Journal of Air Law and Commerce

Volume 86 | Issue 2 Article 3

2021

Rethinking Cyberspace Operations: Widespread Electromagnetic Jamming by States Indicates Cyber Interference Is Not a Use of Force

Vincent L. DeFabo
U.S. Air Force JAG Corps

RETHINKING CYBERSPACE OPERATIONS: WIDESPREAD ELECTROMAGNETIC JAMMING BY STATES INDICATES CYBER INTERFERENCE IS NOT A USE OF FORCE

VINCENT L. DEFABO*

TABLE OF CONTENTS

* Vincent L. DeFabo received his J.D. from American University and LL.M. from University of Nebraska-Lincoln in Space, Cyber, and Telecommunications Law. He currently serves in the U.S. Air Force JAG Corps advising the Air Force's two Cyberspace Wings. The author greatly appreciates the support of Professor Jack Beard in the comments to earlier drafts of this work. The views and opinions expressed in this article are those of the author alone and do not necessarily reflect those of the United States Department of Defense, the United States Air Force, or any other government agency.

I. INTRODUCTION

IN 2007, A SOVIET-ERA war memorial was removed from the center square of the Estonian capital, Tallinn.[1] The statue's removal led to massive cyber operations that shut down the Estonian government, television, and bank websites.[2] The cyber operations, likely caused by Russia, came in the form of "distributed denial-of-service" (DDoS) operations to Estonia's web, e-mail, and Domain Name System (DNS) servers.[3]

This incident popularized the *Tallinn Manual* and an "effects-based" approach to categorize cyber operations, which analyzes the effects of the operations and potential State responses.[4] In a

---

[1] *See* Steven Lee Myers, *Estonia Removes Soviet-Era War Memorial After a Night of Violence*, N.Y. Times (Apr. 27, 2007), https://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html [https://perma.cc/CM6B-ZEKE].

[2] *See* Steven Lee Myers, *'E-Stonia' Accuses Russia of Computer Attacks*, N.Y. Times (May 18, 2007), https://www.nytimes.com/2007/05/18/world/europe/18cndrussia.html [https://perma.cc/JPB5-HBJK]; *see also* Marco Roscini, Cyber Operations and the Use of Force in International Law 4 (2014).

[3] Kevin Poulsen, *'Cyberwar' and Estonia's Panic Attack*, Wired (Aug. 22, 2007, 3:51 PM), https://www.wired.com/2007/08/cyber-war-and-e/ [https://perma.cc/8LNV-RC6F]; Myers, *supra* note 2. However, the majority of DDoS attacks came from Russian IP addresses and some even from Russian government institutions. *See* Myers, *supra* note 2; Mark Landler & John Markoff, *In Estonia, What May Be the First War in Cyberspace*, N.Y. Times (May 28, 2007), https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html [https://perma.cc/8LNL-VE6Z].

[4] *See* Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 Vill. L. Rev. 569, 577 (2011) ("[T]he [Estonia] incident arguably reached the use-of-force threshold."); David E. Graham, *Cyber Threats and the Law of War*, 4 J. Nat'l Sec. L. & Pol'y 87, 91 (2010); Sheng Li, Note, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, 38 Yale J. Int'l L. 179, 200–01 (2013) (arguing that under the consequence-based approach, the Estonia incident could be

similar vein, a political commentator claimed, "Blood will need to be answered with blood. . . . [T]he next major war the United States enters will be provoked by a cyberattack."[5] However, these views lack detailed analyses of the United Nations (U.N.) Charter and customary international law. Other scholars question if most cyber operations can be an act of war (i.e., a use of force) under the U.N. Charter.[6]

In 2016, another nefarious interference incident occurred; however, this time, over 110 planes and ships in total were affected through the interference of Global Positioning Systems (GPS) instead of through e-mail and websites, and the likely culprit was North Korea.[7] Another significant difference was that the electromagnetic interference was caused by "jamming" rather than a cyber operation.[8] This raises the question: from an international law perspective, is a DDoS different from jamming by State actors?

---

classified as an armed attack under Article 51 of the U.N. Charter). The Estonia incident has also led to the naming of the *Tallinn Manual* (a scholarly exercise of nonbinding cyber rules for cyber operations) after Estonia's capital from where the Soviet-era war memorial was removed. INT'L GRP. OF EXPERTS, NATO COOPERATIVE CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, 330–37 (Michael N. Schmitt & Liis Vihul eds., 2d ed. 2017) (2013) [hereinafter TALLINN MANUAL 2.0] (defining a "use of force" based on the consequences of the cyber action as established by eight criteria); ROSCINI, *supra* note 2, at 30–31.

[5] RICHARD A. CLARKE & ROBERT K. KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS 7 (2019).

[6] The vast majority of cyber operations deal with subversion, espionage, or sabotage which in itself does not rise to the level of an armed attack under the U.N. Charter. *See* Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 6, 15, 20 (2012) ("The most widespread use of state-sponsored cyber capabilities is for purposes of espionage."); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1030 (2007) (explaining that information operations "[extend] the use of information technology and networks to 'psychological operations' (psyops) that convey information (e.g., broadcasting satellite radio messages) with the aim of manipulating the views of foreign governments, organizations, or individuals"); *see also* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 428 (2011) ("Armed force is only one instrument of coercion, and the easiest to identify."); *see also id.* at 430 ("Like past efforts to define Article 2(4) 'force' as coercion, efforts to expand its coverage beyond armed force so as to include violations of sovereign domain such as propaganda or political subversion never gained significant traction.").

[7] Stephen Evans, *North Korea 'Jamming GPS Signals' Near South Border*, BBC NEWS (Apr. 1, 2016), https://www.bbc.com/news/world-asia-35940542 [https://perma.cc/7DFG-A977].

[8] *See id.*

This Article will focus on one type of cyber operation: interference by cyber means analyzed through *jus ad bellum* (i.e., use of force between States). Classifying interference by cyber means matters because *if* a cyber operation is considered an armed attack or use of force, then physical self-defense measures could be justified under *jus ad bellum*.[9] In other words, if State A's interference by cyber means against State B violates *jus ad bellum* by being a use of force or armed attack, then State B could engage in proportionate self-defense measures, including the use of missiles or ground troops.[10] Yet, there are two reasons interference by cyber means is likely not a use of force.

First, there are adequate means to address DDoS Tallinn-type incidents in the U.N. Charter rather than speculate how States may react to cyber operations. Article 41 of the U.N. Charter defines actions *not* involving the use of force, including "complete or partial interruption of . . . telegraphic, radio, and other means of communication."[11] Applying the ordinary meaning of "communication" and "interruption" and analyzing the travaux préparatoires of the U.N. Charter, communication interruptions (which encompasses interference by cyber means) are not categorized as a use of force.[12]

Second, there have been dozens—if not hundreds—of Tallinn-type electromagnetic interference events during non-hostilities besides the North Korean jamming of planes and ships in 2016.[13] State practice of "jamming" and other electromagnetic interference has occurred since the 1930s.[14] Some examples in-

---

[9] Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 102 (2002).

[10] Counter-Memorial & Counter-Claim of the United States of America, Oil Platforms (Iran v. U.S.), 1997 I.C.J. Pleadings 126, ¶ 4.01 (June 23, 1997). "Actions in self-defense must be proportionate. Force can be used in self-defense, but only to the extent that it is required to repel the armed attack and to restore the security of the party attacked." *Id.* at 141, ¶ 4.31.

[11] *See* U.N. Charter art. 41.

[12] *See* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 36–38 (Bruno Simma ed., 1st ed., 1994). Under Article 31(1) of the Vienna Convention on the Law of Treaties (VCLT), treaty interpretation begins by looking at the ordinary meaning. Vienna Convention on the Law of Treaties art. 31(1), May 23, 1969, 1155 U.N.T.S. 331. Article 32 of the VCLT provides that if the meaning of a treaty is ambiguous or obscure, one can look to the preparatory work, also known as the *travaux préparatoires*. *See id.* art. 32.

[13] *See* JEROME S. BERG, BROADCASTING ON THE SHORTWAVES, 1945 TO TODAY 44–45 (2008).

[14] *Id.* On a basic level, jamming is "the transmission of noise or other interfering material on the frequency of the targeted station so as to disrupt reception." *Id.* at 44. Several countries jammed broadcasts in the 1930s: Austria against the

clude (1) the Soviets blocked a U.S. GPS signal, causing navigation difficulties;[15] (2) Iran jammed European Eutelsat satellite broadcasts;[16] and (3) China conducted cyber interference of U.S. satellites.[17]

With a focused analysis of U.N. Charter Article 41 and State practice of electromagnetic interference, the law as it currently exists is that cyber operations through interference is unlikely to amount to a use of force.[18]

II. INTERNATIONAL LAW PRINCIPLES AND U.S. MILITARY DOCTRINE

A. Jus ad Bellum

Jus ad bellum and *jus in bello* are part of the larger "just war tradition" which "provides part of the philosophical foundation for the modern law of war."[19] *Jus ad bellum* addresses acts by States concerning the resort to force.[20] In contrast, *jus in bello*

Nazis, Germany and Russia against each other, and Italy against the Soviet Union. *See id.* at 44. After World War II, more widespread jamming occurred when the Soviets jammed America's Voice of America broadcast to the Soviet bloc. *See id.* at 45.

[15] David Chandler, *Radio Moscow Blocks U.S. Time Signals*, Associated Press, Mar. 23, 1982.

[16] Paul Sonne & Farnaz Fassihi, *Censorship Inc.: In Skies Over Iran, a Battle for Control of Satellite TV*, Wall St. J. (Dec. 27, 2011), https://www.wsj.com/articles/SB10001424052970203501304577088380199787036 [https://perma.cc/YA32-JND7] (stating that Iran "jams channels like the BBC on Western satellites").

[17] U.S.–China Econ. and Sec. Rev. Comm'n, 112th Cong., 2011 Annual Rep. to Cong. 216 (2011).

[18] The *lex lata* is the "law as it is exists," while the *lex ferenda* is "what the law should be." An underlying argument of this article is that many argue the *lex ferenda* is the *lex lata* in cyber operations, which does not appear to have support in treaty or customary international law. *See* Ki-Gab Park, Lex Ferenda *in International Law* (Oct. 23, 2018), https://legal.un.org/avl/pdf/ls/park-kigab_presentation.pdf [https://perma.cc/Q8JP-A7VM].

[19] U.S. Dep't of Def., Department of Defense Law of War Manual § 1.6.4 (May 31, 2016) [hereinafter DoD Law of War Manual]. "According to St. Augustine, fallen human nature being what it is, there will always be a presumption that generation after generation some evil men will choose disorder, violence, and unjust aggression. At times, the only way to restore order will be to use war as a just instrument of statecraft." Michael Novak, *Just Peace and the Asymmetric Threat: National Self-Defense in Uncharted Waters*, 27 Harv. J.L. & Pub. Pol'y 817, 828 (2004). The Just War Tradition had its early development and theory from Saint Augustine of Hippo who developed the *ad bellum* criteria of "when" a State may use force, such as having a "just cause, right intention, [and] competent authority." *Id.* at 826–27.

[20] DoD Law of War Manual, *supra* note 19, § 1.11; *see* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14,

addresses conduct during war.[21] Additionally, the Kellogg-Briand Pact of 1928 (which attempted to outlaw war in its entirety), the League of Nations, and the Nuremberg Trials in 1945 further developed the custom surrounding *jus ad bellum*.[22] A final key distinction is that *jus ad bellum* only deals with the actions of States rather than the actions of individuals.[23]

Regarding cyberspace, the structure and rules of *jus ad bellum* apply.[24] The United States takes the position that existing *jus ad bellum* is incorporated into cyberspace, which includes integrating the international law approach for cyberspace to the U.N. Charter.[25] However, the United States has not developed clear rules regarding whether *jus ad bellum* applies in cyberspace.[26]

¶¶ 191–94 (June 27); *see also* Jack M. Beard, *Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under Int'l Humanitarian Law*, 47 VAND. J. TRANSNAT'L L. 67, 96 (2014) ("[O]nly illegal 'acts of force' implicate the *jus ad bellum*, and only the 'most grave' forms of the use of force satisfy the requirements for an armed attack justifying an armed response under the UN Charter.").

[21] DOD LAW OF WAR MANUAL, *supra* note 19, § 1.11. According to Saint Augustine of Hippo, *in bello* involves "how" force is to be used and that it discriminates between combatants and noncombatants. *See* Novak, *supra* note 19, at 826–27. The *jus ad bellum* has developed from the Treaty of Westphalia to end the Thirty Years War, which obviously did not result in an end to war but did outline some early developments of State sovereignty. *See* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 214 (2002).

[22] *See* Jensen, *supra* note 21, at 214–15.

[23] *See* Novak, *supra* note 19, at 827. The proposition that only a state can declare war derives from Saint Augustine's principle that only a competent authority may declare war. *See id.*; DOD LAW OF WAR MANUAL, *supra* note 19, § 1.11.1.1.

[24] Former Legal Advisor of the U.S. State Department, Harold Hongju Koh, stated, "states have long had to sort through complicated *jus ad bellum* questions. In this respect, the existence of complicated cyber questions relating to *jus ad bellum* is not in itself a new development; it is just applying old questions to the latest developments in technology." Harold Hongju Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the US-CYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012*, 54 HARV. INT'L L.J. ONLINE 1, 8 (2012) [hereinafter *Koh Remarks*].

[25] *See* ROSCINI, *supra* note 2, at 21. This is further evidenced by the 2012 U.S. National Defense Authorization Act which clarified cyberspace is subject to the existing laws of armed conflict and the DoD Law of War Manual, which indicated that the Article 2(4) prohibition on force and threat of force in the U.N. Charter under *jus ad bellum* applies to cyberspace. *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2012); DOD LAW OF WAR MANUAL, *supra* note 19, § 16.3.1.

[26] *See* Waxman, *supra* note 6, at 432–33 (observing that the United States appears to be trending towards a consequence-based approach to use of force in cyberspace).

The United States is not alone in indicating that *jus ad bellum* and the law of armed conflict apply to cyberspace; similar affirmations come from Australia, China, Cuba, the European Union, Hungry, Iran, Italy, the Netherlands, Qatar, Russia, and the United Kingdom (U.K.).[27] Additionally, Russia has drafted rules for the U.N. that propose limitations on cyber-attack rules, indicating a general view that cyberspace can be viewed through the prism of *jus ad bellum*.[28]

B. Definition of Cyber Operations and Jamming

A basic understanding of military doctrine and definitional framework is necessary to analyze *jus ad bellum* in cyberspace.[29] Although a favorite term of political commentators, the phrase "cyber war" is not often used in the legal analysis because the term can lead to misleading analogies.[30] "Cyber operations" is a more accepted and appropriate term.[31]

The Department of Defense (DoD) defines cyberspace operations as the "employment of cyberspace capabilities where the

---

[27] *See* Roscini, *supra* note 2, at 21–22.

[28] *See* Li Baodong (Permanent Representative of the People's Republic of China), Vitaly Churkin (Permanent Representative of the Russian Federation), Sirodjidin Aslov (Permanent Representative of the Republic of Tajikistan) & Murad Askarov (Permanent Representative of the Republic of Uzbekistan), *Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General*, 3–4, U.N. Doc. A/66/359, annex (Sept. 14, 2011); *see also* Waxman, *supra* note 6, at 456; Beard, *supra* note 20, at 142 ("Russia launched a cyber arms control initiative at the UN General Assembly (fashioned as an 'International Code of Conduct') with a troublesome content-related focus, containing prohibitions on 'information terrorism' as well as new 'information security' concepts that essentially gave unwelcome words the status of weapons."). While the sincerity of Russia's desire to limit cyber-attacks is questionable due to their own repeated use of cyber tools and development, their proposal gives some indication that they view cyber operations according to the *jus ad bellum*. *See* Waxman, *supra* note 6, at 456.

[29] Other sections will show how there is no substantial difference between interruptions or disruptions of the electromagnetic spectrum from a legal standpoint, whether it be cyber operations, jamming, blinding, spoofing, or any related concepts based on Article 41 of the U.N. Charter and State practice.

[30] *See* Roscini, *supra* note 2, at 10–11. *But see* Int'l Comm. of the Red Cross, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts 26 (2019), https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts [https://perma.cc/F6EK-4RPP] ("The ICRC understands 'cyber warfare' to mean operations against a computer, a computer system or network, or another connected device, through a data stream, when used as means or methods of warfare in the context of an armed conflict.").

[31] *See* Roscini, *supra* note 2, at 10–11.

primary purpose is to achieve objectives in or through cyberspace."[32] Cyberspace operations can be shortened to "cyber operations." The use of cyber operations is a growth "from the [i]nternet's interconnectivity and other new forms of communication."[33] New technology in cyberspace does not change the nature of *jus ad bellum*.[34]

Two definitions of jamming assist in the *jus ad bellum* analysis of cyber operations. First, jamming involves overloading frequencies with noise so that communications cannot get through.[35] Second, the DoD defines electromagnetic jamming as the use of the electromagnetic spectrum "with the intent of degrading or neutralizing."[36] Therefore, by combining these concepts, jamming can be defined as the deprivation, limitation, or degradation of the use of communication or radar signals through overloading frequencies or other methods of controlling the electromagnetic spectrum through electromagnetic energy.[37]

Jamming is considered a form of harmful interference, which can also include "spoofing."[38] The transmission of noise to the targeted station is generally meant to disrupt reception.[39] Satellite jamming may interfere with a satellite's capabilities, "preventing it from broadcasting at all."[40] Interference with satellites can happen virtually by interfering with the electro-

---

[32] U.S. DEP'T OF DEF., JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-13, INFORMATION OPERATIONS II-9 (2014), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf [https://perma.cc/6RZ5-YW2V] [hereinafter JP FOR INFORMATION OPERATIONS].

[33] Hollis, *supra* note 6, at 1028–29.

[34] *Id.* at 1039–40, 1041 n.70.

[35] Sarah M. Mountin, *The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals*, 90 INT'L L. STUD. 101, 104 (2014); *see also* BERG, *supra* note 13, at 44.

[36] U.S. DEP'T OF DEF., JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-13.1, ELECTRONIC WARFARE GL-7 (2012), https://fas.org/irp/doddir/dod/jp3-13-1.pdf [https://perma.cc/VE3G-XK3U] [hereinafter JP FOR ELECTRONIC WARFARE].

[37] ELECTRONIC WARFARE FUNDAMENTALS 9-3, 10-5 (2000), https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf [https://perma.cc/R4JE-D8B7].

[38] U.S. DEP'T OF DEF., OFF. OF GEN. COUNS., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 32 (1999), https://fas.org/irp/eprint/io-legal.pdf [https://perma.cc/X6JH-562L].

[39] *See* BERG, *supra* note 13, at 44.

[40] Jonathon W. Penney, *The Cycles of Global Telecommunication Censorship and Surveillance,* 36 U. PA. J. INT'L L. 693, 730–31 (2015). Satellite jamming is done by interfering with the uplink or downlink connections between Earth and the satellites based in space. Mountin, *supra* note 35, at 128; *see* Michel Bourbonnière,

magnetic communications system.[41] Additionally, some input-output (IO) operations are a specific type of manipulation of the electromagnetic spectrum.[42]

A practical application of jamming and interference by cyber means can be seen in two different disruption events involving Moscow. In the 1970s, the Soviet Union jammed western short-wave radio broadcasts in Poland and Lithuania to prevent political unrest directed against Moscow.[43] This jamming of the electromagnetic spectrum was similar to interference by cyber means in Estonia in the Tallinn Square incident.[44] The DDoS operations and the jamming operations both involved degradation of capabilities so severe that functions were lost.[45]

Interference by cyber means should be treated similarly to jamming in a *jus ad bellum* analysis. The *DoD Law of War Manual* draws this connection as well, finding that "bombardment of a network hub" and "the jamming of wireless communications"

Law of Armed Conflict (LOAC) and the Neutralisation of Satellites or Jus in Bello Satellitis, 9 J. CONFLICT & SEC. L. 43, 51–52 (2004).

[41] Deborah Housen-Couriel, *Disruption of Satellite Transmissions* Ad Bellum *and* In Bello*: Launching a New Paradigm of Convergence*, 45 ISR. L. REV. 431, 436 (2012). Jamming can also involve interference with a ground station for satellite jamming or between any transmitter and receiver on Earth. *See* U.S. DEP'T OF DEF., FM 3-14, ARMY SPACE OPERATIONS para. 2-83 (2019) [hereinafter ARMY SPACE OPERATIONS]; *see generally* ELECTRONIC WARFARE FUNDAMENTALS, *supra* note 37.

[42] IO captures the more traditional field of psychological operations and information gathering that are as historic as the history of war itself. *See* Hollis, *supra* note 6, at 1030–31. According to the DoD, IO also incorporates "electronic warfare" which uses electromagnetic and directed energy to control or attack the adversary's electromagnetic spectrum. JP FOR INFORMATION OPERATIONS, *supra* note 32, at II-12; Hollis, *supra* note 6, at 1031; *see also* ROSCINI, *supra* note 2, at 69. Electronic warfare also contributes to IO by "techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the [electronic magnetic spectrum]." JP FOR ELECTRONIC WARFARE, *supra* note 36, at I-14; *see also* Eugenia Georgiades, William J. Caelli, Sharon Christensen & W.D. Duncan, *Crisis on Impact: Responding to Cyber Attacks on Critical Information Infrastructures*, 30 J. MARSHALL J. INFO. TECH. & PRIV. L. 31, 42 (2013) (listing targets of electronic warfare other than computer systems).

[43] Flora Lewis, *Ripple from Poland: Europeans Will Feel It*, N.Y. TIMES (Aug. 28, 1980), https://timesmachine.nytimes.com/timesmachine/1980/08/28/111284168.html (noting that the Soviet Union went so far as to shut down all television broadcasts in the eastern part of Poland during the visit of Pope John Paul II).

[44] Poulsen, *supra* note 3.

[45] Further examples are in Section IV in the discussion about customary international law. However, this initial example is to highlight the similarities of jamming and DDoS.

are in the same category.[46] Thus, if jamming is not a use of force, then timeout errors (like DDoS) and other interference by cyber means are not a use of force either.[47]

C. Treaty Analysis Missing from Effects-Based Analysis

The *Tallinn Manual* and other effects-based approaches appear to support the existing *jus ad bellum* analysis for jamming.[48] The *Tallinn Manual* finds that, during peacetime, jamming is not internationally permitted; however, it does not classify jamming as a use of force even if employed by the military.[49] Others take the logic of the *Tallinn Manual* and go a step further, finding that jamming satellites can be a use of force.[50] The *Tallinn Manual* and the effects-based approach do not base this analysis on treaties or customary international law; instead, they rely on a theoretical approach of what States may do.[51]

This approach is misguided because States' use of force under the *jus ad bellum* analysis is best analyzed under customary international law and treaties.[52] In Article 38(1), the International Court of Justice (ICJ) recognizes international conventions, custom, and general principles of law as the building blocks for

---

[46] *See* DoD Law of War Manual, *supra* note 19, § 16.1.2.2. ("[T]he bombardment of a network hub, or the jamming of wireless communications, would not be considered cyber operations" that are more physically destructive "even though they may achieve military objectives in cyberspace.").

[47] Poulsen, *supra* note 3; Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. Rev. 43, 55 (2009); Hollis, *supra* note 6, at 1041 (stating that the instrumentality approach concludes cyber operations are not armed force because they lack characteristics associated with traditional military coercion).

[48] Rule 62 of the *Tallinn Manual* provides that "[t]he International Group of Experts concluded that the ITU regime governing use of the electromagnetic spectrum and associated earth orbits is well-established and applicable to their use for cyber activities." Tallinn Manual 2.0, *supra* note 4, at 296.

[49] *See id.* at 297 (stating that during peacetime, states have engaged in jamming operations, which is governed by the ITU and not permitted, whereas military radio interference operates under a different framework than the ITU). At first, the *Tallinn Manual* appears to treat interference along the electromagnetic spectrum the same: whether it is jamming or a DDoS, the application to the *jus ad bellum* is effects-based. *See id.* at 296 n.726.

[50] *See* Mountin, *supra* note 35, at 196, 123 ("[E]xisting 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.").

[51] *See* Waxman, *supra* note 6, at 436 ("A significant problem with this [consequence-based] view is that it fails to draw a principled distinction between cyberattacks and other nonmilitary political or economic interference, which can also cause significant harm.").

[52] *See* Hollis, *supra* note 6, at 1039.

international law interpretation.[53] International law is primarily expressed in treaties or international customs, and it is not based on desired outcomes.[54]

The U.N. Charter has particular importance because it embodies *both* customary and treaty law.[55] The "present cornerstone of the *jus ad bellum* matrix is the U.N. Charter, in particular its Article 2(4) and Chapter VII."[56] Placing the proper weight of the U.N. Charter results in a *jus ad bellum* analysis that focuses on the modality of States' actions.[57]

D. Use of Force and Armed Attack

Under Article 2(4) of the U.N. Charter, all member nations "shall refrain . . . from the threat or use of force against the territorial integrity or political independence of any State."[58] Therefore, an intervention involving an armed force is a use of force and violates this basic tenant of the U.N. Charter.[59] This understanding regarding the use of an armed force is also accepted as part of customary international law binding all States in the world.[60]

The most serious form of a use of force is an "armed attack" under Article 51 of the U.N. Charter.[61] An armed attack triggers the inherent right to self-defense.[62] *Jus ad bellum* limits the right

---

[53] Statute of the International Court of Justice art. 38, ¶ 1, June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 933 [hereinafter ICJ Statute]. Judicial decisions and teachings of highly qualified publicists can be a subsidiary means for interpreting international law. *Id.*

[54] Michael Milde, International Air Law and ICAO 3 (3d ed. 2016).

[55] 1 Oppenheim's International Law 31 (Robert Jennings & Arthur Watts eds., 9th ed.1996). Custom had historically taken preeminence over treaty in defining customary international law. *See id.*

[56] *See* Roscini, *supra* note 2, at 43. For example, the U.N. Charter permits the inherent right to individual or collective self-defense under Article 51, in part because this is a just cause for military action. *See* U.N. Charter art. 51; *see also* DoD Law of War Manual, *supra* note 19, § 1.11.1.1 n.186.

[57] The U.N. Charter's focus on the modality has been labeled by some as an "instrumentality" or instrument-based approach. Hollis, *supra* note 6, at 1040–42 (stating that the instrumentality approach has some support in Article 41 of the U.N. Charter but runs into issues when applied to shutting down communication systems).

[58] U.N. Charter art. 2, ¶ 4.

[59] 1 Oppenheim's International Law, *supra* note 55, at 428–29.

[60] *Id.*; Robert Kolb, An Introduction to the Law of the United Nations 66 (Katherine Del Mar trans., 2010).

[61] *See* U.N. Charter art. 51.

[62] *Id.*

to self-defense to armed attacks.[63] However, the United States considers a use of force and an armed attack in the same category because both give rise to the right of self-defense.[64]

According to the ICJ in the *Nicaragua v. United States* decision, the "most grave [form] of the use of force" is an armed attack.[65] Attacks are distinguished based on their "scale and effects."[66] The scale and effects test also demonstrates that not all violent military actions rise to armed attacks, and some military actions may be classified at a lower standard as a "mere frontier incident."[67]

A recent example of a mere frontier incident is the clash between Indian and Chinese military forces in the Ladakh region, in which twenty Indian troops were killed.[68] In that case, neither side indicated there was an armed attack while blaming the

---

[63] *See* Beard, *supra* note 20, at 78 n.42 (citing Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 51 (Nov. 6)). The right to use armed force in self-defense "is also dependent on meeting a high threshold for attribution of the armed attack." *Id.*; *see also* Ryan Patterson, *Silencing the Call to Arms: A Shift Away from Cyber Attacks as Warfare*, 48 LOY. L.A. L. REV. 969, 985 (2015).

[64] DOD LAW OF WAR MANUAL, *supra* note 19, § 1.11.5.2 ("The United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force."); *see also* Waxman, *supra* note 6, at 427 ("The dominant view in the United States and among its major allies has long been that the Article 2(4) prohibition of force and the complementary Article 51 right of self-defense apply to military attacks or armed violence."). The U.S. position, that an armed attack and a use of force both give rise to a use of force, is not accepted by the majority of nations. *See* DOD LAW OF WAR MANUAL, *supra* note 19, § 1.11.5.2.

[65] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 191 (June 27); *see also* KOLB, *supra* note 60, at 77 (noting the ICJ has "always insisted on the fact that all uses of force are prohibited under article 2 § 4 but not all these uses are automatically armed attacks triggering the application of article 51.").

[66] Nicar. v. U.S., 1986 I.C.J. at 103, ¶ 195. Low level uses of force, therefore, do not trigger the inherent right to self-defense because they do not rise to the level of an armed attack under Article 51. *See* ROSCINI, *supra* note 2, at 45.

[67] Nicar. v. U.S., 1986 I.C.J. at 103, ¶ 195. Additionally, a "use of force" requires an element of coercion. "Armed force is only one form of coercion and is the easiest to identify" and "[l]ike past efforts to define Article 2(4) 'force' as coercion, efforts to expand its coverage beyond armed force so as to include violations of sovereign domain such as propaganda or political subversion never gained significant traction." Waxman, *supra* note 6, at 428–30.

[68] Soutik Biswas, *India-China Clash: 20 Indian Troops Killed in Ladakh Fighting*, BBC NEWS (June 16, 2020), https://www.bbc.com/news/world-asia-53061476 [https://perma.cc/E4T5-N7XF]. "China did not confirm any casualties, but accused India" of crossing the border. *Id.* India also accused China of crossing the border. *Id.*

other country for the skirmish.[69] Thus, small border incidents like this one—even those that result in the loss of life—are not considered an armed attack under the U.N. Charter.[70]

Some effects-based proponents reject the scale and effects test developed in the *Nicaragua* decision, finding that qualitative indicators based on the consequences (e.g., number of deaths) are more in line with current international law.[71] The problem with dropping the scale and effects test for a multi-faceted criteria test is that doing so blurs the lines of what constitutes a use of force. An effects-based model can lead to the conclusion that virtually any cyber operation could be an armed attack.[72] Without reason, this lack of clarity in the *jus ad bellum* analysis could lead to a more opaque approach to cyberspace based on policy goals rather than international law. Such an approach is also problematic because even military action resulting in loss of life is not necessarily an armed attack.[73] Thus, it is unclear how much loss of life caused by a cyber operation would constitute an armed attack.

Perhaps one of the most troubling aspects of the effects-based approach is that it could upend developed norms on what is considered "coercion" for a use of force analysis. For example, the classification of economic and political coercion as not a use of force is supported by the *travaux préparatoires* of the U.N. Charter.[74] The *Tallinn Manual*'s effects-based approach appears to endorse the traditional view of political and economic coercion.[75] Yet, the economic impact of cyber operations can have much more devastating consequences and would, thus, upend conventional coercion norms.[76]

---

[69] *Id.*

[70] *See, e.g.*, Land and Maritime Boundary Between Cameroon and Nigeria (Cameroon v. Nigeria; Eq. Guinea intervening), Judgment, 2002 I.C.J. 303, ¶¶ 311, 314, 319 (Oct. 10).

[71] *See* Schmitt, *supra* note 4, at 573, 589.

[72] *See* Reese Nguyen, *Navigating* Jus Ad Bellum *in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079, 1123 (2013).

[73] *See* Cameroon v. Nigeria, 2002 I.C.J. at 451–52, ¶¶ 311, 314, 319.

[74] Schmitt, *supra* note 4, at 573–74. Brazil attempted to include a provision to define the "use of force" as including economic sanctions, but this was rejected and is not reflected in Article 2(4) of the U.N. Charter. *See* Beard, *supra* note 20, at 117 n.198.

[75] TALLINN MANUAL 2.0, *supra* note 4, at 331; *see also* Schmitt, *supra* note 4, at 573–74.

[76] *See* Hollis, *supra* note 6, at 1042.

The *Tallinn Manual* creates a "Jekyll and Hyde" approach to the U.N. Charter because cyberspace is treated as though it is outside of the U.N. Charter framework for physical effects-based cases but inside the U.N. Charter framework for political and economic coercion.[77] The *travaux préparatoires* supports the obscure treatment of cyberspace; the Brazilian delegation proposed that Article 2(4) include a prohibition against the use of "economic measures," but the proposal was rejected.[78] Likewise, efforts to define "force" to include "propaganda or political subversion never gained significant traction."[79]

The rejection of economic and political coercion as force reinforces the idea that the U.N. Charter is limited to traditional military instruments.[80] Thus, the *Tallinn Manual* runs afoul by going outside the U.N. Charter in its classification of certain cyber operations not as uses of force while attempting to remain under the U.N. Charter for political and economic coercion. Such a contradictory classification runs counter to Article 31 of the Vienna Convention on the Law of Treatises (VCLT), which states that a treaty must be read as one congruent document.[81]

E. Effects-Based Approach Misstep

Harold Koh implicitly endorsed some of the effects-based approaches, stating that "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[82] Likewise, the DoD references the effects-based approach in some manuals and doctrines.[83] Such references are

---

[77] *See id.*

[78] *See* U.N. Conference on International Organization, *Summary Report of Eleventh Meeting of Committee I/1*, ¶¶ 7–8, U.N. Doc. 784, I/1/27 (Vol. VI) (June 5, 1945) [hereinafter *Summary Report of Eleventh Meeting*] (rejecting the Brazilian delegation's suggested inclusion of a prohibition against "economic measures"); U.N. Conference on International Organization, *Amendments to the Dumbarton Oaks Proposals Presented by the Brazilian Delegation*, at 252–53, U.N. Doc. 2, G/7 (e)(4) (May 6, 1945) [hereinafter *Proposal Presented by the Brazilian Delegation*]; *see also* Beard, *supra* note 20, at 117 n.198.

[79] Waxman, *supra* note 6, at 430.

[80] Michael Gervais, *Cyber Attacks and the Laws of War*, 30 Berkeley J. Int'l L. 525, 536–37 (2012) ("By explicitly excluding economic coercion from the definition of force in the drafting of Article 2(4), and implicitly rejecting ideological and diplomatic instruments as well, the drafters signaled that the determination of whether a nation has used force in violation of Article 2(4) focuses only on military instruments.").

[81] *See* Vienna Convention on the Law of Treaties, *supra* note 12, art. 31.

[82] *See Koh Remarks*, *supra* note 24, at 4.

[83] *See, e.g.*, DoD Law of War Manual, *supra* note 19, § 16.2.2 n.15.

leading some commentators to speculate that the United States has embraced the effects-based approach.[84]

However, both Koh and the DoD do not go so far as to endorse the *Tallinn Manual* and the effects-based approach entirely. Koh also indicated that the old analysis of *jus ad bellum* should not be rejected for new technology.[85] Additionally, the DoD Law of War Manual places the main *jus ad bellum* analysis for cyberspace on the U.N. Charter.[86]

More recently, in March 2020, the DoD General Counsel commented in public remarks that initiatives like "the *Tallinn Manual* can be useful to consider, but they do not create new international law."[87] Such a statement seems to indicate that not everything in the *Tallinn Manual* or everything in the effects-based analysis is considered an accurate restatement of the United States' view of international law in cyberspace. The DoD General Counsel's March 2020 remarks also drove home that Article 2(4) of the U.N. Charter and customary international law should be the basis for the "use of force" analysis.[88]

However, the General Counsel at least partially endorsed some aspects of the effects-based analysis, stating "DoD lawyers consider whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine."[89] Despite leaving room for some type of effects-based analysis, the explicit callout of the *Tallinn Manual* demonstrates that the DoD is not ready to completely abandon the historical analytical framework for the use of force as applied to cyber operations.[90]

---

[84] *See, e.g.*, Catherine Lotriionte, *Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law*, 3 CYBER DEF. REV. 73, 81, 104 n.49 (2018).

[85] *See Koh Remarks*, *supra* note 24, at 3, 7–8.

[86] DOD LAW OF WAR MANUAL, *supra* note 19, § 16.3.1.

[87] Paul C. Ney, Jr., Gen. Couns., U.S. Dep't of Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020) (transcript available at https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ [https://perma.cc/5AP6-A54T]) [hereinafter Ney Remarks].

[88] *Id.* (noting that whether "a military cyber operation may constitute a use of force" is based on the analysis "within the meaning of Article 2(4) of the U.N. Charter and customary international law").

[89] *Id.*

[90] *See id.* ("Initiatives by non-governmental groups like those that led to the *Tallinn Manual* can be useful to consider, but they do not create new international law, which only states can make."). A further indication in the speech that the DoD does have the expansive view of use of force for cyberspace is that the

Besides the United States, many other nations have made public statements or indications of some version of the effects-based approach to determine if a use of force has occurred where "traditional" kinetic force could have caused comparable damage.[91] Specifically, Australia, France, Germany, the Netherlands, and the U.K. have had public officials make statements that blatantly or implicitly endorse this view.[92]

In determining if interference by cyber means is a use of force in cyberspace, an analysis based on the U.N. Charter—not just potential State actions—is required.[93] It is nearly impossible in international law to run counter to the U.N Charter.[94] Under Article 103 of the U.N. Charter, in the event of *any* conflict between the obligations of the U.N. Charter and *any* other international agreement, "[the] obligations under the [U.N.] Charter shall prevail."[95] The VCLT reiterates the obligation to adhere to the U.N. Charter above all other treaties.[96]

The remaining Sections, dealing with Article 41 of the U.N. Charter and customary international law for electromagnetic interference, demonstrate that cyber interference is like other electromagnetic interference and should be addressed by the U.N. Charter and customary international law under a *jus ad bellum* analysis.

DoD will apply some *jus in bello* principles as a matter of policy because a cyber operation may not technically constitute a use of force. *Id.* ("*[J]us in bello* principles, such as military necessity, proportionality, and distinction, continue to guide the planning and execution of military cyber operations, even outside the context of armed conflict.").

[91] Przemyslaw Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, THE HAGUE PROGRAM FOR CYBER NORMS POL'Y BRIEF, Mar. 2020, at 9.

[92] *Id.*

[93] *See* ICJ Statute, *supra* note 53, art. 38, ¶ 1.

[94] *See* 1 OPPENHEIM'S INTERNATIONAL LAW, *supra* note 55, at 1216. Article 26 of the Vienna Convention on the Law of Treaties states: "Every treaty in force is binding upon the parties to it and must be performed by them in good faith." Vienna Convention on the Law of Treaties, *supra* note 12, art. 26. Therefore, not operating within the bounds of the U.N. Charter would leave the United States, or any other country, running afoul of its treaty obligations.

[95] U.N. Charter art. 103.

[96] Vienna Convention on the Law of Treaties, *supra* note 12, art. 30, ¶ 1; *cf.* 1 OPPENHEIM'S INTERNATIONAL LAW, *supra* note 55, at 1215–16.

III. ARTICLE 41 OF THE U.N. CHARTER AND CYBER OPERATIONS

A. Article 41 of the U.N. Charter: Plain Meaning

Article 41 of the U.N. Charter is included in Chapter VII of the U.N. Charter.[97] Chapter VII of the U.N. Charter covers the collective security actions that the U.N. Security Council can authorize in the case of threats to the peace, breaches of the peace, or acts of aggression.[98] Chapter VII actions can involve a use of force if they are Article 42 actions.[99] Actions not involving a use of force are contained primarily in Article 41.[100] Article 41 states, "The Security Council may decide what measures not involving the use of armed force are to be employed. . . . These may 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."[101]

Article 41 covers measures that are not force with the phrase "not involving the use of armed force."[102] Thus, the list of actions is classified explicitly as not a use of force.[103] Under Article

---

[97] U.N. Charter art. 41.

[98] *Id.*; Kolb, *supra* note 60, at 26. Of note, a State's action need not qualify as an "act of aggression" for the Security Council to take action, and the Security Council could also act in the event of a breach of the peace or a threat to peace. *Id.* at 80. In a similar vein, the Security Council's Chapter VII authorized actions may infringe on the sovereignty of a State and even intervene in a State's domestic affairs. *See* Benedetto Conforti & Carlo Focarelli, The Law and Practice of the United Nations 202 (4th ed. 2010).

[99] Article 42 of the U.N. Charter states:

> Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.

U.N. Charter art. 42; *see* Conforti & Focarelli, *supra* note 98, at 259.

[100] U.N. Charter art. 41; Kolb, *supra* note 60, at 79; *see also* Conforti & Focarelli, *supra* note 98, at 231–34.

[101] U.N. Charter art. 41 (emphasis added).

[102] *Id.*

[103] The U.N. Security Council has referenced Article 41 to stress that it did not intend to authorize forcible action. There is a slight difference in the wording in Article 2(4) which prohibits Members from the "use of force," whereas Article 41 has the additional word "armed" in front of "force." U.N. Charter arts. 2 , ¶ 4, 41. Some commentators have speculated that the use of the word "armed" in front of Article 41 is a qualifier that may distinguish Article 41 from Article 2(4). *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International*

41, actions that do not rise to the level of a use of force include the interruption of all postal, telegraphic, radio, and other forms of communication.[104]

The list of U.N. Security Council actions under Article 41 has the nature of sanctions because of the actions' focus on economic impact.[105] Additionally, the list of actions does not have to be imposed in its entirety, but the cumulative application of all the measures would have the effect of near or total isolation.[106]

Giving "communications" its ordinary meaning finds support in the purpose of Article 41 of the U.N. Charter. Under Article 31(1) of the VCLT, a treaty is interpreted by its object and purpose.[107] The object and purpose of Article 41 are to cover the interruption of communication of all types.[108] If some forms of communication were intended to be excluded, then the phrase "other means of communication" would not have been included. "'[O]ther means of communications' fairly encompasses computer communications and communication over computer networks."[109] Thus, the context of Article 41 also denotes all communication interruptions must be treated the same whether they are over telephones, wireless signals, broadcasting, radio interference, or computer network connections.[110]

The *travaux préparatoires* of the U.N. Charter also confirm the ordinary meaning of "interruption" and "communication."[111] At

---

Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNAT'L L. 885, 904–05 (1999). However, the text's plain meaning and the structure of the U.N. Charter support a congruent interpretation of "force." *See* Waxman, *supra* note 6, at 427–28. For example, the preamble of the U.N. Charter sets out the goal "that armed force shall not be used, save in the common interest." U.N. Charter preamble.

104 KOLB, *supra* note 60, at 82–83.

105 *See* CONFORTI & FOCARELLI, *supra* note 98, at 233–34.

106 *Id.*

107 Vienna Convention on the Law of Treaties, *supra* note 12, art. 31, ¶ 1.

108 *See* KOLB, *supra* note 60, at 83. Although, practice has shown some limitations to limiting communication for humanitarian reasons if the situation has called for it. *Id.*

109 David J. DiCenso, *Information Operations: An Act of War?*, AIR & SPACE POWER CHRONS., July 31, 2000, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/dicenso1.pdf [https://perma.cc/89YA-MGGT].

110 *See id.*

111 *See* Vienna Convention on the Law of Treaties, *supra* note 12, arts. 31, ¶ 1, 32; THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 12, at 36–38 (stating that under Article 32 of the VCLT, preparatory works, such as the *travaux préparatoires*, can be used to confirm the meaning resulting from the application of Article 31).

the Dumbarton Oaks Conference, the Soviet Union proposed interruption of communications as action short of armed force.[112] After some discussion, the United States and the U.K. representatives agreed to include interruption of communication in the draft version of what would become Article 41, which was submitted to the San Francisco Conference.[113]

Further discussions at the San Francisco Conference included the Greek representative's remarks that the Security Council is empowered to take a range of measures. The representative indicated that the interruption of communication or severance of diplomatic relations was a less severe option, and it differed from sanctions by armed forces.[114] There were no objections to the Greek representative's observation on this point.[115] The representatives who drafted the U.N. Charter likely believed the Security Council had wide latitude in interruption of communications.

Some may argue that the communication interruption under Article 41 only applies to communication between States, and the drafting of Article 41 was meant to be a form of keeping communication from going in and out of a country, not within a country.[116] The modern example would be an "infoblockade," which "blocks all electronic information from entering or leaving a State's borders."[117] However, the profound changes in communication essentially make all electronic communications cross State borders, especially in the age of satellite communica-

---

[112] *See* RUTH B. RUSSELL, A HISTORY OF THE UNITED NATIONS CHARTER: THE ROLE OF THE UNITED STATES, 1940–1945, at 466 (1958).

[113] *Id.*; U.N. Conference on International Organization, *Observations of the Government of Venezuela on the Recommendations Adopted at the Dumbarton Oaks Conferences for the Creation of a Peace Organization*, at 211, U.N. Doc 2, G/7(d) (1) (Oct. 31, 1944) [hereinafter *Observations of the Government of Venezuela*] ("[M]easures, not including the use of armed force . . . might include total or partial interruption of railway, maritime air, postal, telegraphic, radiotelegraphic and other communications.").

[114] *See* U.N. Conference on International Organization, *Verbatim Minutes of the Fourth Plenary Session*, at 286, 288, U.N. Doc. 24, P/8 (Apr. 29, 1945) [hereinafter *Verbatim Minutes*] (citing comments by John Sofianopoulos, Chairman of the Delegation of Greece).

[115] *See id.*

[116] *See* KOLB, *supra* note 60, at 82–83 (noting the text of Article 41 provides for the "interruption of communication of all types *with* the sanctioned State") (emphasis added).

[117] Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1188 n.137 (2011).

tion.[118] Thus, even taking the interruption at face value, it would be difficult to find a form of electromagnetic communication that at some point does not cross State boundaries.[119]

In the 1970s, the United States held that Article 41 of the U.N. Charter can be construed broadly.[120] During the Iran hostage crisis, the acting U.S. Attorney General determined that

> [t]he range of measures appears to be quite broad. . . . Article 41 can be construed to include an international news embargo: a complete or selective restriction of news transmitted—either directly or indirectly. . . . It would at the very least include *severance of the means of transmission that link* the embargoed country with the outside world, *e.g.*, *microwave transmission links*.[121]

The acting Attorney General also surmised that the U.S. President might possess the authority to sever communication links without a Security Council resolution unilaterally.[122] In 1979, interference by cyber means was not a widely known capability, but the United States' initial position appears to be that electromagnetic interference (i.e., cyber means) falls under Article 41.[123]

B. Effects-Based Approach Rejection of the U.N. Charter

The *Tallinn Manual* initially appears to agree with the ordinary approach to communication and interruption under Article 41 of the U.N. Charter in Rule 76, which is in the context of a threat to peace, breach of the peace, or an act of aggression.[124] Likewise, interruption is generally given its ordinary meaning

---

[118] *See* Housen-Couriel, *supra* note 41, at 432, 436, 442. There is also a general wariness to treat cyber activities that involve cross-border intrusions too broadly as a violation of sovereignty. Beatrice A. Walton, Note, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law*, 126 Yale L.J. 1460, 1476–77 (2017).

[119] *See* Housen-Couriel, *supra* note 41, at 432, 436, 442.

[120] *See* The President's Auth. to Take Certain Actions Relating to Commc'ns from Iran, 4A Op. O.L.C. 153, 153 (1980), https://www.justice.gov/file/22336/download [https://perma.cc/88NL-9ZBM].

[121] *Id.* at 153–54 (emphasis added).

[122] *See id.* at 154.

[123] *See id.* at 153–54.

[124] *See* Tallinn Manual 2.0, *supra* note 4, at 357–58 (stating that under Rule 76, the U.N. Security Council may authorize non-forceful measures including cyber operations). For "communication," the *Tallinn Manual* states that under Article 41, "the Security Council may decide upon a complete or partial interruption of cyber communications with a State or non-State actor." *Id.* at 358.

for most effects-based approaches.[125] Thus, the effects-based approach initially appears to endorse Article 41.[126]

However, the effects-based approach finds itself too wedded to the consequence of cyber operations. Michael Schmitt added the additional qualifier that the U.N. Security Council is limited under Article 41 in that "physical harm to persons or objects could not be authorized pursuant to Article 41."[127] In Schmitt's analysis, there is no citation to other parts of the U.N. Charter or the *travaux préparatoires* indicating why the U.N. Security Council should include a qualifier of physical harm to persons or objects.[128] The effects-based approach would state that under Article 2(4) "force" must denote violence, but the means that bring about the violence—whether kinetic or electronic—does not matter.[129] Yoram Dinstein also advocates that the means of attack do not matter, but the violent consequences do.[130]

Other effects-based supporters have also come to this conclusion for satellite interference. One supporter draws this conclusion "because drafters of the Charter never contemplated satellite signal interference would be used to cause physical damage and human injury."[131] The main argument appears to be an attack on U.N. Charter drafters themselves. Specifically, according to Schmitt, the drafters "took a cognitive shortcut by framing the treaty's prohibition in terms of the *instrument* of coercion employed—force."[132] However, there are major concerns with Schmitt's arguments. Namely, that

> [i]t is also possible . . . to view the word "force" as conveying what appears to be its plain meaning in the text: physical armed force . . . . [I]t is a cognitive transcription of the desire of states to limit the most serious prohibitions and penalties of the U.N. Charter to the instrument whose misuse gave rise to the U.N. Charter regime . . . .[133]

---

[125] *See* Schmitt, *supra* note 4, at 584. Schmitt states that interruption of cyber communication is included, stating, "An interruption could be broad in scope, as in blocking cyber traffic to or from a country, or surgical, as in denying a particular group access to the Internet." *Id.*

[126] *See generally id.*

[127] *Id.*

[128] *See id.*

[129] YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 88 (5th ed. 2011).

[130] *See* Dinstein, *supra* note 9, at 103.

[131] Mountin, *supra* note 35, at 192.

[132] Schmitt, *supra* note 4, at 573.

[133] *See* Beard, *supra* note 20, at 118 (citing D. W. BOWETT, SELF-DEFENSE IN INTERNATIONAL LAW 148 (1958) ("Taking the words in their plain, common-sense meaning, it is clear that, since the prohibition is of the 'use or threat of force[,]'

If the terms "communication" and "interruption" are to be given their ordinary meaning, then the term "force" should likewise be given its ordinary meaning using the established modes of treaty interpretation.[134]

Another effects-based argument is that approaches to the prohibition of force based on the type of instrument are outdated in modern warfare. The argument states that warfare and the meaning of "force" have evolved because historic interpretations leave the world "ossified at the level of military technology that existed at the end of World War II."[135] Some have even stated that all non-physical forces, such as electronic jamming and cyberspace, should be differently analyzed because they did not exist at the U.N. Charter's drafting.[136]

It is historically disingenuous to assume the U.N. Charter drafters were unaware of the results of interference, including in the physical world. Jamming during peacetime occurred as early as the 1930s, with Austria jamming Nazi broadcasts, Germany and Russia jamming each other, and Italy jamming Soviet broadcasts.[137] When the U.N. Charter was drafted, the International Telegraph Union was reformed into the International Telecommunication Union (ITU) to deal with the effects of harmful interference.[138] ITU's first order of business was to condemn jamming, which it did in every resolution from 1947 onward.[139]

There are historical examples of interference along the electromagnetic spectrum in wartime, indicating this technology was well-known. The Army Signal Corps was formed in 1860, and the management of the telegraph became its responsibility.[140] By World War I, jamming enemy signals had become routine for communication lines,[141] and by World War II, jamming in-

---

they will not apply to economic or political pressure but only to physical, armed force.")).

134 Vienna Convention on the Law of Treaties, *supra* note 12, art. 31, ¶ 1.

135 Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, 76 INT'L L. STUD. 73, 84 (2002).

136 *See* Li, *supra* note 4, at 187–88.

137 *See* BERG, *supra* note 13, at 44.

138 *See id.* at 39.

139 *See* Penney, *supra* note 40, at 723–24.

140 *See* REBECCA ROBBINS RAINES, GETTING THE MESSAGE THROUGH: A BRANCH HISTORY OF THE U.S. ARMY SIGNAL CORPS 7, 9 (1996), https://history.army.mil/html/books/030/30-17-1/CMH_Pub_30-17-1.pdf [https://perma.cc/DM7D-SEDP].

141 *See id.* at 263.

cluded radio and radar navigational aids for aircraft and seacraft.[142] This substantial, historical evidence demonstrates that interference along the electromagnetic spectrum was well-known during the U.N. Charter's formation.

In World War II, the Germans employed the Fritz X, also known as the Ruhrstahl X-1.[143] The precision-guided, armor-piercing bomb utilized against Allied ships used a radio command missile system, which demonstrated the ability to affect the physical world in person-to-person contact and in person-to-machine control.[144] The Allies were able to develop various electronic countermeasures to interfere with the Fritz X.[145] Fritz X radio pulses and the countermeasures to prevent physical destruction demonstrate that the use of the electromagnetic spectrum to alter the physical world existed before the U.N. Charter's initial drafting.[146]

Besides historical examples, the provisions on the use of force make little sense if they are not considered in the framework of the U.N. Charter and its organization.[147] The U.N. Charter's purpose of being the preeminent international document on *jus ad bellum* analyses would capture all existing forms of warfare and those short of warfare, including electromagnetic spectrum interference.

C. Travaux Préparatoires of Article 41

Other portions of the U.N. Charter's drafting history demonstrate that interference by cyber means likely does not rise to the level of a use of force. At Dumbarton Oaks, the Soviets argued for the Security Council to have measures that were "short of

---

[142] *See* George Raynor Thompson & Dixie R. Harris, The Signal Corps: The Outcome (Mid-1943 Through 1945) 89 (1966). The U.S. Army continued to be the leader in electromagnetic interference through the 1990s with U.S. Air Force Signals Intelligence "at the leading edge on cybersecurity." *See* Clarke & Knake, *supra* note 5, at 102.

[143] *Fritz X Glide Bomb - German WWII*, WorldWar2Headquarters, http://worldwar2headquarters.com/HTML/museums/Chino/fritz-x-bomb.html [https://perma.cc/7JAF-W43X].

[144] *See id.*

[145] *See id.*; *see also* Thompson & Harris, *supra* note 142, at 301 ("[W]hen radar pulses burst into the realms of radio and when inhuman radio-guided missiles put in their terrifying appearance, the electromagnetic frequencies employed by the new military engines became suddenly too dangerous to neglect. The spectrum itself became a weapon that could be deadly.").

[146] *See generally* Kolb, *supra* note 60, at 20 (noting the historical gatherings leading up to the United Nations' establishment).

[147] *See* Conforti & Focarelli, *supra* note 98, at 14.

armed force," which member States could then use in the event of a threatening situation.[148] The proposed measures included total or partial interruption of postal, telegraphic, radiotelegraphic (i.e., radio broadcasts), and other communications, and later became Article 41 of the U.N. Charter.[149]

At the San Francisco conference, members clarified that the most critical aspect of the draft proposals for Article 41 from Dumbarton Oaks was that they did *not* involve force.[150] Members pointed out that Article 41 itself and interruption of communication did not amount to a use of force or military actions.[151]

---

[148] *See* RUSSELL, *supra* note 112, at 466.

[149] *Observations of the Government of Venezuela*, *supra* note 113, at 211.

[150] *See* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 12, at 624 ("The most important limitation on Art. 41 is that it may not involve the use of armed force. The application of armed force is regulated in Art. 42 . . . ."). Article 41 may in fact be the best example of what is not a use of force because it is a non-exhaustive list. The full Soviet list included:

> (a) appeal by the Council to the parties to settle things peacefully; (b) a similar appeal warning of possible use of other measures; (c) economic pressure on the parties to a dispute; (d) severance of diplomatic relations; (e) severance of economic relations, including interruption of transportation and communications; (f) provision, by states "not possessing sufficient armed forces," of territory for bases; (g) sea and land blockade; (h) naval and air demonstrations; (i) air raids on military objectives in an aggressor country; and (j) military operations by member states against an aggressor.

See RUSSELL, *supra* note 112, at 466 n.56.

[151] *See* U.N. Conference on International Organization, *Replacement for Pages 19–21 of Skeleton Charter – Second Draft*, at 531, U.N. Doc. WD 161, CO/78(1) (June 4, 1945) (Article 45, which eventually became Article 41, was labeled "Non-Military Sanctions"); *Verbatim Minutes*, *supra* note 114, at 288 ("[T]he Council should be empowered to determine what measures could be employed . . . . Those measures *could range from the interruption of means of communication* or the mere severance of diplomatic relations to the application of sanctions by armed force.") (emphasis added). In discussing Article 47x (now Article 44), Mr. Robertson (the Canadian representative) asked "whether the expression 'to use force' appears anywhere else in the Charter. The usual formula is to say 'take action under some articles.'" U.N. Conference on International Organization, *Summary Report of Fourteenth Meeting of Coordinate Committee*, at 81, Doc. WD 288, CO/116 (June 13, 1945). Chairman Mr. Pasovlsky—the U.S. representative who was present at Dumbarton Oaks and is considered the primary author of the UN Charter—referred to Article 45 (now Article 41) "which speaks of 'measures not involving the use of armed force.'" *Id.* One could, after reading the *travaux préparatoires* for Article 41, improperly conclude that a State's military could not be involved in interruption of radio, telegraphic, or other forms of communication through the use of the phrase "nonmilitary." *See* RUSSELL, *supra* note 112, at 466 (referring to the measures as "nonmilitary"). However, Article 41-type measures can be enforced with the use of a State's military based on previous ICJ opinions and a long history of State practice. *See* Oil Platforms (Iran v. U.S.),

The ICJ reinforced this view in the *Tadić* decision when it found that the ordinary meaning of Article 41 did not involve the use of force.[152]

Additionally, Article 41 is the *best* example of what is not a use of force. When the Soviets proposed a full list of measures at Dumbarton Oaks,[153] the U.K. and U.S. initially opposed the list.[154] However, the British and Americans finally relented by ensuring that Article 41 was worded in permissive terms to indicate a non-exhaustive list.[155] By the San Francisco conference, the list's non-exhaustive nature seemed to be a settled matter since the debate centered on making sure the option for "partial" or "complete" interruption only related to communication and not diplomatic encounters.[156]

Decades later, in the *Tadić* decision, the ICJ clarified that Article 41 is a non-exhaustive list, specifically stating that Article 41 could include actions such as creating an international tribunal.[157] Thus, even if one argues cyberspace did not exist at the U.N. Charter's inception and could not have fallen under the Article 41 framework,[158] the non-exhaustive nature demonstrates that all communication interruptions are similar and do not involve a use of force.[159] The phrase "other communica-

---

Judgment, 2003 I.C.J. 161, ¶ 34 (Nov. 6) (strongly reaffirming the distinction made by the ICJ in *Military and Paramilitary Activities in and Against Nicaragua*).

[152] Prosecutor v. Tadić, Case No. IT-94-1-T, Decision on the Defence Motion on Jurisdiction, ¶ 26 (Int'l Crim. Trib. for the Former Yugoslavia Aug. 10, 1995) ("The Article, on its face, does not limit the discretion of the Security Council to take measures not involving the use of armed force.").

[153] *See* RUSSELL, *supra* note 112, at 466 n.56.

[154] *See id.* at 466.

[155] *See id.*

[156] U.N. Conference on International Organization, *Summary Report of Twenty-Third Meeting of Coordination Committee*, at 152–53, Doc. WD 442, CO/206 (Sept. 5, 1945) ("[T]he article had been slightly revised so that the words 'partial or complete' *would apply to the interruption of communication channels and not to the severance of diplomatic relations.*") (emphasis added).

[157] *Tadić*, Case No. IT-94-1-T, Decision on the Defence Motion on Jurisdiction, ¶¶ 26–29 ("Chapter VII confers very wide powers upon the Security Council and no good reason has been advanced why Article 41 should be read as excluding the step, very appropriate in the circumstances, of creating the International Tribunal to deal with the notorious situation existing in the former Yugoslavia.").

[158] Schmitt, *supra* note 4, at 572.

[159] Jann K. Kleffner & Heather A. Harrison Dinniss, *Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations*, 89 INT'L L. STUD. 512, 516 (2013) ("Under Article 41 of the Charter, the Security Council may also mandate non-forceful measures be taken in situations it deems to be a threat to the peace, breach of the peace or act of aggression. Such enforcement measures may

tions" encompasses cyberspace because actions in cyberspace are communicative tools by their very nature.[160]

There are recent indications that military actions in cyberspace, like other forms of communication interruption, do not rise to the level of a use of force.[161] For example, in its *2018 Department of Defense Cyber Strategy*, the DoD stated that the U.S. military would "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[162] Likewise, Russia, China, and North Korea are using their militaries to operate in cyberspace outside of armed conflict with various actions, including espionage and interference by cyber means.[163]

D. Economic Impacts of Jamming

The leading interpretation is that Article 2(4) covers "armed coercion" and does not extend in scope to political or economic coercion.[164] There can be severe impacts under Article 41 that can even lead to death, but that does not mean they rise to the level of a use of force.[165] Marco Roscini stated that "economic sanctions that cause starvation among the population are not a use of armed force" and "sanctions may be enforced with the use of weapons, but are not weapons themselves, as implied in Article 41 of the UN Charter."[166] Likewise, cyber operations may have severe effects, but it is not the effects or second-order consequences that make a cyber operation a use of force.[167]

---

include, *inter alia, partial or total disruption of telecommunications which may well contain a cyber element.*") (emphasis added).

[160] *See* U.S.-China Econ. and Sec. Rev. Comm'n, *supra* note 17, at 215 ("[E]lectronic manipulation" includes jamming of "different types of electronic interference or signals that flood communications channels.").

[161] *See* Gervais, *supra* note 80, at 535 ("[C]yber espionage and exploitation fails to rise to the level of warfare because the purpose or outcome of both cyber espionage and exploitation is to monitor information and not to affect a computer system's functionality."); *see also* Beard, *supra* note 20, at 139 (asserting that states have resisted treating cyber espionage, sabotage, and subversion as "cyberwar").

[162] *See* U.S. Dep't of Def., 2018 Department of Defense Cyber Strategy 1 (2018) https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [https://perma.cc/3GLZ-AFHX].

[163] *See* Clarke & Knake, *supra* note 5, at 18–19 (referring to Russia's NotPetya operation as an "operation run by a military unit").

[164] *See, e.g.*, Schmitt, *supra* note 103, at 911–12.

[165] *See* Roscini, *supra* note 2, at 49.

[166] *Id.*

[167] *See* Schmitt, *supra* note 103, at 912–13.

State practice has demonstrated that "economic" coercion is not considered a use of force in communication interruptions; thus, creating implications for cyberspace. For example, multiple jamming efforts of satellites have carried television broadcasts throughout the Middle East.[168] A primary culprit is Iran, having jammed BBC Persia television in 2009 and 2010;[169] the Eutelsat satellite constellation for about a decade in the 2010s;[170] and the United States broadcasts to its region in 2012.[171]

Iranian jamming demonstrates that the interruption of television broadcast communications falls below a use of force. The complaint was not brought to the U.N. Security Council's attention but to the ITU's.[172] In other words, instead of a U.N. body—which handles threats to peace and security—the ITU dealt with the Eutelsat complaints.[173]

A few States have made public statements that cyber operations causing severe financial impact may violate the non-intervention principle, which falls short of classifying cyber operations as a use of force.[174] Thus, States' public statements and the considerable economic losses caused by jamming both call into question the premise of the effects-based analysis.[175]

---

[168] *See supra* notes 170–72 and accompanying text.

[169] *See* Anne Wainscott-Sargent, *Fighting Satellite Interference on All Fronts*, VIA SATELLITE (Mar. 1, 2013), https://www.satellitetoday.com/uncategorized/2013/03/01/fighting-satellite-interference-on-all-fronts/ [https://perma.cc/RN3H-NZ8B].

[170] *See* Stephanie Nebehay, *U.N. Tells Iran to End Eutelsat Satellite Jamming*, REUTERS, https://www.reuters.com/article/us-iran-jamming-itu/u-n-tells-iran-to-end-eutelsat-satellite-jamming-idUSTRE62P21G20100326 [https://perma.cc/T6LN-NYHX] (Mar. 26, 2010, 6:23 AM); *see also* SMALL MEDIA, SATELLITE JAMMING IN IRAN: A WAR OVER AIRWAYS (2012), https://smallmedia.org.uk/media/projects/files/satjam.pdf [https://perma.cc/4EJ6-N7U2].

[171] *Tehran Jamming Foreign Broadcasts*, RADIO FREE EUROPE: RADIO LIBERTY (Oct. 4, 2012, 8:42 AM), https://www.rferl.org/a/tehran-jamming-foreign-broadcasts/24728694.html [https://perma.cc/EVL9-G8FJ].

[172] Sonne & Fassihi, *supra* note 16.

[173] *Id.* The ITU spokesperson stated that "[i]n this case there is evidence that there is a deliberate attempt to block the satellite transmissions" and that Iran should "'eliminate it as a matter of highest priority.'" *See* Nebehay, *supra* note 170.

[174] *See* Ney Remarks, *supra* note 87.

[175] The Director of Public Affairs at the Broadcasting Board of Governors stated in response to the Iranian jamming that "[w]hen you consider the time spent on finding other options, contacting audiences and affiliates, the potential loss of audiences not just in Iran, but other markets that depend on those satellites for content from VOA and other BBG networks, the costs are considerable." SMALL MEDIA, *supra* note 170. Simply because economic consequences could be

Schmitt attempts to parse out these economic and diplomatic measures in his effects-based model through a seven-factor analysis.[176] He does this primarily through the "invasiveness" factor.[177] However, economic coercion is part and parcel with the same actions in both cyberspace and jamming.[178] The complication with Schmitt's approach is that the effects caused by cyberspace and those caused by economic sanctions seem arbitrary. By "extending its principles outside the regime of cyber weapons [Schmitt] introduces measures of coercion not traditionally included in the prohibition on force, such as economic, diplomatic, or ideological coercion."[179] It unnecessarily reignites a debate that economic coercion should be treated as a use of force, which has chiefly been settled by State practice.[180]

Additionally, the United States has held that Article 41-type actions by the Security Council or the United States are not a use of force.[181] Thus, despite potentially severe effects and economic impact, neither economic sanctions nor interference by cyber means are considered a use of force.[182]

E. Security Council's Implementation of Article 41

The U.N. Security Council has implemented Article 41 several times for partial or complete interruptions for postal, telegraphic, radio, or other means of communications. The imple-

---

severe, the Article 2(4) prohibition on the use of force does not cover economic coercion. *See Summary Report of Eleventh Meeting*, *supra* note 78, at 334–35; *Proposal Presented by the Brazilian Delegation*, *supra* note 78; *see also* Gervais, *supra* note 80, at 536–37.

[176] Schmitt, *supra* note 103, at 914–15, 915 n.81.

[177] *Id.* at 914 ("In armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target state . . . .").

[178] *See* Beard, *supra* note 20, at 117–118 ("[E]fforts by a few states to explicitly include one important type of destructive, nonphysical conduct in the Article 2(4) prohibition against force—acts of economic coercion—were rejected.").

[179] Gervais, *supra* note 80, at 540.

[180] This becomes particularly perplexing since a substantial portion of cyber operations are not militaristic in nature, but "take the form of espionage, crime, or political or economic coercion." *See* Patterson, *supra* note 63, at 975.

[181] The President's Auth. to Take Certain Actions Relating to Commc'ns from Iran, 4A Op. O.L.C. 153, 153–54.

[182] *See* Roscini, *supra* note 2, at 49 ("[E]conomic sanctions that cause starvation among the population are not a use of armed force in spite of their severe humanitarian consequences: sanctions may be enforced with the use of weapons, but are not weapons themselves, as implied in Article 41 of the UN Charter.").

mentation of Article 41 by the U.N. Security Council indicates that measures under it do not rise to the level of a use of force. Article 41 has become a common tool for peace maintenance, and the Security Council has imposed it more than twenty times since the Iraqi invasion of Kuwait in 1990.[183] Specifically, the Security Council uses Article 41 when it wants to signal it is *not* using force.[184] The Security Council has even become creative and utilized Article 41 to establish other non-forceful measures, such as establishing international criminal tribunals.[185]

In 1966, the Security Council implemented Article 41 for the first time in Southern Rhodesia, which was also the first time there were recommendations for communication interruptions.[186] At first, the Security Council proposed implementing all sanctions under Article 41 to ensure practical application of the Security Council decision.[187] However, the full range of mea-

---

[183] *See* 2 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 1308 (Bruno Simma et al. eds., 3d ed. 2012).

[184] *See id.* at 1311 ("The range of measures available under Art. 41 is very broad, *but it explicitly excludes action involving the use of force. The SC has thus used references to Art. 41 to stress that it did not intend to authorize forcible action. 'Use of force' in this context should be interpreted widely to include, for example, naval demonstrations and blockades.*") (emphasis added).

[185] Prosecutor v. Tadić, Case No. IT-94-1-T, Decision on the Defence Motion on Jurisdiction, ¶¶ 26–29 (Int'l Crim. Trib. for the Former Yugoslavia Aug. 10, 1995).

[186] U.N. Sec. Council, *Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*, *in* REPERTOIRE OF SECURITY COUNCIL PRACTICE, ARTICLE 41 MEASURES – MEASURES NOT INVOLVING THE USE OF ARMED FORCE, 1966-1968, at 208, https://www.un.org/securitycouncil/content/repertoire/actions#rel3 (choose "1966–1968") [https://perma.cc/5C2J-K45Q] [hereinafter 1966–1968 SECURITY COUNCIL PRACTICE].

[187] At the 1259th meeting of the Securtiy Council, on November 13, 1965, the representative of the United Kingdom introduced a draft resolution which called upon all Members of the United Nations to endorse and support the economic sanctions which the United Kingdom was about to apply on the "illegal and unconstitutional regime in Southern Rhodesia" following its declaration of independence from the United Kingdom—including an embargo on supplies of oil and petroleum products, and of rail, sea, air, postal telegraphic, radio and other means of communication and severance of diplomatic and consular relations—in accordance with Article 41 of the Charter. U.N. Sec. Council, *Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*, *in* REPERTOIRE OF SECURITY COUNCIL PRACTICE, ARTICLE 41 MEASURES – MEASURES NOT INVOLVING THE USE OF ARMED FORCE, 1964–1965, at 191, https://www.un.org/securitycouncil/content/repertoire/actions#rel3 (choose "1964–1965") [https://perma.cc/X8P3-Y5CM] [hereinafter 1964–1965 SECURITY COUNCIL PRACTICE]; S.C. Res. 253 (May 29, 1968). By March 19, 1968, initial discussions indicated that the sanctions must be total, and all Members of the United Nations "must be asked to implement all the measures provided for in Article 41, including the

sures was not initially implemented, leaving communication uninterrupted.[188] By 1970, the Security Council passed further Article 41 measures but did not call explicitly for the complete interruption of communications.[189] Nonetheless, the Australian Postmaster General shut down all postal and telecommunication services for the Rhodesian Information Centre under the auspices of Article 41 measures.[190]

---

interruption of rail, sea, air, postal, telegraphic, radio and other means of communications, including also information media such as the press, films and television programmes." 1966–1968 SECURITY COUNCIL PRACTICE, *supra* note 186, at 208.

[188] At the 1533rd meeting of the Securtiy Council, on March 13, 1970, the representative of the United States called for a "speedy and unanimous decision to deny recognition to" Southern Rhodesia, but he explained that

> His delegation was . . . opposed to imposing a communication ban, not only because of the traditional attachment of the United States to freedom of movement and speech, but also because it believed that cutting off communication and free flow of information would not contribute to a solution of the problem, but rather tend to harden further the attitude of the white minority [in Southern Rhodesia].

U.N. Sec. Council, *Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*, *in* REPERTOIRE OF SECURITY COUNCIL PRACTICE, ARTICLE 41 MEASURES – MEASURES NOT INVOLVING THE USE OF ARMED FORCE, 1969–1971, at 202, https://www.un.org/securitycouncil/content/repertoire/actions#rel3 (choose "1969–1971") [https://perma.cc/URB9-S8UJ] [hereinafter 1969–1971 SECURITY COUNCIL PRACTICE]. The draft resolution that included the interruption of communication failed. *Id.* The Security Council was likely implementing Article 42 by permitting an oil embargo to and from Southern Rhodesia, but it was not explicit in doing so. *See* S.C. Res. 221 (Apr. 9, 1966). The United Kingdom was expressly authorized to arrest and detain tankers exporting oil and could use military force, so it is assumed that this is a use of armed force; thus, the Security Council was authorizing actions under Article 42 with regard to the oil embargo. *See id.* ¶ 5; *see also* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 12, at 624–25.

[189] S.C. Res. 277 (Mar. 18, 1970). Resolution 277 of the U.N. Security Council called on all member states to take further measures under Article 41, including the interruption of transportation to and from Southern Rhodesia, and requested all member states take all possible further action under Article 41 in order "to deal with the situation in Southern Rhodesia." *Id.* ¶¶ 8–9, 11. Resolution 277 (and the previous resolution regarding Southern Rhodesia, Security Council resolution 253) did not explicitly mention the interruption of communication, but the Security Council's measures implemented under Article 41 against Southern Rhodesia included the interruption of telephone communications of the Rhodesian Information Centre, causing Australian domestic courts to debate whether Security Council decisions could take effect in Australia without further legislation. *See* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 12, at 626, ¶ 14.

[190] 52 INTERNATIONAL LAW REPORTS 1–2 (Elihu Lauterpacht ed., 1979). "In April 1973, the Australian Postmaster General directed that all postal and tele-

If these interruptions of communications between Australia and South Rhodesia were permissible under Article 41 as measures that did not rise to the level of a use of force, similar communication interruptions could be unilaterally used by a State without rising to the level of a use of force. A State could cut off all e-mail, cut off all other forms of telecommunications, and shut down internet service between two countries, and none of these would be considered a use of force.[191]

Since the Cold War ended, the Security Council's implementation of Article 41 has become more common.[192] In 2004, the Security Council demanded Côte d'Ivoire authorities "stop all radio and television broadcasting inciting hatred, intolerance and violence."[193] In 2011, Resolution 1967 dealt with a situation in Côte d'Ivoire in which the local media, Radiodiffusion Télévision Ivoirienne (RTI), continued to incite violence.[194] The resolution called for the partial interruption of all media communication to propagate false information and incite hatred, specifically naming RTI.[195] Such Security Council Article 41 actions indicate communication interruptions are not a use of force.[196]

---

communication services for the Rhodesian Information Centre be withdrawn forthwith. This direction was made with a view to implementing Resolutions of the Security Council of the United Nations and in particular the Resolution of 18 March 1970." *Id.* Specifically, the Postmaster General's Department disconnected their telephone, changed the post office box lock, and stopped mail and telegrams. *Id.*

[191] In contrast, the South Rhodesian situation demonstrates that Article 42 measures involve the use of force. *See* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 12, at 624–25. The Article 42 measures involving the use of force cover more traditional physical acts, such as direct invasion or naval blockade. *See* U.N. Charter art. 42.

[192] CONFORTI & FOCARELLI, *supra* note 98, at 237 ("Sanctions [under Article 41] have been adopted and renewed many times . . . [since the end of the Cold War,] against Iraq since 1990, the former Yugoslavia since 1991, Somalia since 1992, Liberia since 1992, Haiti since 1993, Angola since 1993, Rwanda since 1994, Sudan since 1996, Sierra Leone since 1997, Afghanistan [and non-State actor Al Qaeda] since 1999, Ethiopia and Eritrea since 2000, the Democratic Republic of Congo since 2003, the Ivory Coast since 2004, Lebanon since 2006, [North] Korea since 2006 and Iran since 2006 . . . .").

[193] S.C. Res. 1572, ¶ 6 (Nov. 15, 2004).

[194] *See* S.C. Res. 1967, ¶ 10 (Jan. 19, 2011).

[195] This was only a partial interruption of communications because the resolution permitted other media without prejudice. *Id.*

[196] The Security Council also clarified its decision not to interrupt communication in certain resolutions. In 1993, during the turmoil in the former Yugoslavia, the Security Council passed a resolution imposing sanctions on financial and non-financial institutions with an exception for telecommunications and postal

When the Security Council and States speak or implement communication interruptions, they generally do not cite the terminology of using force or armed attack. Thus, actions under Article 41 of the U.N. Charter are measures that do not rise to the level of a use of force, and all interference along the electromagnetic spectrum—including interference by cyber means—is likely not a use of force either.

IV. ELECTROMAGNETIC INTERFERENCE: WIDESPREAD AND SYSTEMATIC STATE PRACTICE DURING NON-HOSTILITIES

A. Customary International Law

Article 41 of the U.N. Charter demonstrates that under a *jus ad bellum* analysis, it is improbable that cyber interference will rise to the level of a use of force. Besides treaty analysis, customary international law is the other primary method of analysis.[197] Generally, State practice has not treated any stand-alone cyber operations by States as armed attacks or a use of force, which demonstrated that customary international law cuts against the effects-based approach in cyberspace.[198]

---

services. *See* S.C. Res. 820, ¶¶ 21, 27 (Apr. 17, 1993). The decision to not interrupt telecommunications was later changed during the NATO campaign in the former Yugoslavia when actual airstrikes (as opposed to jamming) targeted TV broadcast transmitters. *See* Int'l Crim. Trib. for the Former Yugoslavia, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, ¶¶ 71–73 (June 8, 2000), https://www.icty.org/x/file/Press/nato061300.pdf [https://perma.cc/HY69-VVL9]. The justification given was that "[s]trikes against TV transmitters and broadcast facilities [were] part of [NATO's] campaign to dismantle the FRY propaganda machinery which [was] a vital part of President Milosevic's control mechanism." *Id.* ¶ 74; *see also* Press Release, Int'l Crim. Trib. for the Former Yugoslavia, Prosecutor's Report on the NATO Bombing Campaign, U.N. Press Release PR/P.I.S./510-e (June 13, 2000), https://www.icty.org/en/press/prosecutors-report-nato-bombing-campaign [https://perma.cc/959Q-8M98] (involving an example of an interruption of communications during wartime which was analyzed under a different legal standard than the *jus ad bellum* analysis).

197 The International Court of Justice adopted this framework for interpreting international law in Article 38(1) of the ICJ Statute, recognizing international conventions, custom, and the general principles of law of recognized civilized nations as the building blocks for international law interpretation. *See* ICJ Statute, *supra* note 53, art. 38, ¶ 1. As stated previously, existing *jus ad bellum* rules involving use of force, like treaties and customary international law, extend to cyber. *See* Roscini, *supra* note 2, at 25.

198 *See* Beard, *supra* note 20, at 78–79 ("[T]he continuing failure of states to treat damaging cyber acts standing alone as armed attacks is highly significant

Historic State practice is the best way to determine customary international law.[199] According to the ICJ, State practice must be "extensive and virtually uniform" to be considered customary international law, which is a historical analysis.[200] However, the effects-based model makes arguments based on potential *prospective* State behavior.[201] Much of the effects-based analysis is speculative, finding that "the *consequences* suffered [is what] matter[s] to states" and thus rejects not only the U.N. Charter's framework but also the traditional, historical analytical framework.[202]

The ordinary meaning of the U.N. Charter's text can only be rejected when it is clearly contrary to customary international law because of the U.N. Charter's long-standing history of defining *jus ad bellum*.[203] Thus, the effects-based approach to interference by cyber means would have to be found in a primary

---

since the establishment of customary international law is dependent on the finding of such state practice . . . .").

[199] *See* ICJ Statute, *supra* note 53, art. 38, ¶ 1(b) (defining customary law as "general practice accepted as law"); *see also* 1 OPPENHEIM'S INTERNATIONAL LAW, *supra* note 55, at 25–26 ("However, the formulation in the Statute serves to emphasise that the substance of this source of international law is to be found in the practice of states."). Customary international law is different from *usage* because of the binding nature of custom versus the mere habit found in usage. *Id.* at 27.

[200] North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.), Judgment, 1969 I.C.J. 3, ¶ 74 (Feb. 20).

[201] The effects-based analysis uses seven criteria of what can be classified as a use of force in cyberspace. *See* Schmitt, *supra* note 4, 576–77. According to Schmitt,

> The criteria are admittedly imprecise, thereby permitting states significant latitude in characterizing a cyber operation as a use of force, or not. . . . [A] tendency towards resolving grey areas in favor of finding a use of force *can be expected to emerge*. This State practice *will over time* clarify the norm and its attendant threshold.

Id. at 578 (emphasis added).

[202] *Id.* at 573. The International Court of Justice identified the two components that are required to establish customary international law in the *North Sea Continental Shelf* case in the absence of a treaty obligation. *See North Sea Continental Shelf*, 1969 I.C.J. at 43–44, ¶ 76–77. First, there must be acts by the states concerned that "amount to a settled practice." *Id.* at 44, ¶ 77. Second, such settled practice must also be "evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it." *Id.* Regarding the law of armed conflict, the United States has endorsed the view that states are bound to follow all treaties they are party to and all applicable customary international law. *See* U.S. DEP'T OF THE NAVY, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS § 5.1.2.1 (2007).

[203] *See, e.g.*, U.N. charter arts. 2, ¶ 4, 41, 42, 51; *see also* ICJ Statute, *supra* note 53, art. 38, ¶ 1.

obligation that would potentially constitute a rule of law.[204] Additionally, the ordinary meaning of Article 41 of the U.N. Charter for communication interruptions could only be rejected if there is extensive and virtually uniform behavior to demonstrate that electromagnetic interference is a use of force.[205] Yet, there is a lack of evidence in customary international law of reframing *jus ad bellum* to cyberspace based on an effects-based approach.[206]

B. Widespread Systematic State Practice

There appear to be widespread and systematic instances of jamming in the international context. In recent years, there have been dozens of known instances of satellite transmission interference during non-declared hostilities.[207] These instances include "Cuban disruption of Iranian broadcasts in 2009; . . . Iranian disruption of Eutelsat transmissions since 2009, the subject of formal protest to the ITU; Brazilian hackers' disruption of US Navy FLTSAT-8 in 2010; Jordanian jamming of Al-Jazeera transmissions in 2011; and China's blocking of BBC transmission in 2012."[208]

However, there are limitations to reviewing all State practices of electromagnetic interference when analyzing *jus ad bellum*. Verification of jamming can be difficult to attribute to one State because of the operations' covert nature and technical complications.[209] Even if States suspect one another, there may be geopolitical reasons for not admitting one's military equipment or civilian targets are susceptible to jamming or other forms of electromagnetic interference. This is not that different from cyberspace, where attribution can be nearly impossible at times.[210] The examples of customary international law that follow are based on available public information. Even with a limited vantage point, trends emerge on how States approach jamming and other forms of interference during non-declared hostilities.

---

[204] *See North Sea Continental Shelf*, 1969 I.C.J. at 41–42, ¶ 72.

[205] *See id.* ¶ 74.

[206] *See* Hollis, *supra* note 6, at 1029 ("Unlike the expansion of criminal law to include cybercrimes, however, the law of war has gone unchanged [in cyber].").

[207] *See* Housen-Couriel, *supra* note 41, at 440.

[208] *Id.*

[209] *See generally* Electronic Warfare Fundamentals, *supra* note 37, at 5-15, 6-23, 9-6.

[210] *See* Beard, *supra* note 20, at 77–79, 80–81.

One of the most well-known jammed satellite constellations is Eutelsat.[211] Recently, the number of deliberate jamming events has dramatically increased, going from fifty-four Eutelsat cases in 2010 to 109 in 2011 and spiking to at least 340 in 2012.[212] The number of minutes of jamming is on the rise as well: In fact, "[i]n June 2011, [Eutelsat] had 148 minutes of jamming. In March 2012, it was 4,714 minutes. In May 2013, it had increased to 46,000 minutes, and in August 2013 it reached 53,000 minutes."[213]

These amounts are substantial for a company that is one of the world's largest satellite operators and ranked third in global revenues for all customized communications.[214] The size and profitability of Eutelsat operations along with their close connection to the European Union, have not prevented the company from being jammed.

Iran is the likely culprit of many of these interference incidents (i.e., jamming), and some incidents have resulted in a formal ITU protest.[215] Yet, these interferences have not led to a referral to the Security Council or a declaration by government officials that Iran is engaged in an armed attack. Instead, the interferences have been treated as a lower level of international wrong through "naming and shaming."[216]

---

[211] Eutelsat began as a hybrid consortium of European Union governments and the private sector in 1982. *See* HANDBOOK OF SPACE LAW 109 (Frans von der Dunk & Fabio Tronchetti eds. 2015).

[212] Sargent, *supra* note 169.

[213] Peter B. de Selding, *U.S. Halt to Jamming of Cuban Broadcasts Could Aid International Efforts to Combat Interference*, SPACENEWS (Oct. 9, 2014), https://spacenews.com/42133us-halt-to-jamming-of-cuban-broadcasts-could-aid-international/ [https://perma.cc/E22B-DBDD].

[214] World Teleport Ass'n, *Global 20 of 2020: Top Teleport Operators*, https://www.worldteleport.org/page/TopOps_2020_Global [https://perma.cc/86NP-FG32]; *see also* HANDBOOK OF SPACE LAW, *supra* note 211, at 301. Eutelsat became much more of a private company by 2005, offering 30 percent of its shares in an Initial Public Offering, is one of the world's largest satellite operators, and has expanded to multi-media and the Internet. *Id.*

[215] Sonne & Fassihi, *supra* note 16 ("Eutelsat says it has filed numerous complaints with a U.N. agency that manages outer-space frequencies, the International Telecommunication Union, an arm of which stated in March that the interference 'appeared to be emanating from Iran.'").

[216] The ITU spokesperson took the unusual step of publically condemning Iran stating that "[i]n this case there is evidence that there is a deliberate attempt to block the satellite transmissions" and that Iran should "eliminate [the source of interference] as a matter of highest priority." Nebehay, *supra* note 170. However, there is no indication based on public information that much else happened to Iran.

Other numbers of stand-alone jamming events during peacetime indicate that the practice is widespread and systematic. A February to November 2016 study found 9,833 instances of GPS[217] interference affecting 1,311 commercial vessels, with the disruptions coming from "ten or more locations in Russia and Russian-controlled areas."[218] At least 400 instances involved false coordinates or denial-of-service outside of conflict zones in places like St. Petersburg, Moscow, and Vladivostok.[219] The scale of jamming demonstrates that other countries besides Iran are involved in widespread, systematic, GPS interference efforts during non-declared hostilities.

North Korea is also involved in widespread jamming. According to the Federal Aviation Administration (FAA), North Korea is involved in widespread intentional interference with GPS and navigation communication networks, including the jamming of U.S. aircraft and maritime vessels.[220] In March and April 2016, North Korea broadcasted a jamming signal on at least 100 occasions, affecting 962 planes, nearly 700 fishing vessels, and many cellphone base stations.[221] Between 2010 and April 2016, North Korea had engaged in at least four rounds of GPS jamming.[222]

---

[217] Global Navigation Satellite System (GNSS) is the broader category of geospatial timing services that includes the American NAVSTAR GPS system, the Russian GLONASS system, the European Galileo GNSS system, and the Chinese Beidou (Compass) system. *See* HANDBOOK OF SPACE LAW, *supra* note 211, at 556. For ease of understanding, "GNSS" jamming or interference will be referred to as "GPS" through the remainder of this article.

[218] C4ADS, ABOVE US ONLY STARS: EXPOSING GPS SPOOFING IN RUSSIA AND SYRIA 15 (2019), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf [https://perma.cc/J9VG-DGPZ] ("Using Automatic Identification System (AIS) ship location data collected at scale, C4ADS identified [the] . . . instances" of interference that appear to have originated from Russia.). Some of these events may be related to conflict zones near Ukraine and Syria. *Id.* at 13; *see also* SECURE WORLD FOUND., GLOBAL COUNTERSPACE CAPABILITIES: AN OPEN SOURCE ASSESSMENT 2-19 (Brian Weeden & Victoria Samson eds., 2020), https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf [https://perma.cc/4PXD-H45U].

[219] C4ADS, *supra* note 218, at 15.

[220] Amendment of the Prohibition Against Certain Flights in the Pyongyang Flight Information Region (FIR) (ZKKP), 83 Fed. Reg. 47,059, 47,061 (Sept. 18, 2018) (to be codified at 14 C.F.R. pt. 91).

[221] Kyle Mizokami, *North Korea Is Jamming GPS Signals*, POPULAR MECHS. (Apr. 5, 2016), https://www.popularmechanics.com/military/weapons/a20289/north-korea-jamming-gps-signals/ [https://perma.cc/AF5U-NFNR].

[222] *Id.*

A large number of recent interference events demonstrate that multiple countries engage in interruptions of communications systems. These events are just a snapshot during a short period. Since States do not always admit when they are jammed, jamming is likely more widespread and attribution is problematic.[223] Recent State practice indicates jamming does not rise to a use of force because the events were neither referred to the Security Council nor resulted in known Article 51 self-defense measures.

C. Broadcast Jamming: Everyone's Doing It

Besides the number of recent incidents, there is a long history of jamming. Some commentators argue that this electromagnetic interference is a new form of warfare and can be classified as a use of force.[224] However, jamming during non-declared hostilities has occurred for nearly ninety years.[225] The systematic and widespread use of jamming historically demonstrates that communication interruption over the electromagnetic spectrum likely does not amount to a use of force.

Jamming during peacetime occurred as early as the 1930s, with Austria jamming Nazi broadcasts, Germany and Russia jamming each other, and Italy jamming Soviet broadcasts.[226] The ICJ stated in the *North Sea Continental Shelf* cases that whether a custom has developed depends on if widespread and representative practice occurs, including by States that are specifically affected.[227] States have historically not treated stand-alone

---

[223] *See* Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. Conflict & Sec. L. 229, 231, 233 (2012); *see also* David Wright, Laura Grego & Lisbeth Gronlund, The Physics of Space Security: A Reference Manual 121–22 (2005) (explaining that it is difficult to locate an uplink jammer because they can operate from a large area); *see also* Mountin, *supra* note 35, at 121 ("Locating sources of interference and distinguishing a bona fide jamming attack from other forms of communication degradations or disruptions caused by systemic disturbances or natural phenomena like solar flares and astronomical storms is also difficult.").

[224] Li, *supra* note 4, at 187–88 ("Rather than permitting law to become 'ossified at the level of technology that existed at the end of World War II[,]' [the effects-based analysis] adopts an evolving definition that permits non-physical force—such as electronic jamming, directed-energy weapons, and cyber-attacks—to fall under the umbrella of military force.").

[225] *See* Berg, *supra* note 13, at 44.

[226] *See id.*

[227] North Sea Continental Shelf (Ger. v. Den; Ger. v. Neth.), Judgment, 1969 I.C.J. 3, ¶ 73 (Feb. 20) ("[B]efore a conventional rule can be considered to have become a general rule of international law, it might be that, even without the

jamming as an act of war. This may be because "[*e*]*very* country in the world has engaged in this type of intentional military radio jamming and many, to varying degrees and with varying methods, have engaged in jamming of foreign broadcasts to protect themselves from foreign ideas thought to be counter to established societal goals."[228] Widespread military jamming, which has historically occurred and continues to occur during peacetime, refutes the notion that this activity occurs only during armed conflict.[229] If every country in the world has participated in jamming during peacetime, then the custom has likely developed that it is not a use of force.

The *North Sea Continental Shelf* cases also analyze the time element of custom, which is helpful in determining if a custom has developed in jamming under *jus ad bellum*. While short periods can develop new customary international law, an "indispensable requirement" is that the practice is "both extensive and virtually uniform."[230]

The Soviet Union's jamming activities, which occurred during the Cold War without open hostilities, illustrate the behavior of one of the major international players at a critical time. "Never, however, has the practice of jamming radio broadcast signals during peacetime been as blatantly exhibited as it was by the Soviet Union and its East European Satellites against Western democracies."[231] The Soviets began jamming Voice of America (VOA), British Broadcasting Corporation (BBC), and Radio Free Europe in 1948 and continued until at least 1988.[232] There

---

passage of any considerable period of time, a very widespread and representative participation in the convention might suffice of itself, provided it included that of States whose interests were specifically affected.").

[228] COLD WAR BROADCASTING: IMPACT ON THE SOVIET UNION AND EASTERN EUROPE 52–53 (A. Ross Johnson and R. Eugene Parta eds., 2010) (emphasis added).

[229] *See id.*

[230] *North Sea Continental Shelf*, 1969 I.C.J. at 43, ¶ 74 ("Although the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law on the basis of what was originally a purely conventional rule, an indispensable requirement would be that within the period in question, short though it might be, State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform in the sense of the provision invoked.").

[231] COLD WAR BROADCASTING: IMPACT ON THE SOVIET UNION AND EASTERN EUROPE, *supra* note 228, at 53.

[232] *See* BERG, *supra* note 13, at 45–46. There would be periods in which the jamming would stop or diminish at times. *Id.* For example, jamming stopped briefly during 1963 and 1964 following the atomic test ban agreement. *Id.*

was no public acknowledgment that Soviet jamming was a use of force during these forty years.

The widespread and virtually uniform acceptance of jamming during peacetime is not limited to the former Soviet Union. China engaged in widespread jamming of VOA from 1956 to 1978.[233] The jamming resumed in 2001 and included BBC and several Tibet transmissions.[234] Chinese jamming of BBC broadcasts occurred as recently as 2013.[235] In 2011, Ethiopian journalists asked China to stop providing jamming equipment and technology to the regime for jamming Ethiopian Satellite Television inside Ethiopia; China's motivation was likely to interfere with anti-Chinese programming.[236] Such a request demonstrates that China does not view broadcast jamming as a use of force because it has engaged in this behavior outside of an armed conflict.

The United States and Cuba have also engaged in a series of broadcast jamming events against each other.[237] Cuba initially engaged in some jamming around the Cuban missile crisis, but the brunt of its jamming began in 1985 up through the mid-2010s.[238] The United States condemned the Cuban and Soviet jamming of U.S. radio and television broadcasts as human rights violations.[239] However, the United States never claimed the jamming efforts amounted to a use of force or an armed attack.[240] This may be partly because the United States engaged in jam-

---

[233] *See id.* at 46.

[234] *See id.* at 46–47.

[235] *Radio Jamming—Not A Thing of The Past*, ECONOMIST (Feb. 26, 2013, 7:08 AM), https://www.businessinsider.com/radio-jamming—not-a-thing-of-the-past-2013-2 [https://perma.cc/XKC8-6WRP] ("Amid all the fevered talk and high-tech details surrounding the 'cyber cold war' that China seems to be waging—and perhaps winning—against America and many other nations, there is something refreshingly nostalgic about new accusations that China is, in the high style of the actual cold war, jamming the BBC's shortwave radio broadcasts.").

[236] *EFJA Urges China To Stop Complicity in Jamming Ethiopian Satellite TV Transmissions*, ETHIOPIAN FREE PRESS JOURNALISTS ASS'N (June 22, 2011), https://ifex.org/efja-urges-china-to-stop-complicity-in-jamming-ethiopian-satellite-tv-transmissions/ [https://perma.cc/X37W-PNU2].

[237] de Selding, *supra* note 213.

[238] *See id.*; BERG, *supra* note 13, at 47.

[239] *See* Jamie Frederic Metzl, *Rwandan Genocide and the International Law of Radio Jamming*, 91 AM. J. INT'L L. 628, 628–29, 645–46 (1997).

[240] *See id.* at 628–29. The United States viewed interference with these transmissions as a breach of international law in violation of the right to free expression. *Id.* The Soviets' and the Cubans' view was that "state sovereignty precluded such undesirable foreign transmissions, and jamming was a legitimate and often-used countermeasure." *Id.* at 629.

ming of Cuban broadcasts for decades.[241] The U.S. jamming of Cuban broadcasts only became widespread knowledge when the United States announced it would stop the practice in 2014.[242]

Democracies other than the United States have also jammed broadcast signals. South Korea jammed North Korean television broadcasts from 1945 to 1999 under special security law.[243] In 2012, Iran claimed that the U.K. was jamming Iranian broadcasts on Eutelsat's Hotbird satellite network, possibly as retaliation for Iran jamming Eutelsat broadcasts in 2009.[244] Such examples indicate that peacetime broadcast jamming extends even to democracies.

The list of countries engaged in broadcast jamming in recent history is extensive. Egypt claims their jamming of Israeli cellphones was accidental and that the real target of its jamming efforts in 2018 was Sinai jihadis loyal to the Islamic State; yet, outages in Israel and the Gaza strip still occurred.[245] Additionally, the Qatar-based news agency, Al Jazeera, claimed the Egyptian military jammed its satellite broadcasts in 2013.[246] Finally, Vietnam, North Korea, Iran, Chile, and Zimbabwe have all engaged in jamming broadcasts during peacetime.[247] From a statistical standpoint, satellite jamming incidents rose from 5% in 2010 to 15% in 2013.[248]

However, nothing states that broadcast jamming is not an international wrong. The ITU has labeled "harmful interference"

---

[241] de Selding, *supra* note 213.

[242] *Id.*

[243] Charles Lee, *N. Korean Broadcasts Allowed in South*, UPI (Oct. 22, 1999), https://www.upi.com/Archives/1999/10/22/N-Korean-broadcasts-allowed-in-South/9258940564800/ [https://perma.cc/M686-TP67].

[244] Dave Klingler, *Satellite-Jamming Becoming a Big Problem in the Middle East and North Africa*, ARS TECHNICA (Mar. 28, 2012, 6:30 AM), https://arstechnica.com/science/2012/03/satellite-jamming-becoming-a-big-problem-in-the-middle-east/ [https://perma.cc/T35S-HTN6]; *cf.* Sonne & Fassihi, *supra* note 16.

[245] Dan Williams, *Egyptian Jamming of Sinai Insurgents Disrupts Phones in Israel, Gaza*, REUTERS, https://www.reuters.com/article/us-israel-egypt-telecoms/egyptian-jamming-of-sinai-insurgents-disrupts-phones-in-israel-gaza-idUSKCN1GJ1K3 [https://perma.cc/V4JK-W4UY] (Mar. 7, 2018, 5:56 AM).

[246] Joel Gulhane, *Al Jazeera Accuses Armed Forces of Jamming Satellite Signals*, DAILY NEWS EGYPT (Sept. 4, 2013), https://dailyfeed.dailynewsegypt.com/2013/09/04/al-jazeera-accuses-armed-forces-of-jamming-satellite-signals/ [https://perma.cc/48NC-AEXC].

[247] *See* BERG, *supra* note 13, at 47.

[248] Steve Lambakis, *Foreign Space Capabilities: Implications for U.S. National Security*, NAT'L INST. FOR PUB. POL'Y 17 (2017), https://nipp.org/wp-content/uploads/2021/03/Foreign-Space-Capabilities-pub-2017-1.pdf [https://perma.cc/F35L-4KJB].

a violation of ITU obligations under Article 45 of the ITU Constitution.[249] Thus, intentional jamming "violates the principle of international recognition under the ITU Radio Regulations."[250] However, being an international wrong and not living up to the ITU Convention do not make broadcast jamming a use of force.[251] Communication interruptions appear to be accepted and do not receive much condemnation other than public shaming.[252]

Turning to cyberspace, Russia has engaged in similar interference by cyber means like it has in other forms of electromagnetic interference. According to the U.K.'s National Cybersecurity Center, Russia shut down the French television station TV5Monde.[253] The Russian military intelligence hacking team (i.e., Fancy Bear) likely carried this out.[254] When Russia jammed the BBC and VOA, its behavior was condemned but not declared a use of force.[255]

There is also some evidence that the United States has not treated interference by cyber means as a use of force. In 2011 and 2012, there were two waves of DDoS cyber operations against some of the world's largest financial institutions, such as Bank of America and JPMorgan.[256] Media outlets and unnamed officials of President Obama's administration blamed Iran for the DDoS operations.[257] President Obama's administration se-

---

[249] Constitution and Convention of the International Telecommunication Union, art. 45, Dec. 22, 1992, 1825 U.N.T.S. 331 [hereinafter ITU Constitution].

[250] Mountin, *supra* note 35, at 134–35; *see* Radio Regulations of the Int'l Telecomm. Union art. 15 (2020 ed.), https://www.itu.int/en/myitu/Publications/ 2020/09/02/14/23/Radio-Regulations-2020 [https://perma.cc/8KD4-KM3G]. Part of the ITU's lack of ability to address interference during peacetime is because under Article 48 of the ITU Constitution, military radio installations are generally exempt with some caveats such as avoiding interference, to the extent possible, with distress messages. ITU Constitution, *supra* note 249, art. 48; *see* Housen-Couriel, *supra* note 41, at 451–52 (even during peacetime, military radio installations are generally exempt from the requirement to avoid harmful interference except with regard to distress messaging).

[251] *See* Metzl, *supra* note 239, at 639.

[252] *See id.* at 638.

[253] *See* CLARKE & KNAKE, *supra* note 5, at 25.

[254] *See id.* at 19.

[255] *See id.* at 25.

[256] *See id.* at 85.

[257] *See, e.g.*, Ellen Nakashima, *Iran Blamed for Cyberattacks on U.S. Banks and Companies*, WASH. POST (Sept. 21, 2012), https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html [https://perma.cc/LWH2-RGA3]; *see also* CLARKE & KNAKE, *supra* note 5, at 85.

lected a limited response and chose to treat the cyber operations "like any other mildly disruptive internet activity."[258] The response included the Department of Homeland Security (DHS) notifying the owners of infected accounts to delete the malware and slow the DDoS cyber operations.[259] The decision to have DHS notify affected users and the fact that DoD did not respond with a kinetic attack is indicative that the United States did not view the actions as a use of force.

D. Interference by Cyber Means Causing Interoperability and Functionality Issues

The more contested issue to resolve is not if broadcast jamming rises to a level of a use of force, but if interoperability issues through interference rise to the level of a use of force. The effects-based rationale would likely come to a similar conclusion about broadcast jamming and cyber interference, albeit for different reasons. For example, disruptions to National Football League television coverage resulting in financial losses would likely never rise to the level of a use of force under an effects-based analysis.[260] Instead, the determining factor for the effects-based analysis would be the severity of consequences.[261]

Schmitt's first and most significant factor in his seven-factor effects-based analysis is "severity."[262] Under this factor, physical harm to individuals or property would amount to a use of force, whereas minor inconveniences would not.[263] A related concept under the *Tallinn Manual* is if interference by cyber means constitutes an attack.[264] There is not a consensus by *Tallinn Manual* members, but a majority would find that the loss of functionality qualifies as an armed attack if physical replacement of parts is required for restoration.[265]

---

[258] *See id.* at 86.

[259] *See id.*

[260] *See* Mountin, *supra* note 35, at 178.

[261] *See* Schmitt, *supra* note 4, at 576; *see also* Mountin, *supra* note 35, at 178 (implying severity of consequence matters most in analyzing the *jus ad bellum* for electronic jamming of satellites).

[262] Tallinn Manual 2.0, *supra* note 4, at 334.

[263] *See id.*; *see also* Mountin, *supra* note 35, at 178.

[264] *See* Tallinn Manual 2.0, *supra* note 4, at 417. Under Rule 92, a potential "attack" through cyber interference is analyzed as more of a *jus in bello* analysis than a *jus ad bellum* analysis; whether a cyber operation is an "attack" is based solely on death, injury, or damage to objects. *See id.* at 415.

[265] *See id.* at 417.

One of the most cited examples for this proposition is when a cyber operation is used to disable an air traffic control system, causing airplanes to crash.[266] Even scholars who primarily support an "instrument"-based approach, such as Duncan Hollis, question the traditional U.N. Charter framework for a use of force when an entire air traffic control system is shut down, causing significant casualties.[267] Additionally, the DoD Law of War Manual states that disabling civilian air traffic control services resulting in airplane crashes is a commonly cited example of cyber activity that could amount to a use of force.[268]

However, custom around jamming calls into question this premise of functionality loss as a use of force. As discussed above, in the spring of 2016, North Korea jammed GPS signals on at least 100 occasions, affecting the functionality of 962 planes.[269] However, this was not the first time that North Korea jammed airplane communication or navigation. As early as 1977, North Korea jammed planes' communications signals.[270] In 2012, North Korea jammed 1,016 airplanes and 254 ships—grounding flights and keeping ships in port.[271]

North Korea is not alone in jamming GPS signals. Moscow also frequently jams GPS signals. In fact, Moscow has jammed GPS signals beyond the previously mentioned 9,833 instances of

---

[266] *See, e.g.*, Schmitt, *supra* note 103, at 916; Silver, *supra* note 135, at 91 (arguing a cyber operation that disables air traffic control system and causes planes to crash is a use of force).

[267] *See* Hollis, *supra* note 6, at 1042 (raising questions in the context of air traffic control and plane crash scenario).

[268] DoD Law of War Manual, *supra* note 19, § 16.3.1 (citing *Koh Remarks*, *supra* note 24). According to DoD regulations, electronic warfare can have navigation warfare "effects by protecting or denying transmitted . . . (GNSS) or other radio navigation aid signals." JP for Electronic Warfare, *supra* note 36, § I-16. This is done by "degrading, disrupting, or deceptively manipulating [position, navigation, and timing] transmissions." *Id.*

[269] Mizokami, *supra* note 221; *see also North Korea 'Jamming GPS Signals' Near South Border*, BBC News (Apr. 1, 2016), https://www.bbc.com/news/world-asia-35940542 [https://perma.cc/L23H-5S2G].

[270] John Saar, *American 'Rat Racers' Train Hard to Defend South Korea*, Wash. Post (June 10, 1977), https://www.washingtonpost.com/archive/politics/1977/06/10/american-rat-racers-train-hard-to-defend-south-korea/ed8b56f6-a931-47ae-84fb-9e60b2325ed1/ [https://perma.cc/2ETS-8VRV] ("North Koreans sometimes attempt to jam communications among U.S. planes . . . .").

[271] Jonathan Saul, *Governments Confront Rising Threat to Ships from Signal Jamming*, Reuters, https://www.reuters.com/article/shipping-navigation-gps-idUSL5N0E926V20130530 [https://perma.cc/8TQD-4A7H] (May 30, 2013, 9:15 AM).

GPS interference.[272] Moscow has caused interference involving 1,311 commercial vessels that were coming from locations in Russia and Russian-controlled areas.[273] As early as 1982, Moscow engaged in jamming GPS signals, including those in Colorado and Hawaii used for navigation by airplanes and ships.[274] However, the United States did not publicly indicate the activity as a use of force. Rather than a DoD response, the Federal Communications Commission Chairman stated that if the action continued, the United States would make a complaint to the Soviet Union.[275] The United States would likely have been more aggressive if it viewed the interference as a use of force.

Recently, Norway has accused Russia of jamming critical GPS and other communication systems. During multiple NATO exercises since 2017, "blocking" signals coming from Russia have impacted military aircraft and vessels in and around Norway and Finland.[276] During a major NATO exercise from October through November 2018, the jamming intensified, threatening both military and civil aviation.[277] At first, the Russians denied the jamming took place.[278] However, Norway and Finland claimed they were able to demonstrate that Russia caused the jamming.[279] Lieutenant General Morten Haga Lunde, the head

---

[272] C4ADS, *supra* note 218, at 15 (using Automatic Identification System (AIS) ship location data collected at scale, C4ADS identified the 9,833 instances of interference that appear to have originated from Russia).

[273] *See id.* The raw number of times jamming occurs in less than a year is revealing of how commonplace Russian jamming is in international territories. *See id.* C4ADS is a non-profit security organization that partnered with the University of Texas at Austin for a study of GPS jamming in Russia. *See id.* at 2. A reasonable conclusion can be drawn that Russian jamming of navigational signals has occurred much more than 9,833 times because this was a study done for a short time period. *See id.* at 3 (the study was done for a year, ending in November 2018). However, even if jamming has only occurred 9,833 times, that in itself is a high mark for consistent State practice in the area of jamming—at least by Russia.

[274] Chandler, *supra* note 15.

[275] *Id.*

[276] Gerard O'Dwyer, *Norway Accuses Russia of Jamming Its Military Systems*, DEF. NEWS (Mar. 8, 2019), https://www.defensenews.com/global/europe/2019/03/08/norway-alleges-signals-jamming-of-its-military-systems-by-russia/ [https://perma.cc/MH3H-T7EZ].

[277] *See* Associated Press, *Norway Says GPS Jamming During the Biggest NATO War Game in Decades a Big Problem for the Military and Civilians*, BUS. INSIDER (Feb. 11, 2019, 8:35 AM), https://www.businessinsider.com/norway-gps-jamming-during-nato-drills-in-2018-a-big-concern-2019-2 [https://perma.cc/4XB4-JXKV].

[278] *See* O'Dwyer, *supra* note 276.

[279] *See* Nerijus Adomaitis, *Norway Says It Proved Russian GPS Interference During NATO Exercises*, REUTERS, https://www.reuters.com/article/us-norway-defence-

of Norwegian Intelligence Service, stated, "Jamming is also a threat to, among other things, to civilian air traffic, police and medical-related operations in peacetime."[280] The statement reveals Norway's view that it was peacetime, rather than hostile, action. There is no indication from Lieutenant General Morten Haga Lunde that Norway, a NATO member, viewed this jamming as a use of force.[281] Instead, the Norwegian response follows a common theme with GPS jamming of aircraft: a complaint might be filed against the offending party, but no Article 51 defensive measures or referrals to the U.N. Security Council are taken.[282]

The United States has also engaged in jamming of navigational aids outside of an armed conflict. In 1987, during three days of Iranian military exercises called Operation Martyrdom, the United States used radar-jamming aircraft to jam Iranian radars, causing systems to malfunction.[283] The United States jammed the Iranian training radars because the radars had homed-in on the U.S. naval ships as part of "pre-firing drills" for their missiles.[284] There was no declared conflict between the United States and Iran.

More recently, in 2018 and 2019, the U.S. Navy engaged in wide-scale GPS jamming along the southeastern coast of the United States.[285] The majority of this jamming was part of an exercise conducted by a Carrier Strike Group.[286] In one exercise, GPS jamming was projected to extend to the Florida Keys and included parts of the northwestern Bahamas.[287]

---

russia-idUSKCN1QZ1WN [https://perma.cc/S9M5-9G3Q] (Mar. 18, 2019, 10:58 AM).

[280] O'Dwyer, *supra* note 276 (emphasis added).

[281] *See id.*

[282] *See* Adomaitis, *supra* note 279.

[283] *Iran Radar Jammed by U.S. Planes—Anti-Ship*, SAN DIEGO UNION-TRIB., Aug. 7, 1987, at A-1.

[284] *Id.*

[285] SECURE WORLD FOUND., *supra* note 218, at 3-13.

[286] *Id.*

[287] Max Chesnes, *FAA: Navy Exercise Might Affect GPS Signals in Small Planes Flying Along Southeast*, TC PALM, https://www.tcpalm.com/story/news/local/indian-river-county/2020/01/17/gps-affected-navy-exercise-southeast-florida-small-planes-faa/4499470002/ [https://perma.cc/4CSQ-LD9J] (Jan. 21, 2020, 2:41 PM); Mark Collins & Zachery Lashway, *GPS Jamming May Shut Down Navigation*, WJXT NEWS4JAX, https://www.news4jax.com/weather/2020/01/17/gps-jamming-may-shut-down-navigation-in-southeast/ [https://perma.cc/K6SG-CDF4] (Jan. 20, 2020, 10:46 AM). The projected jamming of January 2020 Navy exercise may have also affected Cuban territorial waters by comparing the map published in the *U.S.A. Today* story and a map of the U.S. territorial sea. *See* Chesnes, *supra*;

Additionally, there have been multiple reports of Chinese jammers being placed on the islands in the South China Sea and jamming of GPS signals near the Port of Shanghai.[288] Chinese GPS jamming began in 2018, and by July 2019, over 300 ships were affected.[289] In other words, GPS jamming is on the rise and is not limited to one nation.

The effects-based supporter may question this widespread and systematic jamming of aircraft GPS and find that the consequences' severity still has not reached the appropriate level of harm. In 2002, Dan Silver, an effects-based supporter, explained how some scholars note the absence of state actions following airplane crashes caused by cyber interference indicates that there is a lack of customary international law.[290] According to Silver, this may be due to the recent development of cyber operations.[291] However, it has been eighteen years since Silver made this observation and wide-scale civilian airplane crashes through cyberspace have not occurred.[292] Cyberspace may never cause the degree of destruction on air traffic control systems as previously theorized.

The international flying community has accepted GPS jamming as the norm and has adjusted accordingly. For example, International Civil Aviation Organization (ICAO) identified sixty-five interference incidents between 2017–2018 in the Middle East Region.[293] In its *2016 Global Air Navigation Plan*, ICAO recommended that because of the vulnerability of GPS signals to interference, conventional radio navigation aids should be re-

---

cf. Nat'l Oceanic & Atmospheric Admin., *U.S. Maritime Limits & Boundaries*, https://nauticalcharts.noaa.gov/data/us-maritime-limits-and-boundaries.html [https://perma.cc/M662-FTNY] (map and coordinates of the U.S. territorial sea).

288 SECURE WORLD FOUND., *supra* note 218, at x, 1-16.

289 *Id.* "The effect of the spoofing was also unique: the position of the ships was jumping every few minutes in a ring pattern that showed as large circles over weeks." *Id.*

290 *See* Silver, *supra* note 135, at 78.

291 *Id.*

292 *See* Schmitt, *supra* note 103, at 887; *see also* Lee Rainie, Janna Anderson & Jennifer Connolly, *Cyber Attacks Likely to Increase*, PEW RSCH. CTR. (Oct. 29, 2014) https://www.pewresearch.org/internet/2014/10/29/cyber-attacks-likely-to-increase/ [https://perma.cc/RU2N-RGMG].

293 Int'l Civil Aviation Org. [ICAO], *MIDANPIRG Commc'n, Navigation & Surveillance Sub-Grp.: CNS Plan. & Implementation in the MID Region*, at 2, ICAO Doc. CNS SG/9-WP/12 (2019), https://www.icao.int/MID/Documents/2019/CNS%20SG9/CNS%20SG9-WP12-%20GNSS%20Issues.pdf [https://perma.cc/4TQ9-UNT5].

tained, and alternative navigation solutions should be created as a backup.[294] There is no doubt that continued reliance on conventional radio navigation aids or other navigation solutions is due to the interference of GPS.[295]

The vulnerability of GPS as targets is also not purely hypothetical. In July 2020, a ransomware attack took place on one of the pilots' underlying systems to store flight planning and FAA's aeronautical database to update GPS routes.[296] While the incident was far from trivial and several aircraft were grounded for days, it showed how flying has built-in redundancies to deal with cyber threats since many pilots relied on backup systems and could continue their planned routes.[297] The pilots who did not have updated GPS or backup systems did not take off because specific rules prevented them from flying without updated navigation routes.[298] Thus, an aircraft accident caused by interference through cyber means is unlikely due to the lack of advanced planning and recognition that cyber threats can target GPS.

One could argue that if there is a wide-scale interference by cyber means in which multiple planes crashed, that would be considered a use of force. Such an idea is a realpolitik argument that losing life and property would call for a forceful response.

---

[294] Int'l Civil Aviation Org. [ICAO], *2016–2030 Global Air Navigation Plan*, at 100, ICAO Doc. 9750-AN/963 (5th ed. 2016), https://www.icao.int/publications/Documents/9750_5ed_en.pdf [https://perma.cc/ACF3-63B2].

[295] *See id.* Unintentional interference does not even have to be broadcasting on the same frequency; it can be caused by solar effects. *See* Int'l Civil Aviation Org. [ICAO], *supra* note 293, at 23. "GNSS signals are delayed by varying amounts of time depending on the density of ionized particles (ionosphere) which itself depends on the intensity of solar radiation and other solar energy bursts. The solar activity can cause GNSS service to be degraded or temporarily lost." *Id.*

[296] Lily Hay Newman, *A Cyberattack on Garmin Disrupted More Than Workouts*, WIRED (July 27, 2020, 7:53 PM), https://www.wired.com/story/garmin-outage-ransomware-attack-workouts-aviation/ [https://perma.cc/B5XY-NJWJ] ("The fly-Garmin and Garmin Pilot apps both suffered days-long outages, hindering some Garmin hardware used in planes, including flight-planning mechanisms and the ability to update mandatory FAA aeronautical databases."). A ransomware attack is a form of malware attack where an outside user encrypts files and then demands ransom to restore access, usually in the form of Bitcoin. Josh Fruhlinger, *Ransomware Explained: How It Works and How to Remove It*, CSO (June 19, 2020, 3:00 AM), https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html [https://perma.cc/W8BA-N2CT].

[297] *See* Newman, *supra* note 296.

[298] *Id.*

Besides being unlikely, attribution is another problem with this hypothetical.[299]

However, even if interference by cyber means can be attributed to a State, the victim State could potentially use force in that hypothetical under preemptive self-defense.[300] This is because such an action carried out by the offending State could be interpreted as the preparatory stages of an upcoming armed attack. A State would likely engage in intentional cyber interference of GPS to cause multiple airplane crashes only in preparation for an armed attack. This scenario is like the jamming of reconnaissance satellites that monitor nuclear weapons sites. If several of these satellites are jammed, it would not be a

---

[299] *See* Beard, *supra* note 20, at 78–80; *see also* THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 141 (2017) (technical issues with attribution are difficult to overcome in cyber).

[300] The ICJ intentionally avoided addressing anticipatory self-defense in the *Nicaragua* case. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 347, ¶ 172 (June 27) (dissenting opinion by Schwebel, J.) ("[The ICJ] rightly observes that the issue of the lawfulness of a response to the imminent threat of armed attack has not been raised in this case, and that the Court accordingly expresses no view on that issue."). Anticipatory self-defense is permitted if the U.N. Security Council has not had the opportunity to act and immediacy, necessity, and proportionality call for forceful action in response to an anticipated armed attack. *See* Leo Van den hole, *Anticipatory Self-Defence Under International Law*, 19 AM. U. INT'L L. REV. 69, 79, 97–98 (2003). The concept of preemptive self-defense in international law is established from the Caroline Affair in 1837. *See* Howard Jones, *The Caroline Affair*, 38 HISTORIAN 485, 485 (1976). British forces entered the United States, seized the ship, *The Caroline* (which was being loaded with men and supplies to support a rebellion in Canada), set it on fire, and sent it over Niagara Falls. *See id.* at 485, 491. The U.S. representative, Daniel Webster, acknowledged the right to preemptive self-defense in a letter to his British counterpart, Henry S. Fox, stating "[i]t will be for [the U.K.] Government to show a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation." Letter from Daniel Webster to Henry S. Fox (Apr. 24, 1841), *in* DIPLOMATIC AND OFFICIAL PAPERS OF DANIEL WEBSTER, WHILE SECRETARY OF STATE 123, 132 (1848); *see also* BOWETT, *supra* note 133, at 188–92 (asserting that Article 51 does not preclude actions taken against an imminent danger); Beth M. Polebaum, *National Self-Defense in International Law: An Emerging Standard for a Nuclear Age*, 59 N.Y.U. L. REV. 187, 200–02 (1984) (asserting that because the U.N. Charter is silent on the issue of defensive use of anticipatory force, a presumption that preemptive attacks are permitted exists). This is a high standard for preemptive self-defense indicating that there would have to be a clear sign that a State's interference by cyber means on the GPS systems—causing planes to crash—is evidence of a pending instant and overwhelming attack.

use of force in and of itself but could indicate an impending armed attack.[301]

Additionally, nothing is preventing a State subject to interference by cyber means—such as GPS interference causing multiple airplane crashes—from going to the U.N. Security Council and receiving authorization to respond with Chapter VII actions.[302] The U.N. Security Council could authorize Chapter VII measures even if there was not a use of force.[303]

Finally, there is no serious attempt to label communication satellite jamming as a use of force, "all that has been done to make the jammers pay the consequences of their interference is 'naming and shaming.'"[304] Naming and shaming is a far cry from self-defense actions and calls into question whether any stand-alone interference activity could ever rise to the level of a use of force.[305] Naming and shaming is more in line with a low-

---

[301] The United States and the former Soviet Union signed an agreement in 1971 that requires immediate notification to the other party if either detects "signs of interference" with the missile warning systems for nuclear weapons. Laura Grego, *A History of Anti-Satellite Programs,* UNION OF CONCERNED SCIENTISTS 4 (2012), https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf [https://perma.cc/T48Z-J5SJ]. A key factor in determining if anticipatory self-defense is justified is the nature of the weapon. *See* Van den hole, *supra* note 300, at 101. If the threat assessment determines a nuclear strike is justified, then anticipatory self-defense is more likely justified. *See id.*

[302] *See* U.N. Charter art. 39 ("The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and 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."); DOD LAW OF WAR MANUAL, *supra* note 19, § 1.11.4 (rationales for the Resort of Force include self-defense and use of force authorized by the U.N. Security Council acting under Chapter VII of the Charter of the United Nations).

[303] *See* U.N. Charter art. 39. Under Article 39, Chapter VII actions allow the Security Council to take Article 41 or Article 42 action if there is a "threat to the peace, breach of the peace, or act of aggression" that is *not* an armed attack or a use of force. *Id.*; *see also* DINSTEIN, *supra* note 9, at 135 (acts of aggression may consist of measures short of war and are not crimes against peace).

[304] Lambakis, *supra* note 248, at 18.

[305] Besides customary international law on behavior, there is one custom-based international agreement that Russia and the United States do not view jamming and other forms of electromagnetic interference as a use of force. *See* Agreement on the Prevention of Dangerous Military Activities art. 6, June 12, 1989, 28 I.L.M. 879. In June 1989, the Soviet Union and the United States signed the agreement that addressed interference with command-and-control networks. *Id.* The agreement is indicative of the widespread jamming since there would be no need for an agreement of activity that was not occurring between the United States and Soviets. Also, the agreed response to an electromagnetic interference was for the offended party "[to] inform the relevant personnel of the armed forces of the other party." *Id.* This is a far cry from declaring these actions as hostile; the pro-

level international wrong than a use of force. The authorization to use force must be more than a mere abstraction based on prospective behavior.[306] Thus, the most commonly cited example of a stand-alone cyber operation being a use of force is a poor demonstration that interference by cyber means can be classified as a use of force.

E. Satellite Blinding

Moreover, the interoperability and functionality position of effects-based reasoning is questioned in light of other activities. During the Cold War, the Soviet Union and the United States also likely engaged in electromagnetic interference of satellites through "blinding," "illuminating," or "dazzling."[307] Interference by blinding or dazzling satellites was not publicly labeled as a use of force during the Cold War or more recent State practice.[308]

The DoD does not always use the term blinding or illuminating in reference to satellite interference, and sometimes prefers

---

cess of notification of an activity already occurring is more in line with confidence building measures for a future arms control agreement rather than a use of force in itself.

[306] William H. Taft IV & Todd F. Buchwald, *Preemption, Iraq, and International Law*, 97 Am. J. Int'l L. 557, 557 (2003) ("In the end, each use of force must find legitimacy in the facts and circumstances that the state believes have made it necessary. Each should be judged not on abstract concepts, but on the particular events that gave rise to it.").

[307] *See* Richard Sale, *Exclusive Graphic Soviet Lasers Said to Zap U.S. Spy Satellites*, United Press Int'l (Jan. 23, 1988), https://www.upi.com/Archives/1988/01/23/Exclusive-Graphic-Soviet-lasers-said-to-zap-US-spy-satellites/8407569912400/#:~:text=the%20suspected%20Soviet%20laser%20'hosings,system%2C%20the%20sources%20told%20UPI [https://perma.cc/JX7L-SJJQ]; Thomas O'Toole, *Space Wars*, Wash. Post (Nov. 6, 1977), https://www.washingtonpost.com/archive/opinions/1977/11/06/space-wars/cb2edd42-cbb4-42ba-8514-202080dccafe/ [https://perma.cc/34FL-XNS4].

[308] *See, e.g.*, Grego, *supra* note 301, at 10. Currently, the United States, Russia, and China all have lasers that can be used to disable or interfere with satellites. *See id.* at 10–11. The United States has acknowledged that testing occurred in the early 1990s. *See id.* at 7.

the term dazzling."[309] In addition, the United States does not consider certain lasers that jam or dazzle satellites as weapons.[310]

Related to blinding is the term "directed energy," which is the umbrella term for a type of operation that is used to "incapacitate, damage, disable, or destroy enemy equipment, facilities, [and] personnel" through electromagnetic energy and atomic or subatomic particles.[311] Blinding is used in some vocabulary

---

[309] The Army is further developing "laser dazzlers to blind surveillance satellites and jammers to disrupt communications and surveillance satellites." *Space and U.S. National Power: Hearing Before the Subcomm. on Strategic Forces of the H. Comm. on Armed Servs.*, 109th Cong. 10 (2006) [hereinafter O'Hanlon Statement] (statement of Michael O'Hanlon, Senior Fellow in Foreign Policy Studies at The Brookings Institute). "Just as a satellite's receiver can be swamped by a jamming signal, a satellite's optical sensor can be dazzled by swamping it with light that is brighter than what it is trying to image." WRIGHT, GREGO & GRONLUND, *supra* note 223, at 125. "Dazzlers are essentially lasers designed to blind electro-optical surveillance satellites much the way shining a flashlight at a camera would blind the camera as it takes the picture." Duncan Blake & Joseph S. Imburgia, *"Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons,"* 66 A.F. L. REV. 157, 177 n.120 (2010) (citing O'Hanlon Statement, *supra*. Using the term "dazzling" might be due in part to avoid confusing it with "blinding lasers" which are prohibited from being directed at human beings on the ground that it would cause permanent blindness, outlined in the following U.N. protocol. *See* Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to be Excessively Injurious or to Have Indiscriminate Effects: Blinding Laser Weapons (Protocol IV), art. 1, Oct. 13, 1995, S. Treaty Doc. 105-1C, 1380 U.N.T.S. 370 [hereinafter CCW Protocol IV]. The United States is a party to CCW Protocol IV. *Id.*

> [E]ye-safe lasers that exist today as nonlethal "laser dazzlers" do not meet the definition of a blinding laser weapon found in CCW Protocol IV; however, the United States and Australia required and conducted a legal review on each and every type of 'dazzling laser' prior to their acquisition and deployment by their militaries.

Blake & Imburgia, *supra*, at 201 n.256.

[310] DOD LAW OF WAR MANUAL, *supra* note 19, § 6.15.1.1 n.383 ("Choice of the term *weapon* was intentional to distinguish the prohibited system from lasers which are used for rangefinding, jamming, dazzling, communications, weapons guidance, and similar purposes.") (citing W. Hays Parks, Special Assistant to the Judge Advocate General of the Army for Law of War Matters, *Memorandum of Law:* Travaux Preparatoires *and Legal Analysis of Blinding Laser Weapons Protocol*, *reprinted in* THE ARMY LAWYER 33, 36 (June 1997)); *see also* ARMY SPACE OPERATIONS, *supra* note 41, para. 2-83 ("Lasers—may be used to temporarily dazzle or permanently blind mission-critical sensors on a satellite.").

[311] JP FOR ELECTRONIC WARFARE, *supra* note 36, at I-16. "Directed energy" operations also include all forms of lasers, including those that cause blinding, and anti-satellite lasers. *Id.* Directed energy weapons fall into a different anti-satellite capability than kinetic based anti-satellite capabilities. *See* Blake & Imburgia, *supra* note 309, at 177; *see also* U.S. GOV'T ACCOUNTABILITY OFF., GAO-12-479, ELECTRONIC WARFARE: DOD ACTIONS NEEDED TO STRENGTHEN MANAGEMENT AND OVER-

because it is easier to frame terminology based on a satellite's functionality.[312]

During the Cold War, the Soviets engaged in satellite interference through blinding on several occasions. In 1975, the Soviet Union emanated a beam to blind three U.S. satellites.[313] Specifically, "Capt. G.R. Villar, former director of British naval intelligence, wrote in 1979 that on five occasions the Soviets 'illuminated U.S. satellites for periods of up to four hours with [the] power of up to 1,000 times that seen in a forest fire or an ICBM launching.'"[314] Some U.S. intelligence analysts believe the Soviets caused the permanent damage of U.S. reconnaissance satellites.[315]

Intelligence reports in the 1980s indicated that the Soviet laser system posed a significant threat to U.S. satellites.[316] However, the Soviet laser system capabilities appeared more disruptive than destructive.[317] While the extent of Soviet Union blinding is not clear, the U.S. response is still illustrative for the *jus ad bellum* analysis. The United States did not declare any perceived Soviet Union satellite blinding as a use of force. Instead, the United States response in the 1980s was to further finance and develop their own directed-electromagnetic energy anti-satellite capabilities with the Mid-Infrared Chemical Laser testing.[318]

SIGHT 5 (2012) (directed energy use includes jamming enemy communications or jamming radar on the electromagnetic spectrum).

312 *See, e.g.*, Kyle Mizokami, *China Could Blind U.S. Satellites with Lasers*, POPULAR MECHS. (Oct. 1, 2019), https://www.popularmechanics.com/military/weapons/a29307535/china-satellite-laser-blinding/ [https://perma.cc/9H8U-R55C]. General John Raymond, commander of SPACECOM and U.S. Air Force Space Command, stated, "We're pretty comfortable [in asserting] that they [China] are developing directed energy weapons—probably building lasers to blind our satellites." *Id.*; *see also* Christopher M. Petras, *The Use of Force in Response to Cyber-Attack on Commercial Space Systems—Reexamining "Self-Defense" in Outer Space in Light of the Convergence of U.S. Military and Commercial Space Activities*, 67 J. AIR L. & COM. 1213, 1224 (2002) (referring to the Soviet Union using "blinding" lasers on U.S. satellites).

313 *See* Petras, *supra* note 312, at 1224.

314 Sale, *supra* note 307.

315 *Id.* ("According to several U.S. intelligence and aerospace industry sources, a KH-11 or Code 1010 satellite, sustained permanent damage in 1978 when it was 'hosed' by a Soviet laser. These sources believe that such incidents have continued up to the present.").

316 *See* Grego, *supra* note 301, at 6.

317 *Id.*

318 *Id.*; *see also* Blake & Imburgia, *supra* note 309, at 178.

There is a possibility that the Soviet's potential blinding of U.S. satellites was not one-sided. "Although official U.S. policy [was] not to interfere with Soviet satellites, U.S. officials acknowledged the United States had done 'mild hosings' of Soviet satellites trying to observe the launch of U.S. missiles" with laser beams coming from Hawaii and California.[319] Mild hosing is a reference to blinding a satellite by temporarily interfering with its sensing capabilities.[320]

Temporary blinding is the type of electromagnetic interference that closely mirrors interference by cyber means.[321] The majority of the blinding incidents of U.S. satellites were temporary and could be classified as interference during a time of non-declared hostilities.[322] Satellite blinding during peacetime demonstrates that satellite interference by cyber means likely does not rise to the level of a use of force.[323]

Looking to a more modern example of blinding in China, in 2006, Chinese lasers fired at U.S. reconnaissance satellites in low-earth orbit, causing temporary issues with the sensors but creating no lasting damage.[324] China acknowledged it fired the lasers; denied that it attempted to blind the U.S. satellites; and claimed it conducted laser-ranging, -finding, or -illuminating to trace the satellite's location.[325] However, the United States viewed China's action as more than identifying a satellite's loca-

---

[319] Sale, *supra* note 307.

[320] Richard Sale, *Despite Thaw, U.S. Continues 'Hosing' of Soviet Satellites*, L.A. TIMES (Oct. 3, 1991, 12:00 AM), https://www.latimes.com/archives/la-xpm-1991-10-03-mn-4616-story.html [https://perma.cc/QVS9-56JF].

[321] There are some indications that permanent blinding was performed by the Soviets, but this is not as well established as with temporary blinding. *See* Sale, *supra* note 307.

[322] *See id.*

[323] Many advocates believe that traditional electronic warfare, such as jamming radio and communications systems, should be treated the same from an operational perspective as cyberspace attack operations. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 311, at 2. As stated in previous sections, there is evidence jamming radio and communications systems and cyber operations should be treated the same from a legal perspective to reflect this operational reality.

[324] Andrea Shalal-Esa, *China Jamming Test Sparks U.S. Satellite Concerns*, STAR (Oct. 5, 2006, 12:00 AM), https://www.thestar.com.my/news/world/2006/10/05/china-jamming-test-sparks-us-satellite-concerns [https://perma.cc/ZV7L-D8RT] (the director of the Pentagon's National Reconnaissance Office confirmed the incident and said the U.S. satellite was not materially damaged); *see also* Lambakis, *supra* note 248, at 24.

[325] *See* Lambakis, *supra* note 248, at 24.

tion.[326] According to the European Space Agency, China also dazzled French satellites in 2006.[327] Thus, China engaged in behavior similar to the Soviet Union's and the United States' actions during the Cold War.

Satellite interference through blinding has never publicly been declared a use of force by any State.[328] Effects-based supporters may argue that this could change with the right circumstances.[329] However, that is another prospective argument that fails to account for the historic State practice and lack of declaration that it is a use of force after it has occurred. Thus, if electromagnetic interference by blinding or dazzling of satellites is not considered a use of force, then a similar type of interference by cyber means against satellites would also not be considered a use of force.

F. SPOOFING

While various forms of electromagnetic interference have been undertaken by multiple States for decades, demonstrating systematic practice under international law, it is helpful to see a newer technological approach. "Spoofing" is another form of a directed energy operation and, depending on the manner of manipulating the electromagnetic spectrum, has a similar *jus ad bellum* analysis as jamming.[330] There is less known State practice in this area, making it difficult to determine if the behavior is a use of force. Nonetheless, the few publicly known examples of spoofing are illustrative of customary international law.

Spoofing is often lumped together with electromagnetic jamming and may be seen as a sub-category of jamming. The Army Space Operations Field Manual lists spoofing and electromagnetic jamming in the same category.[331] Likewise, some scholars lump jamming and spoofing in the same category.[332]

---

[326] U.S.-CHINA ECON. AND SEC. REV. COMM'N, *supra* note 17, at 213 (perceiving China's leaders likely tempted to attack the U.S. space system rather than use traditional war means).

[327] *Id.*

[328] *See* Mountin, *supra* note 35, at 176–77.

[329] *See id.* at 177–78.

[330] ARMY SPACE OPERATIONS, *supra* note 41, paras. 2-81 to 2-83.

[331] *Id.*

[332] *See, e.g.*, Mountin, *supra* note 35, at 130 ("Known as a type of electronic decoy, spoofing is similar to jamming."); *see also* Bourbonnière, *supra* note 40, at 58 ("Electronic weapons are used to interfere with satellite uplinks and downlinks by either spoofing or jamming these links."). For example, the 9,833 instances of

International bodies seem to approach spoofing and jamming in a similar manner, especially in GPS interference. For instance, ICAO views jamming and spoofing as forms of intentional interference, and standards for handling both are similar.[333] Thus, in some ways spoofing and jamming are two sides of the same electromagnetic-interference coin.

Nonetheless, there are some differences between spoofing and jamming. The Army Field Manual explains that "[s]poofing is a technique of broadcasting an emulated signal with false or misleading information in an attempt to deceive a receiver or system into processing the fake data."[334] Spoofing is different from jamming because it mimics the true signals, whereas jamming drowns out the real signal.[335] However, GPS users typically know they are jammed because the interference causes their system to fail to function. Alternatively, when someone is spoofed, they are less likely to know because they believe that the false signal is correct.[336] Thus, there are some differences between jamming and spoofing, even though both are sometimes lumped together.

One instance of Russian spoofing includes an Israeli airport from June 2019. Israel complained that Russian spoofing caused missing data for pilots and had a "significant impact" on airport operations.[337] Rather than admitting it was its electronic warfare system emanating from its base over 200 miles away, Russia denied its role in the spoofing.[338]

Iran has also possibly engaged in a sophisticated form of spoofing against a U.S. Central Intelligence Agency drone in 2011. After capturing the U.S. drone, Iranian electronic warfare specialists claimed they cut off communications to the drone

---

GPS interference by Russia previously cited had jamming and spoofing in the same category. C4ADS, *supra* note 218, at 15.

[333] *See* Int'l Civil Aviation Org. [ICAO], *supra* note 293, at 23.

[334] ARMY SPACE OPERATIONS, *supra* note 41, para. 2-83.

[335] *See* Mountin, *supra* note 35, at 130 (citing WRIGHT, GREGO & GRONLUND, *supra* note 223, at 118).

[336] *See* Bourbonnière, *supra* note 40, at 58.

[337] *Russia Denies Role in Israeli Airport GPS Jamming*, BBC NEWS (June 27, 2019), https://www.bbc.com/news/technology-48786085 [https://perma.cc/5PN3-4HCG].

[338] *See id.* The spoofing of an Israeli airport requires a different *jus ad bellum* analysis from the other situations because this has the potential to be a form of electronic warfare that is part of a larger conflict in the physical world. Essentially, since Russian planes are dropping bombs in Syria, there is already an armed conflict nearby, and this could be a collateral consequence of that nearby conflict.

and reconfigured the GPS coordinates to make it land in Iran rather than its designed landing location in Afghanistan.[339] The United States did not respond by claiming it was a use of force but simply asked for the drone's return.[340] There are different geopolitical factors at play for the U.S. response and questions about what occurred.[341] Nonetheless, if Iran spoofed a drone to capture it, this demonstrates that even the capture of military equipment through spoofing does not rise to the level of a use of force.

Another example of electromagnetic interference involves China's series of cyber operations directed at U.S. satellites from 2007 to 2008.[342] The first three incidents involved electromagnetic interference similar to jamming or spoofing, except China likely conducted the interference by cyber means. Specifically, in October 2007, the U.S. Landsat-7 (a U.S. observation satellite) "experienced 12 or more minutes of interference," which occurred again in July 2008 for the same amount of time.[343] In June 2008, another U.S. observation satellite, the Terra EOS, "experienced two or more minutes of interference," and China was believed to be the culprit.[344] However, the satellite took all the steps to command the Terra EOS in this instance but did

---

[339] Scott Peterson & Payam Faramarzi, *Exclusive: Iran Hijacked US Drone, Says Iranian Engineer*, CHRISTIAN SCI. MONITOR (Dec. 15, 2011), https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer [https://perma.cc/KQ5M-ZNEF]; *see also* Frank Oliveri, *The Pentagon's GPS Problem*, CQ WEEKLY (Feb. 9, 2013, 2:45 PM), http://public.cq.com/docs/weeklyreport/weeklyreport-000004218242.html?src=DB [https://perma.cc/UFY4-ST5Z] ("Iran's capture of a U.S. military drone in 2011 is widely believed to have resulted from a spoofing attack where the drone pilot accidentally landed the plane in Iran, believing it was landing at its base in Afghanistan."). The Central Intelligence Agency (CIA) denied that it was spoofing and claimed it was a faulty data stream that caused the drone to be downed in Iran. *See* RID, *supra* note 299, at 15 ("After a ten-week review of the incident the CIA reportedly found that a faulty data stream had caused operators to lose contact with the drone, rather than Iranian interference or jamming."); *see also* Adam Rawnsley, *Iran's Alleged Drone Hack: Tough, but Possible*, WIRED (Dec. 16, 2011, 6:01 PM), https://www.wired.com/2011/12/iran-drone-hack-gps/ [https://perma.cc/K6DB-ANBN] (indicating possibility that drone was spoofed but not in manner described by Iranian engineer). However, the United States may be making the claim so as to not admit one of its drones is capable of being hacked.

[340] Rick Gladstone, *Iran Is Asked to Return U.S. Drone*, N.Y. TIMES (Dec. 12, 2011), https://www.nytimes.com/2011/12/13/world/middleeast/obama-says-us-has-asked-iran-to-return-drone.html [https://perma.cc/V29E-6U9W].

[341] *See id.*

[342] U.S.-CHINA ECON. AND SEC. REV. COMM'N, *supra* note 17, at 216.

[343] *See id.*

[344] *See id.*

not issue any commands.[345] On October 22, 2008, Terra EOS "experienced nine or more minutes of interference," and the party took all necessary steps to control the satellite "but did not issue commands."[346]

The cyber operation activities against Landsat and Terra EOS are similar to other types of jamming or interference that customary international law and Article 41 of the U.N. Charter indicate are not a use of force. Like other electromagnetic incidents, the United States does not publicly indicate these incidents are a use of force. This cyber interference practice on U.S. satellites shows a pattern among States to not declare electromagnetic interference as a use of force.

G. Hypothetical Cyber Operations and Use of Force

Under the *jus ad bellum* analysis, a cyber operation could theoretically be a use of force if it is an activity beyond communication interruption under Article 41 of the U.N. Charter or electromagnetic interference in which States have historically engaged.[347] Specifically if it involves using cyberspace as an extension of traditional weapons.

The control of a drone or satellite by *directing* it to crash could be a use of force. However, it would likely need to be beyond interference-type activities and thus would no longer be classified as interference by cyber means.

Another possibility of a cyber operation being a use of force is a nuclear explosion within a country's missile silo or reactor, which may cause the traditional use of force analysis to be recalculated under the U.N. Charter. However, a nuclear explosion caused through cyberspace is an improbable hypothetical scenario.[348] Reworking a *jus ad bellum* approach for cyberspace before the actual use of force may be politically motivated and create a vague construct not based on traditional international law constructs.[349]

---

345 *Id.*

346 *Id.*

347 *See* U.N. Charter art. 41.

348 Rid, *supra* note 299, at 174. "[C]yber war theorists of the 2010s have never experienced the actual use of a deadly cyber weapon, let alone one a devastating one like 'Little Boy.'. . . Based on a careful evaluation of the empirical record, based on technical detail and trends, and based on the conceptual analysis presented here, a future cyber-Hiroshima must be considered highly unlikely." *Id.*

349 *See* Waxman, *supra* note 6, at 451.

It is worth noting what type of cyber operation is not a use of force. Principally, acts of espionage do not rise to a use of force.[350] The *Tallinn Manual* and effects-based supporters draw similar conclusions that cyber espionage does not amount to a use of force.[351] Additionally, interference in elections is likely a violation of the non-intervention principle but does not rise to the level of a use of force.[352] These topics deserve their own analysis, but cyber-espionage not being a use of force is overwhelmingly the majority opinion.[353]

The type of cyber operation to rise to the level of a use of force would likely have to be beyond mere electromagnetic interference that States have engaged in for ninety years and have become more technically advanced and targeted. Cyber operations would also likely have to be behavior beyond temporary or partial interruption of communication as outlined in Article 41 of the U.N. Charter to be a use of force. Thus, interference by cyber means is not a use of force.

V. CONCLUSION

Interference by cyber means as potential use of force should be analyzed under Article 41 of the U.N. Charter and State practice of electromagnetic interference during peacetime. The U.N. Charter framers did a remarkable job of defining and developing *jus ad bellum* for communication interruption. The ordinary meaning of Article 41 and the drafting history of the U.N. Charter support the ordinary reading. Additionally, State practice of jamming during peacetime has occurred for ninety years, and nearly every nation has engaged in various forms of electromagnetic interference involving GPS, television and radio broadcasts, and satellite operations.[354] The status of *jus ad bellum* for interference by cyber means may cause negative politi-

---

[350] *See* Hollis, *supra* note 6, at 1050–51 (the overwhelming consensus is that espionage is not an armed attack or use of force).

[351] Schmitt, *supra* note 4, at 576 ("[E]spionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state's territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace.").

[352] *See* Ney Remarks, *supra* note 87.

[353] *See* Beard, *supra* note 20, at 69 ("In spite of dire, repeated predictions to the contrary, a cyberwar (an armed conflict limited to cyber actions alone) may in fact be unlikely."); *see also* Patterson, *supra* note 63, at 975 ("Current manifestations of cyber attacks rarely achieve militaristic ends, but rather take the form of espionage, crime, or political and economic coercion.").

[354] *See* BERG, *supra* note 13, at 44.

cal, economic, or other effects. The solution to these negative consequences lies in the traditional means of changing international law.[355]

---

[355] *See generally* Waxman, *supra* note 6 (discussing scholarship focused on how international law might be interpreted or amended to take account of new technologies); Hollis, *supra* note 6 (proposing that a new set of rules should be in place for information operations).