/1674 (2006) at para 6.

[383] An international armed conflict exists whenever there are hostilities, declared war or any other armed conflict between two or more States. *API, supra* note 380, art 2.

[384] A non-international armed conflict exists whenever there are hostilities, declared war or any other armed conflict between governmental armed forces and the forces of one or more groups or between such groups. *API, supra* note 380, art 3.

[385] Droege, *supra* note 112 at 7. Boothby, *supra* note 374 at 388.

[386] For a thorough discussion as to what rules apply to IACs and NIACs and in the spectrum of conflict, see Boothby, *supra* note 374 at 43-54, 429-454.

[387] Michael N. Schmitt, "Classification of Cyber Conflict" (2012) 17:2 J Confl & Sec L 245.

[388] Boothby, *supra* note 374 at 43.

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.[389] Additionally, IHL, does not prohibit disseminating propaganda or economic sanctions deliberately targeting the military and civilian populations.[390] 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 Chapter 4, 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.[391] 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.[392] For a target to constitute a

---

[389] Droege, *supra* note 112 at 27.

[390] Boothby, *supra* note 374 at 43.

[391] Yoram Dinstein, "Legitimate Military Objectives under the Current Jus in Bello" in A.E. Wall ed, *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Newport RI: Naval War College, 2002) 139 at 140.

[392] *Law of War Deskbook*, International and Operational Law Department, (Charlottesville, Virginia: The Judge Advocate General's Legal Center and School, 2001) 139-140. Boothby, *supra* note 374 at 59.

legitimate military objective, the responsible decision maker must determine, based on information reasonably available, that objects "by their nature, location and purpose of use make an effective contribution to military action…or offers a definite military advantage" and that its "total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[393] Attacks against civilian objects are prohibited as attacks traditionally associated with civilian use.[394] 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.[395] Such objects must have an inherent attribute or character that contributes to military action.[396] 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, GPS satellites as well as remote sensing satellites.[397] 'Location' refers to "objects which by

[393] *API, supra* note 380*,* art. 52.

[394] *Ibid*, art 52(1) & (3).

[395] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: University Press, 2012) at 185. *Law of War Deskbook*, *supra* note 392 at 141-142.

[396] *Ibid.*

[397] Jarman, *supra* note 60 at 50.

their very nature have no military function but which, by virtue of their location, make an effective contribution to military action."[398] 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.[399] With commercial communication satellites, this means because such objects make an effective contribution to the military at all times, and especially in armed conflict, as demonstrated during the Iraq War, 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.

---

[398] Yves Sandoz, Christophe Swinarski & Bruno Zimmerman eds, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (The Netherlands: Martinus Hijoff, 1987) at para 2021.

[399] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* 2d ed (Cambridge: University Press, 2010) at 89.

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.[400] This principle, appearing first in 1868 within the preamble of the St. Petersburg Declaration,[401] but now codified in Article 48 of Protocol I of the Geneva Convention of 1949, 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 objects and military objectives and accordingly shall direct their operations only against military objectives.[402]

According to Article 52 of Protocol I, civilian objects are defined as "all objects which are not military objectives."[403] Combatants must always distinguish themselves

---

[400] Boothby, *supra* note 374 at 60.

[401] *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight,* 11 December 1868, online: ICRC < http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=568842C2B90F4A29C12563CD0051547C>.

[402] *API, supra* note 380*,* art. 48.

[403] *Ibid,* art. 52(1).

from civilians, and civilian objects must not be mistaken for military targets.[404] 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 civilians population, civilians and civilian objects."[405] 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.[406] However, 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.[407] Thus, when commercial satellite signals qualify as valid military targets, but collateral effects expected are excessive in relation to military necessity, a violation of the Law of Armed Conflict occurs.

Under Article 51(4), of Protocol I of the Geneva Convention of 1949, indiscriminate attacks are prohibited.[408] 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."[409] With respect to satellite signal interference and discrimination, many technologies used and employed to jam satellite signals may not be

---

[404] *API, supra* note 380*,* art. 57. *Prosecutor v. Kupreskic*, IT-95-16-T, Trial Chamber Decision (14 January 2000) at para 521 (International Criminal Tribunal for the Former Yugoslavia).

[405] *Ibid*, art. 57(1).

[406] Bourbonniére*, "*Law of Armed Conflict," *supra* note 190 at 48.

[407] *API, supra* note 380, art. 51.5(b), 57.2(a), and 57.2(b).

[408] *API, supra* note 380, art. 51(4).

[409] Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law Rules* (Cambridge: University Press, 2009) at 43.

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.

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"[410] 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 the law of armed conflict. 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.

[410] The "fog of war" refers to the uncertainty in situational awareness that arises during war. Carl von Clausewitz, *On War* (Princeton, New Jersey: Princeton University Press, 1976) at 20.

3. The Principle of Proportionality

The principle of proportionality limits attack effects by requiring belligerents to establish a balance between military and humanitarian interests.[411] 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.[412] Proportionality requires a balancing of anticipated military advantage against anticipated damage caused.[413] 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 possible, choose objectives that will "cause the least danger to civilians."[414] 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.[415] 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, it does not in all circumstances constitute a violation of international law.[416]

---

[411] Bourbonniére, "Law of Armed Conflict," *supra* note 190 at 47.

[412] *API, supra* note 380, art 51(5)(b).

[413] *API, supra* note 380, art 57(2). Robert A. Ramey, *Space Warfare and the Future Law of War* (LL.M. Thesis, McGill University Institute of Air and Space Law, 1999) at 58.

[414] *API, supra* note 380, art 57(2).

[415] *API, supra* note 380, art 35 (1)-(2), 85.

[416] Freeland *supra* note 377 at 281. See *Nuclear Weapons, supra* note 381 at 42.

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 1990-1991 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 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.[417]

The bombing of the Iraqi electrical grid clearly suggests commercial communication satellites will be targeted in future conflicts, in lieu of kinetic attacks; 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 signal 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

[417] Yoram Dinstein "Discussion" in A.E. Wall, ed, *Legal and Ethical Lessons of NATOS's Kosovo Campaign* (Newport RI: Naval War College, 2002) 211 at 219.

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.

Chapter Three: Intentional 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 chapter 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 Threat or the 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 mankind."[418] 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[419] and reaffirms the duty of

[418] *UN Charter*, *supra* note 272, preamble.

[419] Ian Brownlie, *International Law and the Use of Force* (Oxford: Clarendon Press, 1963) 112-113 [Brownlie, *Use of Force*].

States to resolve all international disputes through "peaceful means in such a manner that international peace and security…are not endangered."[420]

The principle prohibiting the "threat or use of force" by States is considered *jus cogens*[421] and is an obligation *erga omnes*.[422] The ICJ has opined that the principle is also binding on all States as a customary norm.[423] The prohibition against the "use of force," the scope of which remains hotly contested,[424] is also codified in Article 2(4) of the UN Charter. Article 2(4) is the key prescription in international law regarding the use of force.[425]

Article 2(4), described as "the corner stone of peace"[426] and as "the heart of the United Nations Charter"[427] 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.[428]

---

[420] *UN Charter*, *supra* note 272, art 2(3).

[421] *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* 6th ed (Oxford: University Press, 2003) at 489.

[422] *Erga omnes* obligations are owed to the international community as a whole. *Case concerning the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain),* Judgment, [1970] ICJ Rep 3 at 32.

[423] *Nicaragua, supra* note 367 at 190.

[424] Maogoto & Freeland, *supra* note 54 at 1105.

[425] Michael N. Schmitt, "Computer Network Attack & the Use of Force in International Law: Thoughts on a Normative Framework" (1999) 37 Colum J Transnat'l L 885 at 900 [Schmitt*, "*Computer Network Attack"].

[426] Sir Claud Humphrey Meredith Waldock, *The Regulation of the Use of Force by Individual States in International Law* (Hague Recueil, 1952) at 492.

[427] Louis Henkin, "The Reports of the Death of Article 2(4) are Greatly Exaggerated" (1971) 65 Am J Int'l L 544.

[428] *UN Charter*, *supra* note 272, art 2(4).

This prohibition is complimented by the customary norm of non-intervention, which, as addressed above, dictates States must not directly or indirectly interfere with the internal affairs of other States.[429] 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).[430]

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.[431] 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 (CNAs).[432] 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 UN Charter.[433]

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[434] and (2) actions taken in

---

[429] *Manila Declaration on the Peaceful Settlement of International Disputes,* GA Res 37/10, UN GAOR 68th Sess, UN Doc A/RES/37/10 (1982); *Declaration on Friendly Relations, supra* note 366.

[430] *Nicaragua, supra* note 367 at 209.

[431] Bruno Simma, ed, *The Charter of the United Nations: A Commentary,* 2d ed (Oxford: University Press, 2002) at 117-118.

[432] Walter G. Sharp, *Cyber Space and the Use of Force* (Falls Church, Virginia: Aegis Research, 1999) at 130-133, arguing that United States national policies indicate a wide range of cyber activities should fall within the prohibition of Article 2(4).

[433] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts" in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010* (Washington, DC: National Research Council, 2010) 151 at 153 [Schmitt, "Cyber Operations"].

[434] *UN Charter*, *supra* note 272, chapt 7.

self-defense in response to an "armed attack."[435] 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 Chapter 4, the prohibition on the use of force must be clarified.

1. Defining the Use of Force

Article 2(4) renders only specific uses of force wrongful.[436] While the notion of force is disputed,[437] some suggest the proper view is that "force" denotes "*armed force*,"[438] meaning a "resort to a violent weapon that inflicts human injury."[439] Consistent with this view, armed force also includes all activities related to military action, from the transfer of soldiers and tanks to country borders, to the act of war, including dropping bombs and firing artillery.[440] 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.[441]

---

[435] *UN Charter*, *supra* note 272, art 51.

[436] Schmitt, "Computer Network Attack," *supra* note 425 at 900.

[437] *Ibid* at 904; Simma, *supra* note 431 at 117.

[438] Brownlie, *Use of Force, supra* note 419 at 362; Yoram Dinstein, *War, Aggression and Self-Defence,* 4th ed (Cambridge: University Press, 2005) at 86[*War, Aggression and Self-Defence*]; Schmitt, "Computer Network Attack," *supra* note 425 at 904.

[439] Christopher C. Joyner & Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework" (2001) 12 Eur J Int'l L 825 at 845.

[440] Isavella Maria Vasilogeorgi, *Military Uses of Outer Space: Legal Limitations, Contemporary Perspectives Laws* (LL.M. Thesis, McGill University Institute of Air and Space Law, 2011) at 17.

[441] Simma, *supra* note 431 at 118; *Declaration on Friendly Relations, supra* note 366.

Ultimately, international law perceives the unlawful recourse to the unlawful use of force as an act of "aggression."[442] While there is no legally binding definition of "aggression," UN General 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 (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."[443] 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 invasions, bombardments, and naval blockades.[444] Under Article 4, however, Resolution 3314 does not limit acts of aggression to those only coming from uses of *armed* force.[445]

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.[446] 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 found in the case of *Nicaragua v. United States*.[447] In *Nicaragua*, the International Court

---

[442] Bourbonniére, "Clausewitz Nebulae," *supra* note 290 at 245].

[443] *Definition of Aggression, supra* note 344, art 1.

[444] *Ibid,* art 3.

[445] Noah Weisbord, "Conceptualizing Aggression" (2009) 20 Duke J Comp & Int'l L 1 at 37.

[446] Simma, *supra* note 431 at 119.

[447] *Ibid* at 119-120.

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.[448]

Even though the ICJ did little to clarify the scope of the prohibition on the use of force regarding assisting subversive activities,[449] the ICJ established the use of force includes actively and directly preparing and assisting others to apply armed force.[450]

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 narrower.[451] 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 forms of the use of force."[452] 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."[453] According to Professor Michael Schmitt, the phrase "scale

---

[448] *Nicaragua*, *supra* note 367 at 119.

[449] Simma, *supra* note 431 at 121.

[450] Schmitt, "Computer Network Attack," *supra* note 425 at 909.

[451] Yoram Dinstein, "Computer Network Attacks and Self-Defense" (2002) 76 Int'l L Stud 99, at 100-101 ["CNAs and Self-Defense"].

[452] *Nicaragua*, *supra* note 367 at 191.

[453] *Ibid* at para 195.

and effects" is simple shorthand for the quantitative and qualitative factors considered when determining whether a certain action qualifies as a use of force.[454]

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.[455] 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.[456] 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."[457] Beyond confirming the threshold test in *Nicaragua,* however, the court did nothing to clarify the "most grave forms" of force from those less grave.[458] Accordingly, beyond the requirement that a use of force must be "grave," the parameters of the "scale and effects" criteria remain unsettled.[459]

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.[460] In other words, the issue is not the type of weapon

---

[454] Schmitt, "Computer Network Attack," *supra* note 425 at 915.

[455] *Nicaragua, supra* note 367 at 191.

[456] *Ibid* at para 195.

[457] *Ibid* at para 191.

[458] Andrew Garwood-Gowers, "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," Case Note (2004) 5 Melbourne J Int'l L 241 at 249-251.

[459] *Tallinn Manual, supra* note 370 at 55.

[460] *Nuclear Weapons Case, supra* note 381 at 39.

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 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[461] 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."[462]

---

[461] Brownlie, *Use of Force, supra* note 419 at 362.

[462] Schmitt, "Cyber Operations," *supra* note 433 at 154; Joyner & Lotrionte, *supra* note 439 at 845.

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 Chapter 4.

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 exiting 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 computer network attacks (CNAs).

1. Current Debates over the Application of *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.[463] 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 as well as 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

[463] Oona A. Hathaway, et al, "The Law of Cyber Attack" (2012) 100 Cal L Rev 817 at 845.

characteristics traditionally associated with military coercion."[464] 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.[465] The instrument-based approach "seeks to regulate the conflicts of yesterday,"[466] devoid of modern infrastructure, targets, weapons, capabilities, and is thus wholly inadequate in the modern world.[467]

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."[468] According to Hollis, the target-based approach focuses on determining when a State may respond in self-defense.[469] Under this approach, the mere identity of a target can authorize forceful self-defense.[470] 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, however, expands the right of self-defense significantly, and in doing so, could threaten international peace and security by making armed conflict more likely.[471]

---

[464] Duncan B. Hollis, "Why States Need an International Law for Information Operations" (2007) 11 Lewis & Clark L Rev 1023 at 1041.

[465] Kanuck, *supra* note 55 at 288-289.

[466] *Ibid* at 290.

[467] Hollis, *supra* note 464 at 1041-1042.

[468] *Ibid* at 1041.

[469] *Ibid*.

[470] *Ibid*.

[471] Hathaway, et al, *supra* note 463 at 847.

The effects-based approach, the most compelling and widely accepted of the three, focuses on the consequences or effects of the act.[472] This approach assesses whether the act in question causes effects equivalent to those produced by military force (damage to property or death).[473] 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.[474]

The most well-known proponent of the effects-based approach is Professor Michael N. Schmitt. Professor Schmitt 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.[475] These factors, deriving from that which historically made military force special in international law,[476] 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:

---

[472] *Ibid.*

[473] Hollis, *supra* note 464 at 1041.

[474] Schmitt, "Cyber Operations," *supra* note 433 at 155.

[475] Michael N. Schmitt, "'The Use of Force' in Cyberspace: A Reply to Dr. Ziolkowski," (Paper delivered at the 2012 4th International Conference on Cyber Conflict) (2012) NATO CCD COE Publications, Tallinn 311 at 314.

[476] Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)" (2011) 36:42 Yale J Int'l L 421 at 432.

determining whether the act is unlawful; and (7) responsibility: the extent to which a State is involved in an act.[477]

These factors have also been formally recognized by an International Group of Experts[478] in the *Tallinn Manual on the International Law Applicable to Cyber Warfare* as that which States will likely consider when characterizing whether a non-kinetic act (CNA) is a use of force.[479] 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:

1) 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 of 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.

2) 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.

3) 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.

---

[477] Schmitt, "Computer Network Attack," *supra* note 425 at 914-915: Schmitt, "Cyber Operations," *supra* note 433 at 155-156.

[478] 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 includes 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 370 at 1, 9.

[479] *Ibid* at 48.

4) 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.

5) 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.

6) 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.

7) 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.

8) 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.[480]

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.[481] 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.[482] If the assessment reveals the consequences at issue fall outside the use of force

[480] *Ibid* at 48-51. See also Harrison Dinniss, *supra* note 395 at 63-64.

[481] Schmitt, "Cyber Operations," *supra* note 433 at 157.

[482] Schmitt, "Computer Network Attack," *supra* note 425 at 915.

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.[483]

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 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 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

[483] *Ibid.*

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 satellite(s), 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 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 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, governmental and public services,[484] 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

[484] Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution" (2012) 12:2 J Confl & Sec L 229 at 231.

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."[485] 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, 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

[485] Joyner & Lotrionte, *supra* note 439 at 865.

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. In such matters, a State might be described as not entitled to assert a right of armed self-defense under Article 51 of the Charter. As such, 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, or take the matter before the UN 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 organization 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.[486] 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 Chapter 2, Member States are obligated to comply with ITU provisions and cooperate with others in eliminating harmful interference. [487]

[486] *Tallin Manual, supra* note 370 at 43-44.

[487] See *ITU Radio Regulations*, *supra* note 193, arts, 11.42, 11.42A, 15.21 §13; See also Jakhu, "Satellites," *supra* note 4.

Additionally, under ISL, States bear international responsibility for national activities in outer space.[488]

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 Article VI of the Outer Space Treaty, where acts can always be attributed to States, the difficulty is establishing a sufficient enough link between the State and the non-State entity or actor committing the unlawful act.[489]

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."[490] 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 pin-point the precise source of the interference in a timely manner. What is 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."[491]

The problem of attribution is not limited to acts of intentional interference. It is one of the biggest difficulties associated with CNAs.[492] Such a challenge also extends to

---

[488] *Outer Space Treaty, supra* note 275, art VI.

[489] Malcolm N. Shaw, *International Law* 5th ed (Cambridge: Univeristy Press, 2003) at 701.

[490] *Nicaragua, supra* note 367 at 119-120.

[491] Tsagourias, *supra* note 484 at 233.

[492] Harrison-Dinnis, *supra* note 395 at 99-100.

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.[493] There are also issues of attribution with State-sponsored terrorism activities when the State fails to take responsibility for its role.[494] Nevertheless, in every case, a victim State must establish attribution to a State.

While this thesis 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.[495] Despite this disagreement, a State may not knowingly allow "its territory to be used for acts contrary to the rights of other states"[496] nor can its territory be used for military acts against another State.[497] 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.[498]

In the *Congo v. Uganda* 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.[499] In the *Oil Platforms* case, however, the ICJ effectively held the burden of proof

---

[493] *Ibid* at 100.

[494] *Ibid.*

[495] *Ibid* at 101.

[496] *Corfu Channel, supra* note 300 at 22.

[497] *The Alabama Claims (United States v. Great Britain)* [1872] reprinted in JB Moore, *History and Digest of International Arbitrations to which the United States has been a Party,* Vol 1 (GPO 1898) 495.

[498] Ian Brownlie, "International Law and the Activities of Armed Bands" (1958) 7 Int'l & Comp L Quarterly 712 at 734, cited in Harrison-Dinniss, *supra* note 395 at 101.

[499] *Case Concerning Armed Activities on the Territory of the Congo (Congo v. Uganda),* [2005] ICJ Rep 168, para 301.

rests on the State invoking the right of self-defense.[500] 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."[501] The Court endorsed circumstantial evidence as sufficient, as long as the proof derives from inferences of fact, and those facts do not leave room for reasonable doubt.[502] Thus, "a State should not resort to self-defense on the basis of casual evidence or wild political inferences."[503]

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 those acting under the direction of the State.[504] This would include all individuals or collective entities, making up the organization of the State and acts on its behalf,[505] 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[506] or with agreement of the UN Security Council.

---

[500] *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States),* [2003] ICJ Rep 161 at 57, 61 [*Oil Platforms Case*].

[501] *Corfu Channel, supra* note 300 at 18.

[502] *Ibid.*

[503] Tsagourias, *supra* note 484 at 235.

[504] James Crawford, ed *The International Law Commission's Articles on State Responsibility, Introduction, Text and Commentaries* (Cambridge: University Press, 2001) at 81-85 [*ASR Commentaries*].

[505] *Ibid.*

[506] Tsagourias, *supra* note 484 at 236.

Attacks can also be attributed to a State if they are conducted by State organs,[507] controlled by the State,[508] or due to the State's intentional failure to prevent the attack.[509] 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.[510] In the *Nicaragua* case, the ICJ attributed acts committed by organs of the U.S. to the U.S. but also noted there was insufficient evidence the U.S. had actual control "in all fields as to justify treating the *contras* as acting on its behalf."[511] The ICJ also noted, even though some fields conducted by the *contras* forces were highly dependent on the U.S., they nonetheless did not constitute *de facto* control by the U.S.[512] The ICJ reached a similar conclusion in the *Bosnia Genocide Case.*[513]

Additionally, in the *Tehran Hostages Case*, the ICJ held, to attribute the occupation of the U.S. Embassy by militants to the State of Iran, the U.S. 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.[514] Without launching into the intricacies of these decisions, for attacks to be attributed to a State under international law, the State had to

---

[507] *ASR*, *supra* note 267, art 4.

[508] *Ibid,* art 8.

[509] Tsagourias, *supra* note 484 at 236.

[510] *Ibid.*

[511] *Nicaragua, supra* note 367 at 109.

[512] *Ibid,* para 111.

[513] *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia & Herzegovina v. Serbia),* [2007] ICJ Rep 43 at 399-401 [*Crime of Genocide (Bosnia & Herzegovina)*].

[514] *United States Diplomatic and Consular Staff in Tehran (United States v. Iran)* [1980] ICJ Rep 3 para 58.

have issued specific instructions or directed or controlled the operation.[515] Then, in the *Tadic* 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.[516] Additionally, in the *Tadic 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.[517] In a subsequent decision, the ICJ distinguished the "overall control" test from that conducted for the purpose of establishing State responsibility.[518]

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.[519] If the interference attack cannot be attributed to a State, but is carried out by a non-State actor, the non-State actor can become the target of the Victim State's self-defense action.[520] 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."[521]

---

[515] *ASR*, *supra* note 267, art 8.

[516] *Prosecutor v. Dusko Tadic*, IT-94-1, Judgment (15 July 1999) at para 120 (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber).

[517] *Ibid* at para 132.

[518] *Crime of Genocide (Bosnia & Herzegovina),supra* note 513 at paras 403-405.

[519] Tsagourias, *supra* note 484 at 244; *ASR Commentaries*, *supra* note 504, 81-85.

[520] Tsagourias, *supra* note 484 at 244.

[521] *Nicaragua, supra* note 367 at 176, 196; *Nuclear Weapons Case, supra* note 319 at 41; *Oil Platforms Case, supra* note 431 at 74.

Chapter Four: Lawful Responses to Satellite Signal Interference

Having discussed satellite signal interference as un 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 UN Charter, this Chapter 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 UN Charter. Finally, this Chapter addresses responses available to States under the UN Charter framework, namely actions and measures authorized by the UN 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 (ASR).[522] Reparations can take the form of restitution, compensation, or satisfaction, either singly or in combination.[523] 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.[524] An injured State may also take responsive measures neither amounting to a use of force nor breaching any existing treaty or customary law

[522] *ASR*, *supra* note 267, art 31.

[523] *ASR*, *supra* note 267, art 34.

[524] *ASR Commentaries, supra* note 504 at 211-212.

obligation,[525] 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,[526] including severing diplomatic relations, imposing trade embargos, 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.[527]

Formerly known as reprisals,[528] 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."[529] In other words, countermeasures are peaceful measures, falling outside the scope of accepted exceptions of Article 2(4) of the UN Charter, used to enforce international law.[530] The purpose of countermeasures is to induce a wrongdoing State to comply with its international obligations,[531] not to create new non-rectifiable situations.[532]

---

[525] Schmitt, "Cyber Operations," *supra* note 433 at 159.

[526] Retorsions are lawful unfriendly acts made in response to violations of international law. *ASR Commentaries, supra* note 504 at 281-282.

[527] *Ibid.*

[528] Shaw, *supra* note 489 at 708.

[529] *ASR Commentaries, supra* note 504 at 168-169.

[530] Elena Katselli Proukaki, *The Problem of Enforcement in International Law* (New York: Routledge, 2010) at 68.

[531] *ASR Commentaries, supra* note 504 at 284-287.

According to the ICJ in the *Gabcikovo-Nagymaros* case, specific prerequisites and conditions apply for countermeasures to be justified and lawful.[533] 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.[534] Additionally, the injured State must have called upon the offending State to make reparation for it.[535] Countermeasures must also be proportionate to the act and reversible.[536] Finally, countermeasures must be terminated as soon as the responsible State complies with its obligations.[537]

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.[538] Other unlawful acts include those violating other preemptory norms of international law and those violating humanitarian obligations of a State.[539] Additionally, countermeasures are not to be used as a form of punishment.[540] They are only to be used to vindicate injured States' rights and restore the legal relationship with the responsible State to normalcy.[541]

---

[532] *Ibid.*

[533] *The Case Concerning the Gabcikovo-Nagymaros Project (Hungary v. Slovakia),* [1997] ICJ Rep 7 at 55-57.

[534] *Ibid* at 55.

[535] *Ibid* at 55-57.

[536] *Ibid.*

[537] *ASR Commentaries, supra* note 504 at 286.

[538] *ASR*, *supra* note 267, art 50(1) (a-b).

[539] *Ibid,* art 50(1) (c-d).

[540] *ASR Commentaries, supra* note 504 at 281-287.

[541] *Ibid.*

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.[542] Thus, whenever satellite signal interference is unlawful, a victim State may respond by employing countermeasures.

As previously concluded above, 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[543] 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."[544] In each of these instances, satellite signal interference qualifies as an internationally unlawful act justifying a 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

[542] *ASR*, *supra* note 267, art 49.

[543] 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 367, para 108.

[544] *Corfu Channel, supra* note 300 at 22.

act despite its duty to do so. Thus, when a State suspects attribution 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.[545] The principle of necessity reflects the corrective function to achieve compliance,[546] as well as the purpose of preserving the rights of the injured State.[547] 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.[548] 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.[549] In some situations, however, an injured State "may take such urgent countermeasures as are necessary to preserve its rights"[550] without notifying the wrongdoing State of its intention to do so.[551]

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 black out in communications or led to a loss in critical State services. In either case, a State may resort to an urgent countermeasure to prevent further harm or injury. This would not only

---

[545] *ASR Commentaries, supra* note 504 at 294-296

[546] *Ibid* at 288-293.

[547] *Ibid.*

[548] *ASR*, *supra* note 267, art 52(1).

[549] *Ibid,* art 52(2).

[550] *Ibid.*

[551] *ASR Commentaries, supra* note 504 at 298-299.

qualify as a reasonable use of an urgent countermeasure, but would also prevent the incident from escalating into a situation, if left unaddressed, could ultimately rise to the level of an armed attack, and thus a full blown armed conflict.

Under countermeasures, the principle of proportionality is assessed in quantitative and qualitative terms.[552] Proportionality requires countermeasures be "commensurate with the injury suffered taking into account the gravity of the internationally wrongful act and the rights in question."[553] 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.[554]

In responding to satellite signal interference, a victim State could, but is not required to, employ interference as a reciprocal countermeasure.[555] 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

---

[552] *ASR Commentaries, supra* note 504 at 294-296.

[553] *ASR*, *supra* note 267, art 51.

[554] *ASR Commentaries, supra* note 504 at 282-283.

[555] *Ibid.*

creates a new breach of international law.[556] 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 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 provided for in the UN Charter, or in treaties in force.[557] The Court also issues advisory opinions to legal questions.[558] 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

---

[556] *ASR Commentaries, supra* note 504 at 286.

[557] *Statute of the ICJ*, *supra* note 282, art 36.

[558] *Ibid.*

the Court's authoritative views on important issues of international law.[559] 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.[560] 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) of the UN Charter, States are prohibited from using force or threatening to do so in the course of their international relations. The only accepted exceptions explicitly permitted by the Charter are measures authorized by the UN Security Council[561] and actions taken in self-defense.[562]

1. Measures Authorized by the UN Security Council

Pursuant to Article 24 of the UN 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,

---

[559] Pieter H.F. Bekker, "The UN General Assembly Requests a World Court Advisory Opinion on Israel's Separation Barrier" (December 2003) American Soc Int'l L Insights.

[560] *Monetary Gold Removed from Rome in 1943 (Italy v. France, United Kingdom and United States),* Preliminary Question, [1954], ICJ Rep 32.

[561] *UN Charter*, *supra* note 272, chapt 7.

[562] *Ibid,* art 51.

VII, VIII and XII of the UN Charter, 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).[563] On the legal basis of Chapter VII, the UN Security Council authorized armed action in Korea in 1950,[564] the Arab/Israel War in 1956,[565] Iraq in 1990,[566] Darfur in 2006,[567] Libya in 2011 and Mali in 2012.[568]

However, before the Security Council can adopt any enforcement measure, armed or otherwise, it must, under Article 39 of the UN Charter "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."[569] The range of incidents the Security Council determined as giving rise to "threats to the peace" or "a breach to the peace" is plenty and has involved country specific situations such as inter-State[570] and intra-State conflicts,[571] terrorists' acts,[572] the

[563] *Ibid,* chapt 7.

[564] UN SCOR, UN Doc. Res S/RES/83 (1950).

[565] UN SCOR, UN Doc. Res S/RES/1000 (1956).

[566] UN SCOR, UN Doc. Res S/RES/678 (1990).

[567] UN SCOR, UN Doc. Res S/RES/1706 (2006).

[568] UN SCOR, UN Doc. Res S/RES/1973 (2011).

[569] *UN Charter*, *supra* note 272, art 39.

[570] By resolution 1291 (2000) of 24 February 2000, the UN Security Council noted 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. UN SCOR, UN Doc. Res S/RES/1291 (2000). By resolutions 1497 (2003) of 1 August 2003 and 1509 (2003) of 19 September 2003, the UN 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". UN SCOR, UN Doc. Res S/RES/1497 (2003); UN SCOR, UN Doc. Res S/RES/1509 (2003).

proliferation of weapons of mass destruction[573] or internal conflicts with a regional dimension.[574]

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."[575] 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),[576] a "breach of the peace" is often characterized by hostilities between the armed units of States.[577] However, the UN

---

[571] By resolution 660 (1990) of 2 August 1990, the UN Security Council determined that there existed "a breach of international peace and security with regards to the Iraqi invasion of Kuwait." UN SCOR, UN Doc. Res S/RES/660 (1990).

[572] By resolution 1636 (2005) of 31 October 2005, the UN Security Council determined that the terrorist act that killed former Prime Minister of Lebanon Rafiq Hariri, as well as the act's implications, constituted a threat to international peace and security. UN SCOR, UN Doc. Res S/RES/1636 (2005).

[573] By resolution 1718 (2006) of 14 October 2006, 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". UN SCOR, UN Doc. Res S/RES/1718 (2006).

[574] "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*, online: United Nations, < http://www.un.org/en/sc/repertoire/actions.shtml>. By resolution 1295 (2000) of 18 April 2000, the Council determined that the continuing conflict in Angola constituted "a threat to international peace and security in the region". UN SCOR, UN Doc. Res S/RES/1295 (2000).

[575] *UN Charter*, *supra* note 272 art 39.

[576] Schmitt, "Cyber Operations," *supra* note 433 at 161.

[577] Simma, *supra* note 431 at 721.

Security Council has also found deliberate targeting of civilian populations as well as systematic, flagrant, and widespread violations of international humanitarian and human rights law as threats international peace and security.[578]

As to when the UN Security Council might declare satellite signal interference a "threat or breach of the peace," that is uncertain. 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 as well is unknown because the Security Council enjoys considerable discretion when making determinations.[579] As noted by Professor Schmitt, a "threat to the peace" is a political decision, not a legal one.[580] In other words, it is whatever the Security Council decides it to be.[581]

With this understanding, the question becomes, under what circumstances might the UN 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

---

[578] For example, by resolution 1769 (2007) of 31 July 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, the Sudan, continued to constitute "a threat to international peace and security." UN SCOR, UN Doc. Res S/RES/1769 (2007). Additionally, by resolution 1778 (2007) of 25 September 2007, the Council expressed the gravest concern that the situation in the region of the border between the Sudan, Chad and the Central African Republic constituted "a threat to international peace and security." UN SCOR, UN Doc. Res S/RES/1778 (2007). By resolution 1078 (1996) of 9 November 1996, 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. UN SCOR, UN Doc. Res S/RES/1078 (1996).

[579] *ICTY Tadic, supra* note 516 at 28.

[580] Schmitt, "Cyber Operations," *supra* note 433 at 161.

[581] *Ibid.*

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.[582] For instance, if any one of the five permanent members of the Security Council has an interest in the act of satellite signal interference under consideration and exercises their right to veto, pursuant to Article 27, it would block all but procedural resolutions of the Council.[583]

However, because the use of force, aggressions and acts of violence always presume "a breach of the peace," [584] 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, this 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,[585] a "threat to the peace" determination could be made.

If the Security Council determines peace is threatened, that alone is sufficient to take action as necessary under Articles 41 and 42 of the UN Charter. Such measures may even be preceded by provisional action taken under Article 40 to prevent aggravation of the situation[586] and induce negotiations. Regardless, once the Security Council decides an incident constitutes a threat to international peace and security, breach of the peace or

---

[582] Shaw, *supra* note 489 at 1120.

[583] *UN Charter, supra* note 263, art 27.

[584] Simma, *supra* note 431 at 721.

[585] *Ibid*.

[586] *UN Charter, supra* note 263, art 40.

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."[587] 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 using satellite signal interference as causing physical damage and human injury.[588] Regardless, the UN 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.[589] 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

---

[587] *Ibid*, art 41.

[588] Relying on Schmitt, "Cyber Network Attack," *supra* note 425 at 912.

[589] *UN Charter, supra* note 263, art 42.

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.

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 court recognized the right of self-defense in Article 51 refers to pre-existing customary law.[590] 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.[591]

While States have the inherent right to 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.[592] 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,

---

[590] *Nicaragua, supra* note 367 at 176.

[591] *UN Charter, supra* note 272, art 51.

[592] Simma, *supra* note 431 at 793.

however, armed attacks constitute the "most grave forms of the use of force."[593] 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 on-going 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 signal 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.[594] The ICJ has also repeatedly recognized self-defense warrants only those measures "proportional to the armed attack and necessary to respond to it" and is a

[593] *Nicaragua, supra* note 367 at 191.

[594] Christine Gray, *International Law and the Use of Force* (Oxford: University Press, 2000) at 120-121.

well-established principle in customary law. [595] 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."[596] That is, the force used must be timely,[597] necessary to halt and repel the attack,[598] and non-forcible measures must be either futile or have been exhausted in an unsatisfactory manner.[599] The principle of proportionality addresses the issue of how much force is permissible.[600] 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.[601] 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.[602]

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

---

[595] *Nicaragua, supra* note 367 at 176, 196; *Nuclear Weapons, supra* note 319 at 41; *Oil Platforms, supra* note 431 at 74.

[596] *Oil Platforms, supra* note 4500 at 73.

[597] Dinstein, *War, Aggression and Self-Defence*, *supra* note 438 at 210.

[598] Gray, *supra* note 513 at 121.

[599] Dinstein, "CNAs and Self-Defense," *supra* note 451 at 109.

[600] Schmitt, "Cyber Operations," *supra* note 433 at 167.

[601] *Ibid.*

[602] Harrison-Dinnis, *supra* note 395 at 104.

including 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 Chapter Two, 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 ever employed, 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 Chapter Two, 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.

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 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) of the UN Charter 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, 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.

Bibliography

A. Treaties, Agreements and Conventions (Chronologically in Ascending Order)

International Convention for the Protection of Submarine Telegraph Cables, signed at Paris, 14 March 1884, online: <http://iscpc.org/information/Convention_on_Protection_of_Cables_1884.pdf>.

Hague Convention (V), Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 18 October 1907, 1 Bevans 654.

Hague Convention (IV) Respecting the Laws and Customs of War on Land, 18 October 1907, (1908 Supp.), 36 Stat. 2295, 2 A. J.I.L. 90.

Charter of the United Nations, 26 June 1945, Can TS 1945 No 7.

Statute of the International Court of Justice, 3 Bevans 1179, 59 Stat. 1031.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 27 January 1967, 19 UST 2410, 610 U.N.T.S. 205 (entered into force on 10 October 1967).

The Agreement on the Rescue of Astronauts and the Return of Objects Launched in Outer Space, 22 April 1968, 19 UST 7570, 672 U.N.T.S. 119 (entered into force on 3 December 1968).

Vienna Convention on the Law of Treaties, 23 May 1969, 1155 U.N.T.S. 331.

Convention on International Liability for Damage Caused by Space Objects, 29 March 1972, 961 U.N.T.S. 187, 24 UST 2389 (entered into force 1 September 1972).

Convention on Registration of Objects Launched into Outer Space, 14 January 1975, 28 UST 695, 1023 U.N.T.S. 15 (entered into force on 15 September 1976).

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 U.N.T.S. 3.

Agreement governing the Activities of States on the Moon and Other Celestial Bodies, 18 December 1979, 1363 U.N.T.S. 3 (entered into force on 11 July 1984).

International Telecommunication Union Radio Regulations, (Geneva: ITU 2011).

Constitution of the International Telecommunication Union, cited in *Collection of the basic texts of the International Telecommunication Union adopted by the Plenipotentiary Conference,* 2011 ed. (Geneva: ITU 2011).

B. Cases and Statutes (Chronologically in Ascending Order)

The Alabama Claims (United States v. Great Britain) (1872) reprinted in JB Moore, *History and Digest of International Arbitrations to which the United States has been a Party*, Vol 1 (GPO 1898) 495.

S.S. Wimbleton (United Kingdom v. Germany) (1923), PCIJ (Ser A) No 1.

Factory at Chorzow, Jurisdiction (Germany v. Poland) (1927). PCIJ (Ser A) No 9.

Trail Smelter Arbitration (United States v. Canada) (1938), 3 RIAA.

Phosphates in Morocco, Preliminary Objections (Italy v. France), (1938), PCIJ (Ser A/B) No 74.

Corfu Channel Case (United Kingdom v. Albania), Merits (1949), ICJ Rep 4.

Monetary Gold Removed from Rome in 1943 (Italy v. France, United Kingdom & United States), Preliminary Question, (1954), ICJ Rep 32.

Case concerning the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain), Judgment, [1970] ICJ Rep 3.

United States Diplomatic and Consular Staff in Tehran (United States v. Iran), [1980] ICJ Rep 3.

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), [1986] ICJ Rep 14.

Legality of the Threat or Use of Nuclear Weapons Case, Advisory Opinion, [1996] ICJ Rep 226.

The Case Concerning the Gabcikovo-Nagymaros Project (Hungary v. Slovakia), [1997] ICJ Rep 7.

Prosecutor v. Dusko Tadic, IT-94-1, Judgment (15 July 1999) (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber).

Prosecutor v. Kupreskic, IT-95-16-T, Trial Chamber Decision (14 January 2000) (International Criminal Tribunal for the Former Yugoslavia).

Case Concerning Armed Activities on the Territory of the Congo (Congo v. Uganda), [2005] ICJ Rep 168.

Case Concerning Oil Platforms (Islamic Republic of Iran v. United States), [2003] ICJ Rep 161.

Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia & Herzegovina v. Serbia), [2007] ICJ Rep 43.

C. U.N. Resolutions and Other International Documents (Chronologically in Ascending Order)

Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, 11 December 1868, online: ICRC <http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=568842C2B90F4A29C12563CD0051547C>.

UN SCOR, UN Doc. Res S/RES/83 (1950).

UN SCOR, UN Doc. Res S/RES/1000 (1956).

Question of the Peaceful Use of Outer Space, GA Res 1348 (XIII), UN GAOR, 13th Sess, (1958).

Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, GA Res 1962 (XVII), UN GAOR, 18th Sess, Supp No. 15, UN Doc A/5515 (1963).

International Space Treaties Travaux Preparatoires, UN GOAR, 17th Sess., 1289th Mtg, UN Doc A/C.1/PV.1289 (1962).

Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, GA Res 2625 (XXV), UN GAOR, 25th Sess, Supp No. 18, UN Doc A/8082 (1970).

Resolution of the Definition of Aggression, GA Res. 3314 (XXIV) UN GAOR, 29th Sess., Supp No 31, UN Doc A/9890 (1974).

Manila Declaration on the Peaceful Settlement of International Disputes, UN GAOR 68th Sess, UN Doc A/RES/37/10 (1982).

UN SCOR, UN Doc. Res S/RES/678 (1990).

UN SCOR, UN Doc. Res S/RES/660 (1990).

UN SCOR, UN Doc. Res S/RES/1078 (1996).

UN SCOR, UN Doc. Res S/RES/1291 (2000).

UN SCOR, UN Doc. Res S/RES/1295 (2000).

International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, UNGAOR, 53d Sess, UN Doc A/56/83 (2001).

UN SCOR, UN Doc. Res S/RES/1497 (2003).

UN SCOR, UN Doc. Res S/RES/1509 (2003).

UN SCOR, UN Doc. Res S/RES/1636 (2005).

UN SCOR, UN Doc. Res S/RES/1706 (2006).

UN SCOR, UN Doc. Res S/RES/1718 (2006).

Protection of Civilians in Armed Conflict, SC Res 1674, UNSCOR, 2006, 5430th Mtg, UN Doc S/RES/1674 (2006).

UN SCOR, UN Doc. Res S/RES/1769 (2007).

UN SCOR, UN Doc. Res S/RES/1778 (2007).

UN SCOR, UN Doc. Res S/RES/1973 (2011).

D. Governmental Documents

Testimony of U.S. Ambassador Arthur Goldberg in Treaty of Outer Space, Hearings before Senate For. Relations Comm, 90th Cong., 1st Sess. 70-72 (1967).

Testimony of U.S. Senator Gore in Treaty of Outer Space, Hearings before Senate For. Relations Comm, 90th Cong., 1st Sess. 71 (1967).

U.S., 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), online: Air University <http://space.au.af.mil/space_commission/executive_summary.pdf>.

U.S., General Accounting Office, *Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed* (GAO-02-781) (Washington, DC, US General Accounting Office, August 2002).

U.S. Department of Defense News Transcript, "DoD News Briefing with Deputy National Security Advisor Jeffrey, General Cartwright and NASA Administrator Griffin," 14 Feb 2008.

U.S., President of the United States, *U.S. National Space Policy* (28 June 2010).

U.S., Federal Communications Commission, "FCC Enforcement Bureau Takes Action Against Craigslist Sellers for Marketing Illegal Signal Jamming Devices" Commission Document 15 October 2012, online: FCC <http://transition.fcc.gov/eb/News_Releases/DOC-316796A1.html>.

E. Books (Alphabetical by Author)

Boothby, William H. *The Law of Targeting* (Oxford: University Press, 2012).

Brownlie, Ian. *International Law and the Use of Force* (Oxford: Clarendon Press, 1963).

Brownlie, Ian. *Principles of Public International Law* 6th ed (Oxford: Oxford University Press, 2003).

Cheng, Bin. *General Principles of International Law as Applied by International Courts and Tribunals* (Oxford: Cambridge, 1953).

Cheng, Bin. *Studies in International Space Law* (Oxford: Clarendon Press, 1997).

Christol, Carl Q. *The Modern International Law of Outer Space* (New York: Pergamon Press, 1982).

Christol, Carl Q. *Space Law: Past, Present, and Future* (New York: Springer, 1991).

Crawford, James, ed. *The International Law Commission's Articles on State Responsibility, Introduction, Text and Commentaries* (Cambridge: University Press, 2001).

Dinstein, Yoram. *War, Aggression and Self-Defence*, 4th ed (Cambridge: University Press, 2005).

Dinstein, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict* 2d ed. (Cambridge: University Press, 2010).

Gorove, Stephen. *Developments in Space Law: Issues and Policies* (The Netherlands: Kluwer Academic Publishers, 1991).

Gray, Christine. *International Law and the Use of Force* (Oxford: University Press, 2000).

Greenberg, Lawrence T. et al. *Information Warfare and International Law* (National Defense University Press, 1998).

Harrison Dinniss, Heather. *Cyber Warfare and the Laws of War* (Cambridge: University Press, 2012).

Henckaerts, Jean-Marie & Doswald-Beck, Louise. *Customary International Humanitarian Law Rules* (Cambridge: University Press, 2009).

Jennings, Robert & Watts, Arthur, eds, *Oppenheim's International Law* 9th ed (Essex England: Longman Group, 1992).

Katselli Proukaki, Elena, *The Problem of Enforcement in International Law* (New York: Routledge, 2010).

Lachs, Manfred. *The Law of Outer Space: An Experience in Contemporary Law Making* (Netherlands: Sijthoff Leiden, 1972).

Lambakis, Steven J. *On the Edge of Earth: The Future of American Space Power* (Lexington, Kentucky: The University Press of Kentucky, 2001).

-- *Law of War Deskbook*, International and Operational Law Department, (Charlottesville, Virginia: The Judge Advocate General's Legal Center and School, 2001).

Lyall, Francis & Larsen, Paul B. *Space Law: A Treatise* (Surrey, England: Ashgate, 2009).

Mason, John W. *The Cold War, 1945-1991* (London: Routledge, 2009).

McDougal, Myres S., Lasswell, Harold D. & Vlasic, Ivan A. *Law and Public Order in Space* (New Haven & London: Yale University Press, 1963).

O'Connell, Daniel Patrick. *International Law, Vol. 1* 2d ed (London: Stevens, 1970).

Oppenheim's International Law: *A Treatise* 7th ed (H. Lauterpacht, ed, London: Longmans, 1952)

Pelton, Joseph N. *Satellite Communications* (New York: Springer Science & Business Media, 2012).

Sandoz, Yves, Swinarski, Christophe & Zimmerman, Bruno. eds, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (The Netherlands: Martinus Hijoff, 1987).

Savage, James B. *The Politics of International Telecommunications Regulation* (Boulder, San Francisco & London: Westview Press, 1989).

Schmitt, Michael N. ed, *Tallin Manual on the International Law Applicable to Cyber Warfare* (Cambridge: University Press, 2012).

Sharp, Walter G. *Cyber Space and the Use of Force* (Falls Church, Virginia: Aegis Research, 1999).

Shaw, Malcolm N. *International Law* 5th ed (Cambridge: Univeristy Press, 2003).

Simma, Bruno. ed, *The Charter of the United Nations: A Commentary,* 2d ed (Oxford: University Press, 2002).

Toffler Alvin & Toffler, Heidi. *War and Anti-War: Making Sense of Today's Global Chaos* (New York: Warner Books, 1993).

van Bogaert, E.R.C. *Aspects of Space Law* (The Netherlands: Kluwer Law & Taxation Publishers, 1986).

von Clausewitz, Carl. *On War* (Princeton, New Jersey: Princeton University Press, 1976).

Waldock, Sir Claud Humphrey Meredith. *The Regulation of the Use of Force by Individual States in International Law* (Hague Recueil, 1952).

Wright, David, et al, *The Physics of Space Security: A Reference Manual* (Cambridge, MA: American Academy of Arts and Sciences, 2005).

F. Articles from Journals and Books (Alphabetical by Author)

Bekker, Pieter H.F. "The UN General Assembly Requests a World Court Advisory Opinion On Israel's Separation Barrier" (December 2003) American Soc Int'l L Insights.

Bourbonniére, Michel. "Law of Armed Conflict (LOAC) and the Neutralisation of Satellites or *Ius In Bello Satellitis*" (2004) 9:1 J Confl & Sec L 43.

Bourbonniére, Michel. "The Clausewitz Nebule: The Legitimacy of Military Activities in Outer Space During Armed Conflicts" (2010) 40 Isr YB Hum Rts 243.

Bourbonniére, Michel & Lee, Ricky. "Legality of the Deployment of Conventional Weapons in Earth Orbit: Balancing Space Law & the Law of Armed Conflict" (2007) 18:5 EJIL 873.

Brownlie, Ian. "International Law and the Activities of Armed Bands" (1958) 7 Int'l & Comp L Quarterly 712.

Buchan, Russell. "Cyber Attacks: 'Unlawful Uses of Force or Prohibited Interventions?'" (2012) 17:2 J. Conflict & Sec. L 211.

Carlson, Bruce. "Protecting Global Utilities: Safeguarding the Next Millennium's Space Based Public Services" (2000) Aerospace Power J 37.

Diederiks-Verschoor, I.H. Ph. "Registration of Spacecraft" in Edward McWhinney & Martin A Bradley, eds, *New Frontiers in Space Law* (The Netherlands: Kluwer Law, 1969).

Dinstein, Yoram. "Computer Network Attacks and Self-Defense" (2002) 76 Int'l L Stud 99.

Dinstein, Yoram. "Legitimate Military Objectives under the Current Jus in Bello" in A.E. Wall, ed, *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Newport RI: Naval War College, 2002) 139.

Dinstein, Yoram. "Discussion" in A.E. Wall, ed, *Legal and Ethical Lessons of NATOS's Kosovo Campaign* (Newport RI: Naval War College, 2002) 211.

Droege, Cordula. "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protections of Civilians" (2013) 94 Int'l Rev Red Cross.

Freeland, Steven. "In Heaven as on Earth – The International Legal Regulation of the Military Use of Outer Space" (2011) 8:3 US-China L Rev 272.

Garwood-Gowers, Andrew. "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," Case Note (2004) 5 Melbourne J Int'l L 241.

Gordon, Joy. "The U.S. Embargo against Cuba and the Diplomatic Challenges to Extraterritoriality" (2012) 36 Fletcher Financial World Aff 63.

Hart, Brandon. "Legal Implications Surrounding Recent Interception of Spy Satellite," Joint Center for Operational Analysis J. 24 (June 2008).

Hathaway, Oona A. et al, "The Law of Cyber Attack" (2012) 100 Cal L Rev 817.

Henkin, Louis. "The Reports of the Death of Article 2(4) are Greatly Exaggerated" (1971) 65 Am J Int'l L 544.

Hitchens, Theresa. "Debris, Traffic Management, and Weaponization: Opportunities for and Challenges to Cooperation in Space" (2007) 14 Brown J World Affairs 173.

Hitchens, Theresa. "Multilateralism in Space: Opportunities and Challenges for Achieving Space Security" (2010) 4 Space & Defense 3.

Hollis, Duncan B. “Why States Need an International Law for Information Operations” (2007) 11 Lewis & Clark L Rev 1023.

Housen-Couriel, Deborah. “Disruption of Satellite Transmissions *ad Bellum* and *in Bello*: Launching a New Paradigm of Convergence” (2012) 45:3 Isr LR 431.

Jakhu, Ram & Singh, Karan. “Space Security and Competition for Radio Frequencies and Geostationary Slots” (2009) 58 ZLW 79.

Jakhu, Ram. “Regulatory Processes for Communications Satellite Radio Frequencies” in Joseph N. Pelton, Scott Madry & Sergio Camacho Lara, eds, *The Handbook of Satellite Applications* (New York: Springer Science & Business Media, 2013) 271.

Joyner, Christopher C. & Lotrionte, Catherine. “Information Warfare as International Coercion: Elements of a Legal Framework” (2001) 12 Eur J Int’l L 825.

Juqian, Li. “Legality & Legitimacy of China’s ASAT Test” (2009) 5:1 China Sec 45.

Kanuck, Sean P. “Information Warfare: New Challenges for Public International Law” (1996) 37 Harv Int’l L J 272.

Koplow, David A. “ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons” (2009) 30 Mich J Int’l L 1187.

Lee, Ricky J. “ Article II of the Outer Space Treaty: Prohibition of State Sovereignty, Private Property Rights, or Both?” (2004) 11 Aust. Int’l LJ 128.

Martello, Norman. “Where in the World?” (March 1999) 24 Electric Perspective 14.

Maogoto, Jackson Nyamuya & Freeland, Steven. “Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist” (2007) 41 Int’l L 1091.

McClure, Ryan. “International Adjudication Options in Response to State-Sponsored Cyber-Attacks Against Outer Space Satellites” (2012) 18 New Eng J Int’l & Comp L Ann 431.

Mineiro, Michael C. “FY-1C and USA-193 ASAT Intercepts: An Assessment of Legal Obligations Under Article IX of the Outer Space Treaty” (2008) 34 J Space L 321.

Morgan, Richard A. “Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and “Peaceful Purposes” (1994) 60 J Air L & Comm 237.

Reed, Walter D., & Norris, Robert B., "Military Use of the Space Shuttle" (1979) 13 Akron L Rev 665.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework" (1999) 37 Colum J of Transnat'l L 885.

Schmitt, Michael N. "International Law and Military Operations in Space" (2006) 10 Max Planck Yearbook of United Nations Law 89.

Schmitt, Michael N. "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts" in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010* (Washington, DC: National Research Council, 2010) 151.

Schmitt, Michael N. *"*Classification of Cyber Conflict*"* (2012) 17:2 J Conf & Sec L 245.

Scott, Roger D. "Legal Aspects of Information Warfare: Military Disruption of Telecommunications" (1998) 45 Nav L Rev 57.

Stares, Paul B. "Space and U.S. National Security" in William Durch, ed, *National Interests and the Military Use of Space* (Cambridge, Mass.: Ballinger, 1984) 41.

Tsagourias, Nicholas. "Cyber Attacks, Self-Defence and the Problem of Attribution" (2012) 12:2 J Confl & Sec L 229.

Vlasic, Ivan A. "The Legal Aspects of Peaceful and Nonpeaceful Uses of Outer Space" in Bhupendra Jasani ed, *Peaceful and Non-Peaceful Uses of Space, Problems for the Prevention of an Arms Race* (The Netherlands, Kluwer, 1991).

Vlasic, Ivan A. "Space Law and the Military Applications of Space Technology" in N. Jasentuliyana ed, *Perspectives on International Law* (The Netherlands: Kluwer Law & Business, 1995) 385.

Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)" (2011) 36:42 Yale J Int'l L 421.

Weisbord, Noah. "Conceptualizing Aggression" (2009) 20 Duke J Comp & Int'l L 1 37.

Wilgenbusch, Ronald C. & Heisig, Alan. "Command and Control Vulnerabilities to Communications Jamming" (2013) 69:2 Joint Force Quarterly 56 at 57, online: National Defense University <http://www.ndu.edu/press/lib/pdf/jfq-69/JFQ-69_toc.pdf>.

G. Thesis, Reports, Presentations and Dissertations (Alphabetical)

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

Burris, Matthew. "U.S. Space Security: History, Law & Policy" (Presentation delivered online U.S. Air Force JAG Corps, 25 April 2013), [unpublished].

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

Gydesen, Paul W. *What it the Impact to National Security Without Commercial Space Applications* (Research Project, Air War College, Maxwell Air Force Base, Alabama, 2006), online: Air University < http://www.au.af.mil/au/awc/awcgate/awc/gydesen.pdf>.

Hart, Brandon L. *Anti-Satellite Weapons: Threats, Laws and the Uncertain Future of Space* (LL.M. Thesis, McGill University Institute of Air and Space Law, 2007).

Henri, Yvon. "The ITU Radio Regulations and Space Sustainability" (Presentation delivered to The Brussels Space Policy Roundtable, Brussels, Belgium, 29 November 2012), online: Secure World Foundation <http://swfound.org/media/96609/2012_SSI_Yvon%20Henri.pdf>.

Jakhu, Ram. "Satellites: Unintentional and Intentional Interference" (Presentation delivered at the Radio Frequency Interference & Space Sustainability Panel Discussion, Washington, DC, 17 June 2013), [unpublished].

Jarman, Robert W. *The Law of Neutrality in Outer Space* (LL.M. Thesis, McGill University Institute of Air and Space Law, 2008).

Rausch, Hank. *Jamming Commercial Satellite Communications During Wartime: An Empirical Study: Proceedings of the Fourth IEEE International Workshop on Information Assurance, 2006* (Royal Holloway, United Kingdom, 2006).

Ramey, Robert A. *Space Warfare and the Future Law of War* (LL.M. Thesis, McGill University Institute of Air and Space Law, 1999).

Schmitt, Michael N. "'The Use of Force' in Cyberspace: A Reply to Dr. Ziolkowski," (Paper delivered at the 2012 4th International Conference on Cyber Conflict) (2012) NATO CCD COE Publications, Tallinn 311.

Terrill, Jr., Delbert R. "The Air Force Role in Developing International Outer Space Law" (Air University Press, May 1999).

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

Waldrop, Elizabeth S. *Integration of Military and Civilian Space Assets: Legal and National Security Implications* (LL.M. Thesis, McGill University Institute of Air and Space Law, 2003).

Wilson, Tom. "Threats to United States Space Capabilities" (Paper prepared for the Commission to Assess United States National Security Space Management and Organization), online: <http://www.fas.org/spp/eprint/article05.html>.

H. Articles from Newspapers and Magazines (Alphabetically by Author)

Baker, Luke. "2-EU Ministers Warn Iran on Satellite Jamming" *Reuters* (22 March 2010).

Berlocher, Greg. "Interference: Operators Making Advances in Flight" *Satellite Today* (1 June 2008), online: Satellite Today <http://www.satellitetoday.com/via/featires/23237.html>.

Brandon, John. "GPS Jammers Illegal, Dangerous, & Very Easy to Buy" *Fox News* (17 March 2010), online: Fox News < http://www.foxnews.com/tech/2010/03/17/gps-jammers-easily-accessible-potentially-dangerous-risk/>.

Clark, Stephen. "Reconnaissance Satellites Launched by H-2A Rocket" *Spaceflight Now* (27 January 2013), online: Space Flight Now <http://www.spaceflightnow.com/h2a/f22/#.UbdxspVsWR8>.

de Grasse Tyson, Neil. "The Case for Space: Why We Should Keep Reaching for the Stars" (March/April 2012), 91 Foreign Affairs 22.

de Selding, Peter B. “ITU Implores Iran to Help Stop Jamming” *Space News* (26 March 2010), online: Space News <http://www.spacenews.com/article/itu-implores-iran-help-stop-jamming#.UdWkfhZsWR8>.

--“Falun Gong Hijacks HK Satellite” *Xinhua News Agency* (22 November 2004).

--“Falun Gong Jams Official Chinese TV” *The Washington Post* (9 July 2002), online: The Washington Post < http://articles.chicagotribune.com/2002-07-09/news/0207090078_1_falun-gong-li-hongzhi-hong-kong-based-human-rights-group>.

Ghazai, Mohammad. “Satellite Channel Jamming Rose Sharply After Arab Spring” *The Jordan Times* (15 May 2013), online: The Jordan Times <http://jordantimes.com/satellite-channel-jamming-rose-sharply-after-arab-spring>.

Haeri, Safa. “Cuba Blows the Whistle on Iranian Jamming” *Asia Times* (22 August 2003).

Kleiman, Matthew & McNeil, Sonia. “Red Lines in Outer Space” *The Space Review* (5 March 2012), online: The Space Review <http://www.thespacereview.com/article/2038/1>.

McDermott, Hugh. “How Financial Markets Finance Terrorism” *Law, Crime, Politics”* (8 July 2011), online: Law, Crime, Politics < http://lawcrimepolitics.com/how-financial-markets-finance-terrorism>.

Oliveri, Frank. “The Pentagon’s GPS Problem” *Congressional Quarterly* (9 February 2013), online: Congressional Quarterly <http://public.cq.com/docs/weeklyreport/weeklyreport-000004218242.html>.

Rust, Kate. “Kehler: ‘The Future of Space is Now’” (7 December 2007), online: Air Force Space Command <http://www.afspc.af.mil/news/story.asp?id=123078666>.

Sang-Hun, Choe. “Seoul Says North Korea Tries to Disrupt Air Navigation” *The New York Times* (2 May 2012), online: The New York Times <http://www.nytimes.com/2012/05/03/world/asia/seoul-says-north-korea-tries-to-disrupt-air-navigation.html?_r=0>.

Santoli, Al. "Beijing Describes How to Defeat U.S. in High-Tech War" *China Reform Monitor* (10 October 2000).

Saul, Jonathan. “Governments Confront Rising Threat to Ships from Signal Jamming” *Reuters* (30 May 2013), online: <http://www.reuters.com/article/2013/05/30/shipping-navigation-gps-idUSL5N0E926V20130530>.

Shachtman, Noah. “China Space Attack: Unstoppable” *The Huffington Post* (18 January 2007), online: The Huffington Post < http://www.huffingtonpost.com/noah-shachtman/china-space-attack-unstop_b_38999.html>.

Shachtman, Noah. “Pentagon Paying China – Yes, China – To Carry Data” *Wired.com* (29 April 2013), online: Wired.com <http://www.wired.com/dangerroom/2013/04/china-pentagon-satellite/>.

Stoullig, Jean-Michel. “Rumsfeld Commission Warns Against ‘Space Pearl Harbor’” *Space Daily* (11 January 2011), online: Space Daily < http://www.spacedaily.com/news/bmdo-01b.html>.

Teltsch, Kathleen. "6 Soviet Space Failures Believed To Have Been Probes of Planets" The New York Times (16 June 1963).

Wainscott-Sargent, Anne. “Fighting Satellite Interference on All Fronts” *Satellite Today* (1 March 2013), online: Satellite Today.com <http://satellitetoday.com/via/features/40651.html>.

I. Online and Internet Resources (Alphabetically)

--“9/11 Terrorists Made Millions on the Stock Market” *Charles Sturt University*, online: <http://news.csu.edu.au/director/features.cfm?itemID=4C5F5C13C6A538CCE83C67E0784596AA>.

-- “A Brief History of the National Aeronautics and Space Administration,” online: NASA <http://www.hq.nasa.gov/office/pao/History/40thann/factsheet.htm>.

--“About ITU Membership,” online: International Telecommunications Union <http://www.itu.int/en/about/Pages/default.aspx>.

--“About ITU: Conferences and Meetings: WRC,” online: International Telecommunications Union < http://www.itu.int/ITU-R/index.asp?category=conferences&rlink=wrc&lang=en>.

Acker, Olaf, Potscher, Floran & Lefort, Thierry. “Why Satellites Matter: The Relevance of Commercial Satellites in the 21st Century-A Perspective 2012-2020,” online: <http://www.esoa.net/upload/files/news/Why%20Satellites%20Matter%20-%20Full%20Report.pdf>.

Black, Samuel. "No Harmful Interference with Space Objects: The Key to Confidence Building" (July 2008), online: *Stimson Center* <http://www.stimson.org/images/uploads/research-pdfs/NHI_Final.pdf >.

--"Concern Over China's Missile Test" *BBC News* (19 January 2007), online:<http://news.bbc.co.uk/2/hi/asia-pacific/6276543.stm>.

Cook, William Craig. "How Do Satellites Work?" online: <http://www.williamcraigcook.com/satellite/work.html>.

--Dragon Space, "Britain Concerned by Chinese Satellite Shoot-Down," (19 Jan 2007), online: <http://www.spacewar.com/reports/Britain_Concerned_By_Chinese_Satellite_Shoot_Down_999.html>.

Finkleman, David, et al, "Space Debris Birth to Death Analysis from Concern to Consequences" Center for Space Standards and Innovation Analytical Graphics, Inc., online: <http://www.amostech.com/TechnicalPapers/2008/Orbital_Debris/Finkleman.pdf>.

Foust, Jeff. "WikiLeaks Cables on US-China ASAT Testing," (3 Feb 2011), online <http://www.spacepolitics.com/2011/02/03/wikileaks-cables-on-us-china-asat-testing/>.

Grego, Laura. "A History of Anti-Satellite Programs" (January 2012), online: Union of Concerned Scientists < http://www.ucsusa.org/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf>.

Gruss, Mike. "Panel Ties U.S. Troop Rotations to Satellite Interference Spikes" *Space News* (24 June 2013), online: Space News.com <http://www.spacenews.com/article/military-space/35948military-satellite-communications-panel-ties-us-troop-rotations-to#.Ue254RZsWR8>.

--"How September 11 Affected the U.S. Stock Market" *Investopedia* (11 September 2011), online: < http://www.investopedia.com/financial-edge/0911/how-september-11-affected-the-u.s.-stock-market.aspx>.

Kelly, John. "Debris is Shuttle's Biggest Threat" (5 March 2005), online: Space.com <http://www.space.com/792-debris-shuttle-biggest-threat.html>.

Malik, Tariq. "Station Astronauts Take Shelter from Space Debris" (12 March 2009), online: Space.com < http://www.space.com/6410-station-astronauts-shelter-space-debris.html>.

--"Merriam-Webster Online Dictionary," online <http://www.merriam-webster.com/dictionary/object>.

--"NBN Co Closes in on Satellite Slots," (8 April 2013), online: <http://www.talksatellite.com/Asia-A101283.htm>.

Oberright, John E. NASA Artificial Satellites, online: <https://www.nasa.gov/worldbook/artificial_satellites_worldbook.html>.

Shapiro, Irwin I. "Orbital Properties of the West Ford Dipole Belt," online: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1444922&isnumber=31060>.

--"Sputnik and The Dawn of the Space Age," online: NASA <www.history.nasa.gov/sputnik>.

--"Status of International Agreements Relating to Activities in Outer Space" United Nations Office for Outer Space Affairs, online: United Nations Office for Outer Space Affairs < http://www.oosa.unvienna.org/oosa/en/SpaceLaw/treatystatus/index.html>.

--"The Beep Heard 'Round the World," online: <http://memagazine.asme.org/Web/Beep_Heard_Round_World.cfm>.

--"The Story of Captain Midnight," online: Signal to Noise <http://web.archive.org/web/20070128101239/http://www.signaltonoise.net/library/captmidn.htm>.

Thompson, Loren B. "Lack of Protected Satellite Communications Could Mean Defeat for Joint Force in Future War" Lexington Institute Early Warning Blog (14 April 2010), online: Lexington Institute < http://www.lexingtoninstitute.org/lack-of-protected-satellite-communications-could-mean-defeat-for-joint-force-in-future-war>.

Thorpe, Norman. "The Process of Space Law Development" *International Law Division, USAF, Office of Judge Advocate General,* Paper delivered at Major Command Judge Advocate Conference, Bolling AFB*, D.C.*, 16 November 1967, 3. online: <http://www.docstoc.com/docs/33978175/The-Air-Force-Role-in-Developing-International-Outer-Space-Law>.

--Union of Concerned Scientists, *UCS Satellite Database*, online: Union of Concerned Scientists

<http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html>.

--Union of Concerned Scientists, "The Nature of the USC Database," online: Union of Concerned Scientists <http://www.ucsusa.org/assets/documents/nwgs/common-misconceptions.pdf>.

Weedon, Brian. "2007 Chinese Anti-Satellite Test Fact Sheet" *Secure World Foundation* (23 November 2010), online: Secure World Foundation <http://swfound.org/media/9550/2007%20chinese%20asat%20test%20factsheet.pdf>

--"Satellite Jamming in Iran: A War Over Airways, Media Report" (November 2012), online: <http://www.pbs.org/wgbh/pages/frontline/tehranbureau?satelliteJammingInIranSmallMedia.pdf>.

--"Sputnik and The Dawn of the Space Age," online: NASA <www.history.nasa.gov/sputnik>.