Center on Law, Ethics and National Security

Essay Series
Number 12
January 11, 2022

The "Havana Syndrome" and the Use of Force: Reality, Hypotheticals, and the Effect of Changing International Norms

By Lindsay K. Kenney

THE "HAVANA SYNDROME" AND THE USE OF FORCE: REALITY, HYPOTHETICALS, AND THE EFFECT OF CHANGING INTERNATIONAL NORMS

LINDSAY K. KENNEY

ABSTRACT

As the conflicts and wars known by the authors of the U.N. Charter disappear from the forefront of the modern battlefields, the analytical methods employed by the U.N. Charter have found themselves in new territory. One of the most pressing and studied issues under the U.N. Charter in recent years has been the application of Article 2(4), the general prohibition on the use of force to modern day warfare. This Paper explores that issue in the context of a radio frequency energy attack, aimed at American diplomats, stationed across the globe—a phenomenon known in the press as the "Havana Syndrome." Though the Havana Syndrome only represents a hypothetical weapon at this point in time, it presents an interesting angle of analysis for a modern-day use of force application. This Paper borrows from Michael Schmitt's analytical framework for use of force in the cyber context to provide insight as to how the suggested framework would operate in another legally ambiguous context. This Paper concludes broadly that there has been a shift from a strict adherence to the application of Article 2(4), towards a consequence-based approach. The evolving legal norms in the use of force context will likely continue to stray away from a strict analysis under the narrow construction of Article 2(4). Thus, unless there is a concerted effort for a new framework—which seems unlikely—these next few years will be instrumental in defining a new, modern scope of Article 2(4).

INTRODUCTION

"Havana Syndrome" has been in the popular press since 2016, from reports from American and Canadian diplomatic missions to Havana, Cuba.[1] The federal employees reported "sudden onset of a loud noise,

[1] As a general note, this Paper is utilizing the Havana Syndrome reports to provide an analysis for a hypothetical directed energy, radio frequency weapon, with the same storyline as that of the Havana Syndrome, under the use of force framework in international law. This author recognizes that there is no conclusive evidence of such a weapon, and that the New York Times has reported that there is no human intelligence or signals intelligence pointing to the existence of such a weapon, despite lawmakers and other U.S. officials "openly stat[ing]" that a directed energy, radio frequency weapon is likely the cause of the Havana Syndrome symptoms. However, the suggestion of such a weapon and the facts and circumstances in which the "Havana Syndrome" has appeared around the world provides an interesting basis for analysis under international law, and so

perceived to have directional features … accompanied by pain in one or both ears or across a broad region of the head, and … a sensation of head pressure or vibration, dizziness, followed … by tinnitus, visual problems, vertigo, and cognitive difficulties."[2] Such symptoms have also been reported by personnel at the U.S. Consulate in Guangzhou, China in 2017.[3]

President Biden even signed the aptly named "Helping American Victims Afflicted (HAVANA) Act" on October 8, 2021, to authorize medical and financial support for afflicted diplomats and intelligence officers.[4] by Neurological Attacks The National Academies of Sciences, Engineering, and Medicine ("NASEM") suggested that these symptoms may have been caused by a "direct, pulsed radio frequency (RF) energy," but the evidence of such technical capabilities, and that they were used in relation to the symptoms of personnel from China and has yet to be proved.[5]

The type of analogy this Paper puts forth—analyzing emerging technology with existing law—can raise the questions of whether new regulations are needed, and when are they needed?[6] This Paper does not suggest that new regulations are needed in response to a potential RF weapon, but rather, attempts to highlight ambiguities in the current law, as well as the suggested framework for cyber response, to showcase the avenues of analysis that a state could use under international law when posed with the case presented here. In analyzing the potential use of RF

---

the Paper proceeds as if such a weapon existed conclusively. Alexander Ward and Quint Forgey, *A Blow to the 'Directed-Energy' Havana Syndrome Case*, POLITICO (Dec. 3, 2021), https://www.politico.com/newsletters/national-security-daily/2021/12/03/a-blow-to-the-directed-energy-havana-syndrome-case-495322; Julian E. Barnes and Adam Goldman, *Review Finds No Answers to Mystery of Havana Syndrome*, N.Y. TIMES (Dec. 2, 2021), https://www.nytimes.com/2021/12/02/us/politics/havana-syndrome.html; *Cheryl Rofer*, Claims of Microwave Attacks are Scientifically Implausible, FOREIGN POLICY (May 10, 2021, 12:41 PM), https://foreignpolicy.com/2021/05/10/microwave-attacks-havana-syndrome-scientifically-implausible.

[2] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING & MEDICINE, AN ASSESSMENT OF ILLNESS IN U.S. GOVERNMENT EMPLOYEES AND THEIR FAMILIES AT OVERSEAS EMBASSIES 2 (2020), *at* https://www.nationalacademies.org/news/2020/12/new-report-assesses-illnesses-among-us-government-personnel-and-their-families-atoverseas-embassies [hereinafter NASEM REPORT].

[3] *Raul "Pete" Pedrozo*, The International Legal Implications of "Havana Syndrome," LAWFARE (Dec. 23, 2020, 8:01 AM), https://www.lawfareblog.com/international-legal-implications-havana-syndrome.

[4] Helping American Victims Afflicted by Neurological Attacks Act of 2021, Pub. L. No. 117-46, 135 Stat. 391; *Warren P. Strobel*, Havana Syndrome Victims to Receive Financial Support Under New Law, WALL ST. J. (Oct. 8, 2021, 3:39 PM), https://www.wsj.com/articles/havana-syndrome-victims-to-get-u-s-support-under-new-law-11633717099.

[5] NASEM REPORT, *supra* note 2, at 2; *Pedrozo*, *supra* note 3.

[6] *See* Rebecca Crootof, *Regulating New Weapons Technology: The Impact of Emerging Technologies on the Law of Armed Conflict*, *in* The Impact of Emerging Technologies on the Law of Armed Conflict 9 (Eric Talbot Jensen & Ronald T.P. Alcala eds. 2019) ("When confronted with a new weapons technology, international law scholars, military lawyers, and civil society activists regularly raise two questions: Are new regulations needed?[2] And are they needed *now*?").

weapons, and the legal implications and rights that follow, this Paper recognizes that U.S. adversaries like China and Russia are ever-increasingly relying on non-traditional methods of warfare and lawfare to conduct damaging activities against the U.S. and its allies.[7] However, before discussing the legal implications of any potential microwave attacks, it is important to distinguish the facts: what we do and do not know.

What we do know.

Since the initial reports in 2016, 2017, and 2018 from diplomats and intelligence personnel in Cuba and China, individuals serving in Russia, Poland, Taiwan, Serbia, and Colombia all reported the same symptoms; even recently, an individual on CIA Director Burns' team reported symptoms from a trip to India in September of 2021.[8] The actual science behind the phenomenon also remains unclear. It was initially thought that the symptoms were developed from the use of an acoustic or sonic weapon; however, as stated above, NASEM, as well as an independent 2018 study, concluded that the symptoms likely resulted from a microwave, or radio frequency type energy.[9] The NASEM report, requested by the U.S. Department of State, "An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies," did not reach conclusive answers on what weapon could cause that type of direct energy to target individuals.[10]

The NASEM report found that while the symptoms vary, "[t]he most common and distinctive features of the initial onset and acute phase" among those affected in Havana "were the sudden onset of a perceived loud sound, sometimes described as screeching, chirping, clicking or piercing, a sensation of intense pressure or vibration in the head and pain in the ear or more diffusely in the head."[11] The initial acute phase occurred "only in certain physical locations" and "seemed to originate from a particular direction."[12] While some individual only experienced this initial phenomenon, others that were affected had recurring, and then chronic, symptoms.[13] A University of Pennsylvania examination of 40 affected individuals also found evidence of brain damage.[14] The standing committee concluded that the symptoms of the individuals were consistent with RF

---

[7] *Pedrozo*, *supra* note 3.
[8] *Byron Tau*, Havana Syndrome: What We Know, WALL ST. J. (Oct. 12, 2021, 2:14 PM), https://www.wsj.com/articles/havana-syndrome-symptoms-11626882951.
[9] *Id.*; *see generally* NASEM REPORT, *supra* note 2.
[10] *See* NASEM REPORT, *supra* note 2 ("Multiple hypotheses and mechanisms have been proposed to explain these clinical cases, but evidence has been lacking, no hypothesis has been proven, and the circumstances remain unclear.").
[11] *Id.* at 11.
[12] *Id.*
[13] *Id.*
[14] *Byron Tau*, Havana Syndrome: What We Know, WALL ST. J. (Oct. 12, 2021, 2:14 PM), https://www.wsj.com/articles/havana-syndrome-symptoms-11626882951.

effects after considering multiple possible causes, including "directed, pulsed radio frequency (RF) energy, . . . chemical exposures, infectious diseases and psychological issues."[15] Overall, the study catalogued the symptoms, and excluded some possibilities, but it failed to provide, at least publicly, direct answers.

What we do not know.

We do not know anything concrete. Intelligence agencies have yet to publicly determine how these attacks are orchestrated, what type of weapon is used, or which actor is responsible.[16] The New Yorker reported a "working theory" that foreign intelligence agencies, potentially Russia's GRU military intelligence, "was aiming microwave devices at U.S. officials with the aim of collecting data from their computers and cellphones"—but this has yet to be proven.[17]

Some commentators have suggested that such attacks are highly implausible and that there is "exceedingly weak" evidence that the symptoms of the Havana Syndrome would be caused by microwave effects.[18] While the State Department has declined to comment, they have state that they are "actively working to identify the cause of these incidents"—whatever that means.[19] A 2018 ARB report that cited reports of symptoms from Uzbekistan and Russia also criticized President Trump's State Department's mishandling of the situation.[20] The C.I.A. created a task force aimed at understanding the causes of Havana Syndrome, and current-Director William Burns has stated that the agency is "very focused on getting to the bottom of this."[21] All-in-all, the government provided a variety of political non-answers.

While this Paper will not argue the merits of whether this is indeed an RF attack or make any claims about the plausibility of the science behind such a weapon, it will take the NASEM standing committee at its word that

---

[15] NASEM Report, *supra* note 2, at 2.
[16] *Byron Tau*, Havana Syndrome: What We Know, WALL ST. J. (Oct. 12, 2021, 2:14 PM), https://www.wsj.com/articles/havana-syndrome-symptoms-11626882951.
[17] *Id.*
[18] *Cheryl Rofer*, Claims of Microwave Attacks are Scientifically Implausible, FOREIGN POL'Y (May 10, 2021, 12:41 PM), https://foreignpolicy.com/2021/05/10/microwave-attacks-havana-syndrome-scientifically-implausible.
[19] *Joseph Clark*, 'Havana Syndrome' Mystery Expands With New Cases at U.S. Embassy in Colombia, WASH. TIMES (Oct. 13, 2021), https://www.washingtontimes.com/news/2021/oct/13/havana-syndrome-mystery-expands-new-cases-us-embas.
[20] U.S. DEP'T OF STATE, HAVANA, CUBA ACCOUNTABILITY REVIEW BOARD REPORT 2 (2018), at https://nsarchive.gwu.edu/briefing-book/cuba/2021-02-10/secrets-havana-syndrome-how-trumps-state-department-cia-mishandled-mysterious-maladies-cuba.
[21] *Julian E. Barnes*, C.I.A. to Expand Inquiry into Mysterious Health Episodes Overseas, N.Y. TIMES (Oct. 12, 2021), https://www.nytimes.com/2021/03/04/us/politics/cia-havana-syndrome-mystery.html; *Glenn Thrush*, William J. Burns, The C.I.A. Director, Outlines Plans to Confront the 'Havana Syndrome', N.Y. TIMES (Jul. 22, 2021), https://www.nytimes.com/2021/07/22/us/politics/cia-havana-syndrome.html.

this was indeed and RF attack and analyze a potential use of force scenario based on such an attack. It will do so in the following order: Section I will provide an overview of the international law and U.S. viewpoint on the use of force, Section II will highlight the international implications of an RF weapon both from the U.N. Charter and U.S. standpoints, and Section III will use the emerging cyber operations and use of force framework to analyze the impact of an RF weapon.

I. THE RIGHT OF THE USE OF FORCE AND SELF-DEFENSE UNDER INTERNATIONAL LAW

Both international customary law and international law *lex lata* prohibit the threat of or use of force.[22] Article 2(4) of the United National Charter ("U.N. Charter") provides for a near complete ban on the use of force: *"Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*[23]

The historic ban on force was built on the work of theologians like Saint Augustine, Saint Thomas, and historic international law scholars like Hugo Grotius.[24] These scholars developed the "Just War Tradition" which sought to reconcile what "war did to one's eternal soul."[25] "Just Wars" were generally wars premised upon a just cause—either a law enforcement cause, self-defense, protection of rights, or an exhaustion of all other mechanisms for reconciliation.[26] Since World War I and World War II, a general prohibition to the use of force emerged in the international community, though there are certain instances where a state may resort to force. The rest of this section will describe such instances, as well as how a state may *legally* use force when it has gained the right to do so.

Article 51 of the U.N. Charter provides an exception to the prohibition on the use of force, where a state invokes force as a means of

---

[22] U.N. Charter, art. 2, ¶ 4. This codification is the culmination of the goals of the just war theory, as well as the failed Kellogg-Briand Pact, which was a general treaty, following World War I, which tried to outlaw war as an instrument of international policy. General Treaty for Renunciation of War as an Instrument of National Policy, Aug. 27, 1928, 46 Stat. 2343, 94 L.N.T.S. 57 (commonly known as the "Kellogg-Briand Pact").

[23] U.N. Charter, art. 2, ¶ 4.

[24] *See, e.g.*, U.S. DEP'T OF DEFENSE, LAW OF WAR MANUAL ¶ 1.1.1 (Dec. 2016) [hereinafter DOD LAW OF WAR MANUAL] ("Certain *jus ad bellum* criteria have, at their philosophical roots, drawn from principles that have been developed as part of the Just War Tradition."); War, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (May 3, 2016), https://plato.stanford.edu/entries/war.

[25] Randall Lesaffer, *Too Much History: From War as Sanction to the Sanctioning of War*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 4 (Marc Weller eds., 2015).

[26] *See generally id.* (chronicling the history of the "Just War Theory" from its inception to modern usage).

self-defense when it is the subject of an armed attack.[27] States may also invoke self-defense where it is reasonably believed that an armed attack is imminent.[28] The U.N. Charter describes self-defense as an 'inherent right' and in the *Nicaragua* case, the International Court of Justice ("ICJ") recognized the "'pre-existing customary international law' basis for States" right of self-defense.[29]

Notably, the U.N. Charter does not define "armed attack."[30] Consequently, state actors hold varying views on whether an act of force meets the threshold to qualify as an armed attack. For example, the United States views any use of force within Article 2(4) as an *ipso facto* armed attack under Article 51.[31] However, in the *Nicaragua* case, the ICJ indicated that the scope of an 'armed attack' is narrower than 'use of force'; the ICJ held that armed attacks are "the most grave forms of the use of force" and thus only a use of force that is of sufficient "scale and effects" may amount to an armed attack.[32] Such an assessment is fact-dependent—for example, the ICJ found in the *Nicaragua* and *Oil Platform* cases, respectively, that (i) the supply of arms and general support by the U.S. was a *de minimis* use of

---

[27] Article 42 also provides that the U.N. Security Council may also allow a State to take measures via force for international peace and security where methods short of the use of force fail. This is known as a "collective security system." Sean M. Condron, Justification for Unilateral Action in Response to the Iraqi Threat: A Critical Analysis of Operation Desert Fox, 161 MIL. L. REV. 115, 126 (1999); *see also* U.N. Charter, art. 41 ("The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures."); U.N. Charter, art. 42 ("should the Security Council consider that the 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.").

[28] There is some argument as to the meaning of "imminent" in the use of force context in international law. Many believe that it must be as described in the famous *Caroline* case: "instant, overwhelming, and leaving no choice of means and no moment for deliberation." Ashley Deeks, *"Imminence" in the Legal Advisor's Speech*, LAWFARE (Apr. 6, 2016, 7:00 AM), https://www.lawfareblog.com/imminence-legal-advisers-speech; However, as evidenced since the Obama Administration, some stated believe in a concept known as "anticipatory self-defense," where the actor "has not yet engaged in an armed attack but has the capability to do so and is planning such attacks." *Id.*

[29] *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment (Merits) [1986] ICJ Rep. 14, ¶ 176.

[30] *See generally* U.N. Charter.

[31] DOD LAW OF WAR MANUAL, *supra* note 24, ¶ 1.11.5.2; *see* Harold H. Koh, 'International Law in Cyberspace' (2012) 54 HARVARD INT'L L. J. ONLINE 1, 7 ("[T]he United States has for a long time taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."). The U.S. thus claims that it retains the inherent right to self-defense in response to "any illegal use of force." DOD LAW OF WAR MANUAL, *supra* note 24, ¶ 1.11.5, n. 224 (citing Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MIL. L. REV. 89, 93 (1989)).

[32] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).

force short of an armed attack and (ii) that the mining of a U.S. vessel was not a "grave" use of force, and thus not an armed attack.[33]

Once a state makes a good faith determination that the right of self-defense can be invoked, under customary law, the principles of necessity and proportionality must be complied with for a lawful self-defense action.[34] Each will be described in turn below.

First, in general, the principle of necessity requires that the action be a "last resort" whereby all other "peaceful measures have been found wanting or . . . [clearly] futile."[35] As atoned in the varied letters from U.S. Secretary of State Daniel Webster in the *Caroline* case, the immediacy of the response is indicative of a necessary self-defense measure.[36] However, what is deemed immediate in scope is unclear. The ICJ's decision in the *Nicaragua* case suggests that the U.N. Charter requires narrow reading of the use of force provisions.[37] The Court held the use of force by the U.S. was not compliant with the principle because the threat of the armed opposition had been so diminished in the time since the initial incident.[38] However, as evidenced by the U.S. raid on Libya, the U.S.'s view on immediacy is more expansive than that of the ICJ in the *Nicaragua* case[39]— though it is important to note that this raid was heavily criticized.[40]

---

[33] *Id.* at ¶¶ 237, 238; *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, Judgment (Merits) [2003] ICJ Rep. 161, ¶ 64.

[34] *Nicaragua*, (n. 6) ¶ 176; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, at n. 127 ¶ 41 (Jul. 8); *Oil Platforms* (n. 18) ¶ 76–77. Furthermore, these two principles are considering "inherent in the very concept of self-defense."

[35]Eighth Report on State Responsibility by Mr. Roberto Ago, Special Rapporteur – The Internationally Wrongful Act of the State, Source of International Responsibility (Part 1), UN Doc. A/CN.4/318/Add.5-7 (29 February, 10 and 19 June 1980) ¶ 120.

[36] J. Moore International Law Digest 1906; Secretary Webster denied the necessity of force by the British because he claimed that the British must have proven that the need for self-defense was "instant, overwhelming, leaving no choice of means." Franz W. Paasche, The Use of Force in Combatting Terrorism, 25 COLUMB. J. TRANSNAT'L L. 377, 389 (1987).

[37] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 237 (June 27).

[38] *Id.*

[39] The official U.S. position was that the attack was "neither a peacetime reprisal nor an act of relation, . . . [but] [i]t was a limited act of self-defense against a continuing threat." W. Hays Parks, Lessons from the 1986 Libya Airstrike, 36 NEW ENG. L. REV. 755, 760 (2002).

[40] *See* Jack M. Beard, America's New War on Terror: The Case for Self-Defense Under International Law, 25 HARV. J. L. & PUB. POL'Y 559, 584, n.88 (2002) (noting that there was significant objection to the U.S. raid in 1986, including suggestions that it passed the threshold of self-defense into reprisal due to its lack of adherence to the principals of necessity and proportionality); *see* Christopher Greenwood, International Law and the United States' Air Operation Against Libya, 89 W. VA L. REV. 933, 933 (1987) ("Arab states, on the other hand, condemned it as an act of aggression, while other critics of the raid saw it as an over-reaction which exceeded the limits imposed by international law on the use of force, even if they accepted that Libya was involved in terrorism.").

Second, any response taken in self-defense must be proportional. A proportional response in the *jus ad bellum* context[41] must be constrained "to what is reasonably necessary to promptly secure the permissible objectives of self-defence."[42] While it is not required that the force is of similar kind of the initial attack, it is required that there is a relationship between the scale of the predicate attack and the defensive act.[43] The Court in the *Nicaragua* case found that the force used by the United States (i.e., mining of ports and attacks on Nicaraguan naval vessels) was over the limit of proportionality as compared to the support provided to the Contra regime.[44]

Overall, the decision to use force as a method of self-defense requires an important calculation by any State. However, in evaluating any state's decision to use force, all must recognize the short-time frame and pressures that a particular state and their military officers may be under when conducting and orchestrating a self-defense operation. The U.S. Department of Defense ("DoD") Law of War Manual provides that a commander must make reasonable determinations on proportionality, but such decisions have subjective aspects and commanders may only be judged ex post with a "degree of deference" and keeping in mind the information available to the commander at the time of the decision.[45]

The next section will use the use of force and self-defense framework from both the U.N. Charter and U.S. perspective to discuss the potential implications under international law of potential attacks of the type, nature, and scale as those suggested by the elusive "Havana Syndrome."

II. INTERNATIONAL IMPLICATIONS OF AN RF WEAPON

As discussed above, the assessment of whether force is justified is a fact-dependent endeavor. The claim for self-defense depends on the "scale and effects" of an attack, and in the case of the U.S., the use of *any* level of force.[46] This section will proceed by first looking at the potential that an RF weapon would be characterized as a use of force under international law *lex lata*, and then second, utilize Michael Schmitt's suggested international law

---

[41] Note, that there is a difference between proportionality in the *jus in bello* and *jus ad bellum* contexts, which the DOD LAW OF WAR MANUAL describes. DOD LAW OF WAR MANUAL, *supra* note 24, ¶¶ 1.11.1.2, 3.5.1 (describing the differences between the use of force and law of armed conflict proportionality analyses).

[42] Right of individual and collective self-defence, 69 Oxford university handbook (citing Myres S. McDougal and Florentino P. Feliciano, *The International Law of War: Transnational Coercion and World Public Order* (New Haven Press, 1994) 242).

[43] Robert Chesney, *Who May Be Killed? Anwar al-Awlaki as a Case Study in the International Legal Regulation of Lethal Force*, *in* Y.B. OF INT'L HUMANITARIAN L. 3, 70 (Michael N. Schmitt, Louise Arimatsu & T. McCormack eds., 2010).

[44] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 237 (June 27).

[45] DOD LAW OF WAR MANUAL, *supra* note 24, ¶¶ 5.10.2.2–5.10.2.2.3.

[46] *See* supra n.28–29 and accompanying text.

on the use of force *lex ferenda* as it relates to cyberwarfare[47] to analyze what effects the framework would have on a hypothetical RF weapon with affects such as those from the "Havana Syndrome."

This Paper will not discuss the implications of the suggested RF weapon under the international law framework on weapons, but providing some background is necessary to color the picture. [48] One of the principal customary principles in international law is codified in the Brussels Declaration (1874) with the notion that "belligerents [do not possess] an unlimited power in the adoption of means of injuring the enemy."[49] This principle is codified in the Hague Regulations of 1899[50] and 1907,[51] and Article 35(1) of Additional Protocol I to the Geneva Conventions.[52] A second customary principle is cardinal in the law of armed conflict: the prohibition of "arms, projectiles or material calculated to unnecessary suffering."[53] Lastly, indiscriminate attacks are prohibited; thus weapons must be able to be directed at a specific military object and must be able to be limited as is required by principle of distinction.[54] With any weapons used by a state, these principles must be followed.

These principles underly the current international laws, regulations, and customs relating to the use of force and self-defense—particularly, when a country determines whether they will use force as an act of self-defense. In the *Nuclear Weapons* opinion, the International Court of Justice ("ICJ"), in response to a request for an opinion from the U.N. Charter Security Council, found that the U.N. Charter neither permits nor prohibits *Nuclear Weapons* as an option for states to take into account when

---

[47] Note that this paper uses cyberwarfare and cyber operations interchangeably but recognizes that the term "war" is synonymous with "armed conflict"—a term that has international law consequences—and that no state has claimed that it is in a war or armed conflict based on hostile cyber operations. Michael N. Schmitt, *Terminological Precision and International Cyber Law*, LIEBER INSTITUTE: ARTICLES OF WAR (Jul. 29, 2021), https://lieber.westpoint.edu/terminological-precision-international-cyber-law.

[48] *See generally* Bill Boothby, *Space Weapons and the Law*, 93 INT'L L. STUD. NAVAL WAR COLL. 179 (2017).

[49] Project of an International Declaration concerning the Laws and Customs of War art. 12, Aug. 27, 1874, *reprinted in* THE LAWS OF ARMED CONFLICTS 23 (Dietrich Schindler &Jiri Toman eds., 4th ed. 2004).

[50] Regulations Respecting the Laws and Customs of War on Land art. 22, annexed to Convention No. II with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803, T.S. No. 403.

[51] Regulations Respecting the Laws and Customs of War on Land art. 22, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227, T.S. No. 539 [hereinafter 1907 Hague Regulations].

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

[53] 1907 Hague Regulations, *supra* note 51, art. 23(e).

[54] API, *supra* note 52, art 51(4); *Nicaragua*, (n. 6) ¶ 176; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, at ¶ 78 (Jul. 8) ("States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets.").

determining what is necessary in pursuit of legitimate military objectives.[55] Though many states believed nuclear weapons should be unlawful, there was neither a treaty saying so, nor *opinion juris* on the matter.[56] The Court found that, as applied in all situation, self-defense can only warrant proportional and necessary responses and states must apply such an analysis when using nuclear weapons.[57] In determining the response to a potential use of force via an RF weapon, states must likewise response with proportional and necessary means.

A. Under the law of the use of force: lex lata

To start, this section will focus on whether a hypothetical RF weapon, with effects such as the "Havana Syndrome," would constitute a violation of Article 51 of the U.N. Charter such that a response of force in self-defense would be justifiable.

1. Use of Force under U.S. Law. The victim-state of the Havana Syndrome, the United States, reserves the right to self-defense for *any* use of force within Article 2(4).[58] The DoD Law of War Manual further provides that the U.S. reserves the right to protect its nationals abroad.[59] The threshold of what constitutes force, such that self-defense would be appropriate, under the U.S. requirement is necessarily a much lower bar.[60] The effects of an RF weapon in this instance—targeted, long-lasting, brain damage—could amount to force at the level for which self-defense is justified for the U.S.

Note that any self-defense response by the U.S. in the state where one of the these embassies are located may be justified by the heavily debated principle that the target state was unwilling, or unable to provide protection for targeted U.S. citizens.[61] In this instance, it would likely require some sort of signal from the state in which the targeted U.S. embassies were located.[62] This would clearly be muddled by the issue of

---

[55] *See generally Nuclear Weapons*.
[56] *Id.*
[57] Particularly because nuclear weapons release immense quantities of heat and powerful and prolonger radiation; essentially the power to destroy all civilization and planet ecosystem. *Id.*
[58] *See* footnote 31 and accompanying text.
[59] DOD LAW OF WAR MANUAL, *supra* note 24, ¶ 1.11.5.3 (citing Ambassador William Scranton, U.S. Representative to the United Nations, *Statement in the U.N. Security Council* regarding Israeli action at Entebbe, Jul. 12, 1976, 1976 DIGEST OF U.S. PRACTICE IN INT'L LAW 150 ("[T]here is a well-established right to use limited force for the protection of one's own nationals from an imminent threat of injury or death in a situation where the State in whose territory they are located either is unwilling or unable to protect them. The right, flowing from the right of self defense, is limited to such use of force as is necessary and appropriate to protect threatened nationals from injury.").
[60] See *infra* footnote 29 and accompanying text.
[61] *See infra* Section I.
[62] Note that there is no agreed international consensus for what such a test would entail. *See e.g.*, Ashley S. Deeks, "Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense, 52 VA. J. OF INT'L L. 483 (2012). Though one scholar has

attribution, and the third-party state's relationship, or lack thereof, with the assaulting state. For example, an attack at a U.S. embassy in Ukraine, by the Russian government, may have a different "unwilling or unable" reaction, than would an attack in Colombia.

Additionally, any response in self-defense would need to be limited by the principles of necessity and proportionality.[63] For any self-defense response the U.S. would need to exhaust all diplomatic means and have a belief that there is "no reasonable prospect of stopping the [] attack."[64] This could be evidenced by a pattern of behavior, or lack of diplomatic response by the states in which the embassies are located.[65] As mentioned above, the U.S. (as evidenced by the *Libya Raid*) has a more expansive view of the immediacy, and in this case, where the attacks vary in both geographic location and timeframe, it is possible that the U.S. could claim that the immediacy of an attack has a more extended timeline, but it is likely such a claim would see the same backlash as the *Libya Raid* did.[66] A proportional response could involve destroying the method of attack (i.e., the RF Weapons themselves, but regardless of the response), but it would need to consider the harm suffered by the enemy forces in relation to the harm caused.[67]

However, international law *lex lata* would produce a different outcome.

2. Use of Force Under International Law. Under international law *lex lata* an attack must amount to an "armed attack" under Article 51 of the U.N. Charter before a use of force in self-defense is legally justified.[68] As defined in the *Nicaragua* case, the scope of an "armed attack" is narrower than that of the U.S. view.[69] An RF attack would have to be a "grave" form of force, and it must have sufficient "scale and effects" to justify a use of force in self-defense.[70] This fact dependent inquiry likely

---

suggested a test that would apply additional legitimacy to the contested *unwilling and unable* doctrine, there is still no formal test. *See e.g., id.* Additionally, this is a highly contested area of the use of force doctrine in international law, and states disagree on whether this is a valid method of invoking force in self-defense. Elena Chacko and Ashley Deeks, *Which States Support the 'Unwilling and Unable' Test?*, LAWFARE (Oct. 10, 2016, 1:55 PM), https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test.

[63] *See infra* Section I.

[64] DOD LAW OF WAR MANUAL, *supra* note 24, ¶ 1.11.1.3.

[65] *Id.*

[66] *See infra* footnotes 36–37 and accompanying text.

[67] DOD LAW OF WAR MANUAL, *supra* note 24, ¶ 3.5.1.

[68] *See* infra Section I.

[69] *Id.*

[70] DOD LAW OF WAR MANUAL, *supra* note 24, ¶ 1.11.5.2; *see* Harold H. Koh, 'International Law in Cyberspace' (2012) 54 HARVARD INT'L L. J. ONLINE 1, 7 ("[T]he United States has for a long time taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."); *c.f.* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).

provides that a hypothetical RF attack, such as the ones in the "Havana Syndrome" would probably not amount to an armed attack under Article 51 of the U.N. Charter. The reasons for this are as follows.

It is necessary to note that "armed" (in "armed attack") under Article 51, cannot be equated to "force" under Article 2(4). As provided in the *Nicaragua* case, the supplying of weapons and logistical support may be a use of force, but it is not a "grave form[] of the use of force" as is required by the term "armed attack."[71] There is no bright-line test for what constitutes a "grave" use of force, but in the *Oil Platforms* case, where the U.S. took military action against Iran, a U.S. naval vessel was struck by a mine that injured ten sailors and damaged the ship, the court found that the attacks on the U.S. and Kuwaiti ships were not grace enough to be deemed "armed attacks."[72]

In the case at hand, it follows that a RF weapon, with effects like those in the "Havana Syndrome"—that is, brain damage—would not amount to a "grave" use of force equivalent to that of an "armed attack" under Article 51. It would take significant evidence of more of these attacks, likely with more harm to U.S. military or civilians, for it to reach the level of a "grave" use of force. This is supported by the statement by the ICJ in the *Nicaragua* case that "armed attack" includes:

> not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein".

Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment (Merits) [1986] ICJ Rep. 14, ¶ 195 (quoting the U.N. General Assembly's 1974 Definition of Aggression). Some argue that an issue with this approach, and part of the reason for the U.S.'s lower standard, is that State's would have to wait until attacks reached a certain "gravity" before responding with proportional force, thus meaning that the proportional self-defense use of force would be greater than it would be with a lower threshold, thus exacerbating the chance for a "full-scale military conflict."[73]

The counterargument to the above opinion, is that State's may still use countermeasures, where a use of force is not justified.[74] This suggests

---

[71] *Nicaragua*, ¶ 191.

[72] *See* William H. Taft, Self-Defense and the *Oil Platforms* Decision, 29 YALE J. OF INT'L L. 295, 296–98 (2004) (noting that a Kuwaiti ship was also attacked, leading to the *Oil Platforms* cases).

[73] *Id.* at 301.

[74] *See* Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, 4th INT'L CONF. ON CYBER CONFLICT 284, 284 (2012),

that a proper response from the U.S. to a "Havana Syndrome" weapon could be diplomatic measures, economic sanctions, or countermeasures. Countermeasures are described by the U.N. as those that "would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[75] However, considering the nuances of the threshold of force, states would have to ensure that their counter-measure response, fell below the level of force under Article 2(4).[76]

III. IMPLICATIONS UNDER A CHANGING USE OF FORCE FRAMEWORK

This Paper will use the emerging use of force framework for cyberwarfare to analyze whether a potential RF weapon could trigger grounds for the U.S. to use force in self-defense under Article 51 of the U.N. Charter. While there has been a plethora of legal scholarship on the use of force framework and cyberwarfare, states generally seem to concede that while some cyber operations constitute a use of force, it is difficult to identify the specific criteria in making those determinations beforehand.[77] This section will use the framework developed by Michael N. Schmitt, the "Schmitt Analysis," to test how these factors would work in a separate instance.[78]

---

https://ccdcoe.org/uploads/2012/01/5_2_Schmitt_AttackAsATermOfArt.pdf ("The jus ad bellum seeks to maintain peaceful relations within the community of nations by setting strict criteria as to when States may move beyond non-forceful measures such as diplomacy, economic sanctions and counter-measures.").

[75] *Id.* (citing Draft Articles on Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of its 53rd sess., UNGAOR, 56th sess., sup. No. 10 (A/56/10), ch. IV.E.1, at p. 128, available at http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf). Note, that countermeasures would only be available to in response to internationally wrongful acts, so if a state concluded that the "Havana Syndrome" attacks were not internationally wrongful, or if they could not properly attribute the attacks, then countermeasures would not be available. *See* Michael N. Schmitt, *Terminological Precision and International Cyber Law*, LIEBER INSTITUTE: ARTICLES OF WAR (Jul. 29, 2021), https://lieber.westpoint.edu/terminological-precision-international-cyber-law ("Countermeasures are only available in response to cyber operations that constitute internationally wrongful acts; thus, they are unavailable as a response to non-State actor cyber operations that are not attributable to a State.").

[76] Note, that Judge Simma in the *Oil Platforms* case argued that countermeasures would involve force when in response to an act of force that falls below the level of armed attack. Oil Platforms (Islamic Republic of Iran v. U.S.), 2003 I.C.J. 161, ¶¶12–13 (Nov. 6) (separate opinion of Judge Simma). The author does not agree with Judge Simma's contention.

[77] Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, 67 JOINT FORCE QUARTERLY 40, 40 (2012), *available at* https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.

[78] *Id.* at 41; *see generally* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,* COLUMBIA J. OF

Schmitt's suggested framework, developed in 1999, has several factors of consideration: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[79] While this section will admittedly be working in hypotheticals—in both the RF weapon and international law *lex ferenda*—the purpose of it is to explore what the implications of a suggested *new* use of force framework, that would be workable for cyberwarfare, would be in other instances. This is especially important as peacetime uses of force, or near uses of force, are more and more the norm is for adversaries and points of competition to conduct hostile activities in the "gray zone."[80]

The "gray zone" is the operational space below the threshold of war, or between peace and war.[81] State's like China and Russia have been operating here for years, posing difficult legal, political, and tactical questions for other states.[82] An RF weapon with effects such as the Havana Syndrome poses a legal and political question that is similarly vague and difficult to answer. Therefore, using the well-developed cyberwarfare *lex ferenda*, this Paper will try to shed light on how a state could analyze whether the "Havana Syndrome" attacks amount to a use of force.

Schmitt's approach uses a factor-based analysis to bridge the gap between the permissible and impermissible uses of force; that is, the more a like a cyber-attack is to armed force, the more likely states are to brand it a use of force.[83] Though the physical brain damage to the injured U.S. citizens suggests that this was a use of force, there is still value in looking beyond to see the *lex ferenda* cyber framework transposed to a different topic.

1. Severity. "Cyber operations that threaten physical harm more closely approximate an armed attack. Relevant factors in the analysis include scope, duration, and intensity."[84] Under this factor, the "Havana

---

TRANSNATIONAL L. 37 (1999) 885 (describing Schmitt's normative framework and suggested analysis for cyber operations).

[79] *Id.*

[80] *See e.g.*, Matt Peterson, *Competition and Decision in the Gray Zone: A New National Security Strategy*, STRATEGY BRIDGE (Apr. 20, 2021), https://thestrategybridge.org/the-bridge/2021/4/20/competition-and-decision-in-the-gray-zone-a-new-national-security-strategy (citing LYLE J. MORRIS ET AL., GAINING COMPETITIVE ADVANTAGE IN THE GRAY ZONE 8 (RAND Corporation, 2019) (noting China's maritime activity in the South China Sea); LYLE J. MORRIS ET AL., GAINING COMPETITIVE ADVANTAGE IN THE GRAY ZONE 17–22 (RAND Corporation, 2019) (noting that Russia has used war by proxy with their transfer of military equipment in Georgia, military intimidation in Ukraine and Georgia, information operations in the EU and NATO countries, cyberattacks in Ukraine and Estonia, and other political and economic coercion methods).

[81] Matt Peterson, *Competition and Decision in the Gray Zone: A New National Security Strategy*, STRATEGY BRIDGE (Apr. 20, 2021), https://thestrategybridge.org/the-bridge/2021/4/20/competition-and-decision-in-the-gray-zone-a-new-national-security-strategy (citing LYLE J. MORRIS ET AL., GAINING COMPETITIVE ADVANTAGE IN THE GRAY ZONE 8 (RAND Corporation, 2019).

[82] *See supra* note 80.

[83] Foltz, *supra* note 77, at 42–43.

[84] *Id.* at 43.

Syndrome" attacks constitute a use of force *per se* because they caused physical injury. The duration of the consequences to the individual are life-long, as proven by the brain damage catalogued in the NASEM Report, but it is unclear what impact this has on the U.S. political agenda or programs writ large.[85] It is also important to note the discrete, limited nature of these attacks.

2. Immediacy. "Consequences that manifest quickly without time to mitigate harmful
effects or seek peaceful accommodation are more likely to be viewed as a use of force."[86] Immediacy may seem difficult in this case due to the varied nature of symptom onset, however, viewing these attacks as a series of attacks, all of the same nature, would seem to indicate that this factor would pay some role in the analysis. That is, the U.S. could implement countermeasure against the holder/state with the RF weapons, with the expectation that these attacks could come at any time.

3. Directness. "The more direct the causal connection between the cyber operation and the consequences, the more likely states will deem it to be a use of force."[87] This is where the hypothetical nature of the RF weapon causes issue. However, if we assume that there has been concrete evidence of an RF weapon, which causes these symptoms, it would be a clear indication that there is a direct causal nexus between the RF weapon and the injured civilians.

4. Invasiveness. "The more a cyber operation impairs the territorial integrity or sovereignty of a state, the more likely it will be viewed as a use of force."[88] This would be a point of emphasis in the analysis of whether the attacks were a use of force. There is clearly no intrusion on the territory of the United States, and it does not seem to directly violate U.S. sovereignty, but foreign states have the right to protect their nationals abroad.[89] That indicates that this factor is not exhaustive in the use of force inquiry but is still indicative of the invasiveness of such an attack.

5. Measurability. "States are more likely to view a cyber operation as a use of force if the consequences are easily identifiable and objectively quantifiable."[90] There are clearly identifiable and quantifiable injuries in this instance.[91]

---

[85] *See infra* notes 8–15 and accompanying text.
[86] Foltz, *supra* note 77, at 43.
[87] *Id.*
[88] *Id.*
[89] Prior to the U.N. Charter and World War I there was generally "widespread acceptance of the right of a state to protect its nationals abroad." Andrew W.R. Thomson, Doctrine of the Protection of Nationals Abroad: Rise of the Non-Combatant Evacuation Operation, 11 WASH. UNIV. GLOB. STUD. L. REV. 627, 630 (2012). Often the protection of nationals abroad is allowed where the protection does not constitute a use of force under Article 2(4), *or* where a use of force is a "legitimate exercise" of the right of self-defense. *Id.* at 634.
[90] Foltz, *supra* note 77, at 43.
[91] *See infra* notes 8–15 and accompanying text.

6. Presumptive Legitimacy. "To the extent certain activities are legitimate outside of the cyber context, they remain so in the cyber domain, for example, espionage, psychological operations, and propaganda."[92] This factor inquires whether there is presumptive *legal* legitimacy for the State's action.[93] For example, in the Stuxnet cyber-attack against Iran's nuclear materials facilities, there is no "customary acceptance" for the damaging of Iran's nuclear facilities, despite the fact that Iran had been violating multiple U.N. Security Council Resolutions in the operation of its centrifuges.[94] In the immediate case, there is no presumptive legitimacy, or lawful action under the U.N. Charter, either in self-defense (Article 51), or the use of force (Article 2(4)) that would make an RF attack on U.S. diplomats and intelligence personal stationed at U.S. embassies lawful.

7. Responsibility. "The closer the nexus between the cyber operation and a state, the more likely it will be characterized as a use of force."[95] Though no state has claimed responsibility, and none has been attributed (also recognizing that a concrete weapon has not been identified either), the fact that these are targeted against U.S. diplomats and intelligence personnel at U.S. embassies in Cuba, China, Russia, Poland, Taiwan, Serbia, and Colombia, which are all areas of tension between the United States' main points of competition, Russia and China, indicate some level of state involvement.[96]

In summary, the Schmitt Analysis suggests—if not confirms—that this would be a use of force under international law. As recognized by other authors, and Schmitt himself, this suggests that the characterization of an act would turn on the severity factor. This does not necessarily indicate any significant difference in the Schmitt Analysis and the current Article 2(4) use of force framework. In analyzing a hypothetical, and slightly ambiguous, RF weapon attack, against the Article 2(4) use of force framework, this seven-factor analysis actually suggests that the use of force framework under the U.N. Charter is also relatively weak as a constraint on other types of attacks that fall outside of the traditional kinetic military action.[97] Like with cyber operations, as states operate increasingly in the "gray zone," below traditional thresholds of attack, the analysis grows

---

[92] Foltz, *supra* note 77, at 43.
[93] *Id.* at 45.
[94] *Id.* (citing UN Security Council Resolutions 1737 (2006), 1747 (2007), 1803 (2008), and 1929 (2010)).
[95] Foltz, *supra* note 77, at 43.
[96] *Infra* note 8 and accompanying text.
[97] *c.f.* Foltz, *supra* note 77, at 46–47 (finding that the "contemporary interpretations of Article 2(4) reflect the distribution of traditional military instruments of power" current cyber capability do not "mirror the traditional distribution" and that state's will likely need to consider a myriad of additional considerations in determining whether an attack is a use of force, and how to respond appropriately).

increasing complex and includes other various legal, political, economic, and technical factors.[98]

CONCLUSION

As state's operate increasingly in the gray zone, and under traditional thresholds of force, experts struggle with how to adapt, or whether to adapt, existing regulations to constantly advancing technologies. After analyzing the existing law on the use of force to an RF weapon, this Paper concludes with the following:

This analysis highlights the persistent issue of applying modern technology to the Article 2(4) use of force framework. Emerging state practice in the application of Article 2(4) to cyber operations belies an overall shift away from a strict adherence to Article 2(4) towards an approach with a greater focus on consequences. As norms emerge in state's use of force calculations, the trend seems to suggest a more nuanced, larger scope for what could be considered force under international law.

The overall effects of such a shift mirror the nuanced legal and operational landscape today—with a shift from traditional warfare to the major international players operating via lawfare and gray zone operations. This analysis suggests that the evolving norms are unlikely to be limited by the narrow construction of Article 2(4), and as these norms evolve, the emerging question will be whether states will keep allowing these norms to develop organically, or if international consensus will develop so that that a new framework is defined. Currently, there's no indication that states are looking to define a new framework, so the next few decades will be instrumental in how use of force evaluations develop in the modern world.

[98] *See id.* at 46 ("Such additional considerations may include relative cyber strengths and vulnerabilities; strategic risks and opportunities; scope of potential consequences; ability to control escalation; effectiveness of cyber deterrence; potential reactions by adversaries, allies, and international organizations; domestic politics; state declaratory policies; emerging state practice (including state inaction); attribution problems; and other legal, political, and technical constraints.").