MILITARY LAW REVIEW

Volume 231 **Issue 4**

BELLIGERENT TRANSMISSIONS THROUGH NEUTRAL CYBERINFRASTRUCTURE: WHY THE ANARCHY OF CYBERSPACE DEMANDS SPECIAL TREATMENT UNDER THE LAW OF NEUTRALITY

LIEUTENANT COLONEL AMANDA L. LYTHGOE*

> *The Internet is the first thing that humanity has built that humanity doesn't understand, and the largest experiment in anarchy that we've ever had.*[1]

I. Introduction: Belligerent Cyber Transmissions and the Law of Neutrality

In 2009, cyber attackers released a malicious computer code into cyberspace, hopeful that it would make its way to its target: the fortified, digital heart of an Iranian nuclear plant.[2] Unable to control its route,

* Judge Advocate, United States Marine Corps. Previously assigned as Student, 68th Judge Advocate Officer Graduate Course, The Judge Advocate General's School, United States Army, Charlottesville, Virginia. J.D. and LL.M. in International and Comparative Law, 2015, Cornell University Law School; B.S., 2006, United States Naval Academy. Currently assigned as the Special Assistant to the Counsel for the Commandant, United States Marine Corps. Past assignments include Deputy Staff Judge Advocate, Joint Special Operations Command, Fort Liberty, North Carolina, 2020–2023; Regional Victims' Legal Counsel, Legal Services Support Section-West, Camp Pendleton, California, 2017–2019; Defense Counsel, Legal Services Support Section-West, Camp Pendleton, California, 2015–2017; Officer in Charge, Cultural Support Team Program, Combined Joint Special Operations Forces-Afghanistan, Bagram Airfield, Afghanistan, 2012; Intelligence Officer, Current Operations Directorate, Headquarters United States Special Operations Command, MacDill Air Force Base, Florida, 2010–2012; Intelligence Officer, Marine Unmanned Aerial Vehicle Squadron 2, Marine Corps Air Station Cherry Point, North Carolina, 2007–2010. Member of the bars of California, Massachusetts, and New York. This article was submitted in partial completion of the Master of Laws requirements of the 68th Judge Advocate Officer Graduate Course. Many thanks to Captains Bradan Thomas, Ellis Cortez, and Lyndsey "Zee" Andray and Lieutenant Colonels Matt Aiesi and Ryan Boeka for their tremendous assistance in completing this article.

[1] Jerome Taylor, *Google Chief: My Fears for Generation Facebook*, INDEP. (Oct. 22, 2011, 10:44 PM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-chief-my-fears-generation-facebook-2055390.html (quoting Eric Schmidt).

[2] Zachary P. Augustine, *Cyber Neutrality: A Textual Analysis of Traditional Jus in Bello Neutrality Rules Through a Purpose-Based Lens*, 71 A.F. L. REV. 69, 75 (2013).

attackers remotely monitored the code's path as it infected new machines.[3] The worm—later dubbed "Stuxnet"—was sophisticated malware initially designed to spread through local area networks when a user connected an infected device.[4] As the worm traveled through cyberspace, it installed malware on every device it burrowed through,[5] remaining dormant unless the infected computer ran the specific software used by the systems at the Iranian nuclear facility.[6] Once it detected the desired software, the malware sent commands to the nuclear plant's centrifuges, causing them to spin at irregular and dangerous speeds, resulting in physical damage to the system.[7] Although tailored to the unique features of the nuclear plant's isolated systems, the code's embedded propagation mechanisms ultimately failed to prevent Stuxnet's spread beyond its intended target.[8] Instead, Stuxnet proliferated uncontrollably as infected devices were unpredictably connected to other networks, and the attackers modified the code to behave more aggressively.[9] Stuxnet eventually infected at least 100,000 computers located in over 150 countries.[10]

Stuxnet's spread illustrates the anarchy of the domain through which it transited: an interdependent network of devices, information, and

---

[3] KIM ZETTER, COUNTDOWN TO ZERO DAY 27–28 (Broadway Books, 2014) (explaining that every time Stuxnet infected a new system, it transmitted data related to the machine and networks through the internet to servers in Denmark and Malaysia that functioned as command centers for the attack).

[4] *Id.* at 92–93 (noting that while most malware uses the internet to spread, Stuxnet relied on human carriers to transport the code between local networks); Augustine, *supra* note 2, at 101–02; *see* George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1094–99 (2000) (explaining that when information is sent through the internet, data is separated into small packets of data that may be routed through various networks in a random manner).

[5] Augustine, *supra* note 2, at 102 (describing that Stuxnet spread through 155 different countries through countless networks and was facilitated by automatic installation processes).

[6] *Id.*

[7] *Id.* at 100–02 (comparing the effects of the Stuxnet worm to those of a "damage-inflicting conventional weapon" and explaining the attack's goal to force the plant's centrifuges into failure).

[8] ZETTER, *supra* note 3, at 96 fn 14 (Broadway Books, 2014) ("The fact that Stuxnet spread via USB flash drives and local networks instead of through the internet should have made it less likely to spread so widely, yet it did. This probably occurred because some of the companies infected in Iran had satellite offices outside Iran or used contractors who had clients in other countries and spread the infection each time they connected an infected laptop to another client's network or used an infected USB flash drive at multiple sites.").

[9] Nate Anderson, *Confirmed: US and Israel Created Stuxnet, Lost Control of it* ARSTECHNICA (June 1, 2012, 6:00 AM), https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/.

[10] ZETTER, *supra* note 3, at 97; Augustine, *supra* note 2, at 102.

infrastructures, including private and public virtual networks, subject to varying degrees of government regulation and characterized by automated components designed to promote efficiency and speed. Stuxnet likely involved state sponsorship, but experts disagree on whether its employment amounted to the use of force under international law.[11] Nevertheless, the worm's uncontrolled journey through cyberinfrastructure across multiple state borders illustrates an extraordinary challenge in regulating cyberspace activities: determining when the presence of unwelcome transmissions violates state sovereignty.[12]

Cyber architecture morphs daily as countless devices connect to the internet for the first time, spawning fresh pathways and associated vulnerabilities.[13] User demand for speedy access to virtual amenities generates new platforms and connections between network providers.[14] Automated routing components, designed to expeditiously direct internet traffic around congested networks, may send data through unexpected pathways—including through neighboring states—without the knowledge of the end users or the owners of cyberinfrastructure.[15] Some of these users are hostile actors, venturing boldly into this new domain

---

[11] Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html; *see* Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, 67 JOINT FORCES Q., 4th Quarter 2012, at 40.

[12] Eric T. Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L.J. 815, 824 (2012) (posing the question as to whether packets of information traversing cyberspace can violate state sovereignty); *see* Symposium, *Computer Network Attack and International Law*, 76 INT'L L. STUD. 1 app. at 463–65 (2002).

[13] *See* Convention on Cybercrime, pmbl., Nov. 23, 2001, T.I.A.S. No. 13174, 2296 U.N.T.S. 167 (discussing the "profound changes brought about by the digitali[z]ation, convergence and continuing globali[z]ation of computer networks").

[14] *See generally* NAT'L PROT. & PROGRAMS DIRECTORATE, U.S. DEP'T OF HOMELAND SEC., THE FUTURE OF SMART CITIES: CYBER-PHYSICAL INFRASTRUCTURE RISK 2 (2015) ("As technology pervades into our everyday lives, once simple devices have become smarter and more interconnected to the world around us. . . . Removing the cyber-physical barriers in an urban environment presents a host of opportunities for increased efficiencies and greater convenience, but the greater connectivity also expands the potential attack surface for malicious actors.").

[15] Doug Madory, *Large European Routing Leak Sends Traffic Through China Telecom*, ASIA PACIFIC NETWORK INFORMATION CENTRE (APNIC) (June 7, 2019), https://blog.apnic.net/2019/06/07/large-european-routing-leak-sends-traffic-through-china-telecom (observing that internet traffic from Switzerland, Holland, and France was unexpectedly routed through China Telecom's network for several hours earlier in the day).

with increasing frequency.[16] The Stuxnet incident is not anomalous; many states have been victims of cyber attacks,[17] yet the state of the law remains uncertain.[18]

Although the Stuxnet incident occurred outside the context of an international armed conflict, it illustrates the difficulty in controlling—and even predicting—how cyber transmissions travel to their destinations and what they may affect along the way. Belligerent cyberspace operations during an armed conflict may unexpectedly traverse through uninvolved states due to the internet's design: boundary-less, primarily privatized, and with an ever-evolving, fluid architecture. It does not neatly align with state borders or possess static terrain features that promote the application of traditional notions of sovereignty.[19] Inextricably intertwined with sovereignty, neutrality is a fundamental concept in international law denoting a special status during times of armed conflict.[20] The international community must urgently determine the boundaries of state territorial and jurisdictional sovereignty within cyberspace to proscribe belligerent conduct involving neutral cyberinfrastructure. Belligerents must know what conduct is prohibited so they may comply with international law. If transmitting malicious code through neutral cyberinfrastructure violates the law of neutrality, the responsible

---

[16] HARRIET MOYNIHAN, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION 1 (2019) (estimating that over twenty-two states are known to have sponsored cyber operations against other states and that "the number and scale of these operations is growing"); *see generally* Ellen Nakashima, *Pentagon to Boost Cybersecurity Force*, WASH. POST (Jan. 27, 2013), https://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

[17] *MOYNIHAN, supra* note 16 (listing a number of attacks on European companies and governments attributable to China, Iran, and Russia, costing billions of dollars in economic losses).

[18] *See* GEORGE LUCAS, ETHICS AND CYBER WARFARE: THE QUEST FOR RESPONSIBLE SECURITY IN THE AGE OF DIGITAL WARFARE 64–78, 113–19 (Oxford Univ. Press, 2017) (summarizing the international community's failure to achieve consensus in the Tallinn Manual regarding legal approaches to cyberspace and describing the emergent, but still developing, legal norms following cyber incidents in Estonia, Syria, Georgia, and Iran).

[19] William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GA. J. INT'L & COMP. L. 247, 253–54 (2012) (describing the structure of the internet as a "network of networks," both privatized and government, which are connected by wired and wireless communication links, wherein host computers communicate using protocol language to format data for transfer through routers to other connections that gives rise to "essentially anonymous global access").

[20] *See generally* Jensen, *supra* note 12, at 816–17.

belligerent has broken the rules, and the aggrieved neutral state may be obligated to respond.[21]

To prevent confusion over what actions may trigger such undesirable results, a legal framework that applies the law of neutrality to cyberspace must be established. However, the anarchic international legal system displays no consensus on whether transmitting a belligerent's malicious cyber code through neutral cyberinfrastructure is permissible under the law of neutrality. While some experts and a few states have addressed this issue, consensus is far beyond reach.[22]

Relying on its adaptive features, an exception related to neutral communications systems, and its primary purpose, this article posits that the law of neutrality is not violated when malicious code is transmitted through neutral cyberinfrastructure. Using the Hague Conventions of 1899 and 1907 as guides, Part III of this article summarizes the rights and obligations of belligerents and neutral states and identifies the fundamental purposes of the law of neutrality. Part IV evaluates the international treatment of this issue in the *Tallinn Manual 2.0* and explores divergent views therein. Part V exposes the flaws in the *Tallinn Manual 2.0*'s majority opinion, including its failure to acknowledge traditional flexibility in the law of neutrality and its untenable practical implications that undermine the law of neutrality's essential purposes. Part VI explains that transmitting any malicious code, including cyber weapons, through public-neutral cyberinfrastructure should not violate the law of neutrality and urges the United States to lead the international community in adopting this position.

---

[21] OFF. OF GEN. COUNSEL, U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 15.4.2 (2016) [hereinafter LAW OF WAR MANUAL].

[22] *See* U.N. Secretary-General*, Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266,* U.N. GAOR, 76TH SESS., AGENDA ITEM 96, U.N. DOC. A/76/136 (JULY 13, 2021) (stating that "[t]he precise threshold of what constitute [sic] a cyber operations in violation of sovereignty is not settled in international law, and will depend on a case-by-case assessment."). *See also* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0] (constituting a comprehensive attempt by international experts to apply international law governing cyberspace to both war and peacetime legal regimes but constituting only the personal views of the authors and not necessisarily customary international law).

II. Definitions and Presumptions

Before proceeding to the primary discussion of the law of neutrality, it is vital to define its parameters. This article presupposes the context of an international armed conflict between states. It does not address the challenges of attribution in cyberspace and assumes that all cyber transmissions are attributable to a belligerent party to the international armed conflict. There will be no discussion as to whether particular activities in cyberspace qualify as armed attacks or otherwise meet the threshold requirements for the use of force under international law.[23] Legal theories that justify or limit a state's response to a violation of the law of neutrality will not be investigated; the word "response" will encompass all actions that belligerent and neutral states may take in accordance with *jus ad bellum* and *jus in bello* principles, including the use of force or employment of countermeasures.[24]

Whether malicious cyber code is itself a "munition," "communication," or "information" is widely debated and central to the question of whether a particular belligerent transmission violates a neutral state's sovereignty.[25] Such discussion is irrelevant here, as this article proposes that transmitting any malicious code, even code that produces effects tantamount to those of an armed attack, should not violate the law of neutrality when transmitted through neutral cyberinfrastructure on the way to its target. The term "malicious cyber code" refers to *all* types of belligerent transmissions in cyberspace, including transmissions of cyber weapons used in qualifying armed attacks, cyber communications that effectuate command and control, and cyber information and intelligence operations falling below the threshold of the use of force. Finally, "neutral cyberinfrastructure" includes all of a neutral state's sovereign territory and platforms, whether owned by the government or private entities.[26]

---

[23] U.N. Charter art. 2, ¶¶ 3–4; LAW OF WAR MANUAL, *supra* note 21, § 1.11.

[24] TALLINN MANUAL 2.0, *supra* note 22, at 554–55; LAW OF WAR MANUAL, *supra* note 21, §§ 1.11, 3.4.

[25] The problem of categorizing cyber transmissions relates to whether data itself is an object. The experts who authored the *Tallinn Manual* were unable to arrive at a consensus on this issue due to data's intangibility. TALLINN MANUAL 2.0, *supra* note 22, at 437; *see* Tim McCormack, *International Humanitarian Law and the Targeting of Data*, 94 INT'L L. STUD. 222, 223 (2018) (describing digital data as a "complex succession of 1s and 0s" that presents challenges to the traditional notions of the word "object").

[26] TALLINN MANUAL 2.0, *supra* note 22, at 553.

III. The Law of Neutrality

A neutral state is one that is not a party to an international armed conflict.[27] The rules relating to neutral states' protections, rights, and obligations are considered customary international law and enshrined in the Hague Conventions of 1899 and 1907.[28] Save for a few recognized exceptions, the law of neutrality compels belligerent states to respect the sovereignty of neutral states. It prohibits entry into and operations within a neutral state's territory, waters, or airspace "by armed forces or instrumentalities of war."[29]

The law of neutrality serves several purposes. It first seeks to shield the territory and persons of neutral states from the harmful effects of hostilities.[30] Second, it strives to prevent the escalation and spread of an armed conflict by prohibiting the involvement of neutral powers in the hostilities to benefit one belligerent over another.[31] The protection of international commerce is another crucial goal.[32] To accomplish these aims, the law of neutrality proscribes the conduct of belligerents and neutral states in all battlefield domains.[33] Most fundamentally, belligerents must respect the sovereignty of neutral states and may not exercise belligerent rights within neutral territory.[34] Neutral states must treat belligerents equally and avoid assisting one party to the other's

---

[27] LAW OF WAR MANUAL, *supra* note 21, § 15.1.2.2. The law of neutrality applies only during times of international armed conflict. *See generally id.* § 15.2 (discussing the application of the law of neutrality in armed conflicts).

[28] Hague Convention (II) with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803; Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277; Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310 [hereinafter Hague V]; Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415 [hereinafter Hague XIII].

[29] LAW OF WAR MANUAL, *supra* note 21, § 15.3.1.1.

[30] Hague V, *supra* note 28, art. 1 ("The territory of neutral Powers is inviolable."); TALLINN MANUAL 2.0, *supra* note 22, at 553; *see also* LAW OF WAR MANUAL, *supra* note 21, § 15.1.3 (describing the purpose of the law of neutrality).

[31] TALLINN MANUAL 2.0, *supra* note 22, at 553; *see* LAW OF WAR MANUAL, *supra* note 21, § 15.1.3.

[32] TALLINN MANUAL 2.0, *supra* note 22, at 553; LAW OF WAR MANUAL, *supra* note 21, § 15.1.3; OFF. OF THE CHIEF OF NAVAL OPERATIONS, DEP'T OF THE NAVY, NWP 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS para. 7.1 (2017) [hereinafter COMMANDER'S HANDBOOK].

[33] LAW OF WAR MANUAL, *supra* note 21, § 15.3.

[34] Hague V, *supra* note 28, art. 1.

detriment.[35] The objective is to minimize the involvement of third parties and thus contain the conflict, preventing its escalation and spread.[36]

A. The Hague Conventions: The Foundation for the Law of Neutrality

The law of neutrality is rooted in the Hague Conventions of 1899 and 1907, which encompass several conventions dedicated to regulating the behavior of states during times of armed conflict. Hague Conventions V and XIII—which will be referred to as Hauge V and Hauge XIII for the purposes of this article—are the most important in defining the law of neutrality: they articulate specific precautions that neutral states must take to avoid assisting belligerent parties and the measures belligerent parties must take to respect neutral states' territories and citizens.[37] Hague V deals with the rules for neutrality during conflicts on land, and Hague XIII addresses conflict at sea.[38] The law of neutrality adapts to each domain's unique characteristics through subtle modifications that effectively advance its purposes: protecting neutral state sovereignty and persons, preventing conflict escalation, and shielding commerce from harmful interference.[39] Although the Hague Conventions are well over a century old, they constitute current customary international law.[40] At the same time, most attempts to apply the law of neutrality to cyberspace begin with relevant provisions of the Hague Conventions; states and international law experts do not agree on how to adapt them to cyberspace.[41] In particular, experts diverge on whether belligerent transmission of malicious code through neutral cyber infrastructure violates the law of neutrality.

1. Rights and Obligations of Belligerents on Land and at Sea

The Hague Conventions articulate the rights and obligations of belligerents and neutrals in the distinct domains of land and sea. Hague V addresses land warfare and requires belligerents to respect the inviolability of neutral territory, explicitly prohibiting the exercise of belligerent rights

---

[35] *Id.* art. 9.
[36] LAW OF WAR MANUAL, *supra* note 21, § 15.1.3.
[37] *See* Hague V, *supra* note 28; *see also* Hague XIII, *supra* note 28.
[38] *Id.*
[39] LAW OF WAR MANUAL, *supra* note 21, § 15.1.3.
[40] U.S. DEP'T OF STATE, TREATIES IN FORCE: A LIST OF "TREATIES AND OTHER INTERNATIONAL AGREEMENTS OF THE UNITED STATES IN FORCE ON JANUARY 1, 2020, at 557.
[41] *See generally* TALLINN MANUAL 2.0, *supra* note 22.

when it violates the territorial sovereignty of a neutral state.[42] This includes the transporting belligerent forces, supplies, or munitions over a neutral state's land.[43] A belligerent may not construct new communications infrastructure on neutral territory or use pre-existing communications infrastructure to communicate with its forces.[44] An exception exists for belligerent use of pre-existing neutral communications infrastructure, which is also open to the public.[45] Finally, belligerent parties may not recruit or raise troops from neutral territories.[46] These prohibitions address belligerent actions involving deliberate, knowing intrusions of neutral sovereignty as consequences of a military operation that are also likely to contribute measurably and directly to the belligerent's success.

Hague XIII is consistent with Hague V, applies the same principles to the seas, and helps interpret the intent underlying Hague V's provisions.[47] Fundamentally, belligerents may not use a neutral state's sovereign waters to advance its wartime objectives. For example, a belligerent may not arm its vessels in a neutral port or waters or use them as a base for naval operations.[48] Like Hague V, Hague XIII prohibits the erection of communications infrastructure in neutral ports and waters "for the purpose of communicating with the belligerent forces on land or sea."[49] However, unlike Hague V's prohibition on the movement of belligerent convoys across a neutral state's land, the mere passage of a belligerent's vessels through neutral waters does not violate the law of neutrality.[50] In fact, up to three belligerent vessels may dock in a neutral port at one time, so long as they do not remain longer than twenty-four hours or engage in prohibited activities.[51] This critical distinction, wherein belligerent vessels may transit neutral waters and dock in neutral ports under certain conditions while similar acts are *per se* prohibited on land, provides one example wherein the unique characteristics of a battlefield domain may

---

[42] Hague V, *supra* note 28, art. 1.
[43] *Id.* art. 2. The article prohibits the transit of "troops or convoys of either munitions of war or supplies across the territory of a neutral Power." *Id.*
[44] *Id.* art. 3. Belligerents may not build "a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea" or make use of "an installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes." *Id.*
[45] *Id.*
[46] *Id.* art. 4. Belligerents may not form "[c]orps of combatants" or open "recruiting agencies . . . on the territory of a neutral Power to assist the belligerents." *Id.*
[47] Augustine, *supra* note 2.
[48] Hague XIII, *supra* note 28, art. 5.
[49] *Id.*
[50] *Id.* art. 10.
[51] *Id.* arts. 12–20.

necessitate a more permissive interpretation of the law of neutrality. International law regularly employs exceptions and modifications to uphold key principles across domains, which is critical to correctly applying the law of neutrality in cyberspace.

2. Rights and Obligations of Neutral States on Land and at Sea

Article 5 of Hague V articulates that the most fundamental duty of neutral states during armed conflict on land is, in short, to stop belligerent parties from engaging in any of the prohibited wartime activities enumerated in Articles 2–4.[52] Neutral powers may even use force to fulfill this obligation.[53] One exception to this mandate relates to the use of communications infrastructure. Specifically, neutral states are *not* "called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[54] While they may impose restrictions if they so choose, neutral states must do so impartially and apply the same rules to belligerents on both sides of the conflict.[55] A neutral power is thus not required to prevent belligerents from using its communications infrastructure but may do so at its option so long as restrictive measures are fair. Therefore, a belligerent's mere *use* of neutral communications infrastructure within neutral territory is not a violation of the law.

Pertaining to conflict at sea, Hague XIII stipulates that neutral states may not directly or indirectly supply a belligerent with any war material, including warships and ammunition;[56] however, a neutral state is not required to prevent the export or transit of arms, ammunition, or supplies that could be of use to an army or fleet.[57] As mentioned, the mere passage of belligerent vessels through a neutral state's territorial waters and the docking of belligerent vessels in neutral ports for innocent purposes does not violate the law of neutrality.

In sum, while Hague V and Hague XIII both require neutral states to stop *impermissible* belligerent conduct on their sovereign territory or waters, neutral states are not required to stop *all* belligerent conduct. A belligerent's ability to control its conduct relates to whether the conduct is permissible; when it is permissible, there is no obligation for a neutral state

---

[52] Hague V, *supra* note 28, art. 5.
[53] *Id.*
[54] *Id.* art. 8.
[55] *Id.* art. 9.
[56] Hague XIII, *supra* note 28, art. 6.
[57] *Id.* art. 7.

to act. Further, knowledge of belligerent acts is a prerequisite for a neutral state's response to prohibited conduct.[58] Thus arises an implicit requirement for a neutral state "to monitor, to the best of its ability, its own territory and infrastructure."[59] When it is infeasible for a neutral state to detect belligerent activity, such as that on the seas and over radio waves, the law does not impose a strict requirement to stop belligerent conduct.[60] The Hague Conventions accordingly account for both belligerent and neutral state intent and capabilities in proscribing conduct and imposing obligations.

3. Consequences of a Neutral State's Failure to Comply

The aggrieved belligerent may intervene when a neutral state fails to fulfill its obligations to terminate illegal belligerent action in its territorial seas or on its land.[61] Examples of neutral states' violations of these obligations could range from overtly assisting a belligerent to failing to terminate the belligerent use of sovereign territory. The law of neutrality permits an aggrieved belligerent to remedy such a situation by taking action to end the violation where the neutral state is unwilling or unable to do itself.[62] The aggrieved belligerent may execute a countermeasure that could ordinarily constitute an internationally wrongful act.[63] However, a belligerent's right to respond to a violation of the law of neutrality is limited: countermeasures are authorized only in situations where the violation resulted in a relative military advantage for the enemy.[64] In cases where a violation did not harm the aggrieved belligerent's security interests, the belligerent may not act.[65] Even when the violation negatively affected the belligerent, notification to the neutral state is ordinarily

---

[58] *See generally* Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 19–22 (Apr. 9) (holding that that a neutral state must not allow knowingly the use of its territory for acts contrary to the rights of other states and determining that constructive knowledge is sufficient).
[59] Jensen, *supra* note 12, at 826.
[60] *See* Hague V, *supra* note 28, art. 8.
[61] LAW OF WAR MANUAL, *supra* note 21, § 15.4.2.
[62] LAW OF WAR MANUAL, *supra* note 21; *see also* COMMANDER'S HANDBOOK, *supra* note 32.
[63] Augustine, *supra* note 2, at 81; *see* Jensen, *supra* note 12, at 823 (explaining that belligerent actions in response to a neutral state's failure to maintain its neutrality, whether willing or unwilling, "would most certainly constitute a violation of the neutral state's sovereignty"). *See also* LAW OF WAR MANUAL, *supra* note 21 (stating that armed attacks are appropriate under some circumstances).
[64] Jensen, *supra* note 12, at 823.
[65] *Id.*

required before executing a countermeasure.[66] Finally, the countermeasure taken is subject to scrutiny in accordance with the *jus ad bellum* principles of necessity and proportionality.[67]

IV. Neutrality in Cyberspace

The international community agrees that international humanitarian law generally applies to cyberspace.[68] The International Court of Justice (ICJ) further asserts that the law of neutrality applies to every international armed conflict irrespective of weaponry, declaring that "international law leaves no doubt that the principle of neutrality . . . is applicable . . . to all international armed conflict, whatever type of weapons might be used."[69] While the court did not mention cyber weapons specifically, the opinion confirmed that the international community agrees that the principles of neutrality are universally applicable to every domain.[70]

Despite this consensus, few treaties directly address cyber operations, and state practice has yet to emerge to the extent required to constitute customary international law applicable to the cyber domain.[71] The classified and imperceptible nature of most cyber activities gives states little incentive to express their positions and policies publicly, leading to a dearth of *opinio juris*.[72] Therefore, the consensus that international law generally applies to cyber operations does not extend to *how* it applies. In areas where limited consensus does exist, it does not yet amount to customary international law.[73]

The absence of formal state agreement is only partly due to the infancy of the cyber domain and state reluctance to publish national policies and positions. Direct application of existing international law to the unique aspects of the cyber domain is impractical and results in divergent opinions. The law of neutrality developed from situations where entrance to or exit from a neutral state's territory was a *physical act*.[74] Unlike land, sea, and

---

[66] *Id.*
[67] LAW OF WAR MANUAL, *supra* note 21, § 15.4; COMMANDER'S HANDBOOK, *supra* note 32, para. 7.3.
[68] TALLINN MANUAL 2.0, *supra* note 22, at 553.
[69] The Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 89 (July 8).
[70] *See, e.g.*, Wolff Heintschel von Heinegg, *Neutrality in Cyberspace*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 35, 37–38 (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., 2012).
[71] MOYNIHAN, *supra* note 16, at 1.
[72] *Id.*; *see also* TALLINN MANUAL 2.0, *supra* note 22, at 3.
[73] TALLINN MANUAL 2.0, *supra* note 22, at 3.
[74] *Id.* at 554.

air, the internet is virtual and has no territorial boundaries; cyber transmissions cross national borders at the speed of light, undetected, and on paths determined by autonomous equipment—not by the volition of the sender.[75] Due to how information travels through cyberspace, belligerent cyber transmissions are highly likely to traverse through neutral cyberinfrastructure, potentially violating state sovereignty.[76] International experts disagree on whether transmitting a belligerent's malicious code through neutral cyber infrastructure violates the law of neutrality.[77] Due to the physical structure of networks and the automation of packet routing, the resolution of this disagreement will affect the conduct of all military communications and operations in cyberspace during armed conflict. The *Tallinn Manual 2.0* presents the minority and majority views on this topic, which are based in conflicting interpretations of Articles 2 and 8 of Hague Convention V.[78]

A. The *Tallinn Manual 2.0*: Revealing an International Divide

The *Tallinn Manual 2.0* comprises the most comprehensive effort to address the application of international law to cyberspace during times of armed conflict and peace. It proffers 154 rules governing cyber operations and includes commentary from renowned international law experts.[79] While it does not constitute law, it is the best starting place to evaluate the legality of belligerent transmissions through neutral cyberinfrastructure.[80] Chapter 20 addresses neutrality and reveals consensus on some matters, acknowledging "widespread agreement that [the law of neutrality] applies to cyber operations taken against, or by use of, cyberinfrastructure that is located within the territory of neutral states."[81] This consensus is based on the "well-established principle" prohibiting belligerents from "conducting hostilities within neutral territory."[82]

---

[75] *Id.* (acknowledging that automatic routing of data may mean that "the sender or the owner of the neutral cyber infrastructure cannot necessarily control the route it takes"); Walker, *supra* note 4, at 1096. *See generally* Stahl, *supra* note 19, at 253 ("[R]outers operate by identifying data's destination addresses and transferring that data to another router closer on the network to its destination until it reaches its destination. The system of routers ensures that there are multiple paths data can take to reach its destination, which allows the system to continue to function in the event that communication links or routers are out of service." (citations omitted)).

[76] Jensen, *supra* note 12.

[77] TALLINN MANUAL 2.0, *supra* note 22, at 559.

[78] *Id.* at 555–57.

[79] *Id.* at 2–3.

[80] *Id.*

[81] Heintschel von Heinegg, *supra* note 70, at 35.

[82] TALLINN MANUAL 2.0, *supra* note 22, at 555.

Of the two proffered rules most directly address the meaning of this prohibition in cyberspace, neither presents a definitive answer as to whether belligerent transmission of malicious cyber code through neutral territory is a violation. First, Rule 150 prohibits belligerent action taken against neutral cyberinfrastructure.[83] The prohibition of such action, defined as action "intended to detrimentally affect neutral cyberinfrastructure," is uncontroversial.[84] Damage to cyber infrastructure from malicious code represents a clear violation of a neutral state's rights.[85] The rule does not discuss belligerent actions that do not result in harm.[86] Second, Rule 151 deals with a belligerent's use of neutral cyberinfrastructure.[87] This rule limits "use" to belligerent cyber activities that originate from within neutral territory or that remotely control neutral cyber infrastructure from outside the neutral state.[88] "Use" of neutral cyber infrastructure thus does not include a belligerent's transmission of malicious cyber code *through* it.[89]

Where such a transmission originates and terminates at points outside the territory of the neutral state, the international group of experts could not agree.[90] The majority and minority views are rooted in the disparate interpretation and application of Articles 2 and 8 of Hague V.

1. Belligerent Use of Neutral Telecommunications Systems

Article 8 of Hague Convention V contains a significant exception to the law of neutrality related to belligerent use of neutral communications infrastructure that is open to the public.[91] Specifically, a neutral state has no obligation to prevent "the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[92] The majority of *Tallinn* experts rely on Article 8 to assert that the same exception applies in cyberspace if the character of a belligerent transmission is merely communicative.[93] Under this interpretation, if a neutral state were aware belligerents were

---

[83] *Id.*
[84] *Id.* ("The exercise of belligerent rights by cyber means directed against neutral cyber infrastructure is prohibited").
[85] *Id.*
[86] *Id.* at 556.
[87] *Id.*
[88] *Id.* at 556–57.
[89] *Id.* at 556.
[90] *Id.* at 556–57.
[91] Hague V, *supra* note 28, art. 8.
[92] *Id.*
[93] TALLINN MANUAL 2.0, *supra* note 22, at 556–57.

exercising command and control via emails transiting through its cyber infrastructure, it would be under no obligation to take action to stop them.

The Article 8 exception is logical because belligerent radio transmissions are, in most cases, far less intrusive and disruptive to a neutral state than the physical penetration of its territory by equipment or personnel. Records from the Hague Conventions indicate that this exception stems from the practical problems associated with stopping belligerents from using open, public communications systems.[94] The exception is also consistent with the Hague Conventions' tendency to permit belligerent conduct when such acts do not involve deliberate control and operation.[95] While the *Tallinn Manual 2.0* aptly observes that "a single email message sent from belligerent territory may automatically be routed through neutral cyberinfrastructure before reaching its intended destination; the sender or the owner of the neutral cyberinfrastructure cannot necessarily control the route it takes," experts rely exclusively on the character of the transmission to conclude that it is permissible.[96] The majority does not remark on comparative degrees of intrusion or the practical challenges inherent in preventing such transmissions.

2. Transport of Belligerent Munitions and Supplies Across Neutral Territory

The *Tallinn Manual 2.0*'s experts compare the transmission of cyber weapons to activities prohibited in Article 2 of Hague Convention V.[97] Specifically, a belligerent's transportation of munitions or supplies across the neutral sovereign territory violates the law of neutrality.[98] The majority directly applies this provision to the belligerent transmission of cyber weapons through neutral cyberinfrastructure and concludes that such transmissions are illegal.[99] They arrived at this conclusion even after

---

[94] CARNEGIE ENDOWMENT FOR INT'L PEACE, THE REPORTS TO THE HAGUE CONFERENCES OF 1899 AND 1907, at 543 (James Brown Scott ed., 1917) [hereinafter THE HAGUE REPORTS] ("We are here dealing with cables or apparatus . . . the operation of which, for the transmission of news, has the character of a public service. There is no reason to compel the neutral State to restrict or prohibit the use by the belligerents of these means of communication. Were it otherwise, objections of a practical kind would be encountered, arising out of the considerable difficulties in exercising control, not to mention the confidential character of telegraphic correspondence and the rapidity necessary to this service.").

[95] *See* Augustine, *supra* note 2, at 75 (observing that relevance of a state's ability to effectuate control and operation over situations to the law of neutrality at sea).

[96] TALLINN MANUAL 2.0, *supra* note 22, at 554.

[97] *Id.* at 557.

[98] *Id.*

[99] *Id.*

acknowledging the unique nature of cyberspace, wherein data is broken into packets during transmission.[100] The minority group, however, rejected Article 2's direct application to the transmission of any kind of data, even cyber weapons, citing the article's purpose as "to prevent the physical transport of weapons."[101] Like the analysis pertaining to Article 8, the experts mention neither the conduct's relative degree of intrusiveness nor the practicality of observing and stopping belligerent transport of physical supplies and munitions over land.[102] Notably, the U.S. Department of Defense adopts the minority view, illustrating that the divide has surfaced in national policies and thus prompting a fresh examination of Hague Convention V's provisions.[103]

V. Transmitting Malicious Code: Why the *Tallinn* Majority Gets It Wrong

The Hague Conventions addressed a need for specific rules governing the conduct of hostilities in order to protect the rights of belligerents and neutrals alike. Although the rules are relatively straightforward, they do not amount to a rigid framework. Scrutiny reveals the general principles adapt to specific domains and the inclusion of special exceptions to account for a range of belligerent conduct.[104] Belligerent use of neutral public communication systems is one such exception.[105] Embracing common sense flexibility, this exception arose to account for practical challenges inherent in monitoring and preventing the use of radio signals.[106] Similarly, reports document that Hague V's explicit prohibition on belligerent transportation of supplies and munitions through neutral territory addresses the physical intrusion inherent in logistical operations over land.[107] The *Tallinn* majority's approach, based on the character of the transmitted data, problematically ignores the purpose of these

---

[100] *Id.* The experts "saw no reason to differentiate between the transmission of a complete cyber weapon or a cyber weapon . . . on the basis that the transmission of individual components would violate neutrality." *Id.*

[101] *Id.*; *see also* THE HAGUE REPORTS, *supra* note 94, at 539 (emphasizing the inviolability of neutral territory and the seriousness of physical intrusion resulting from the passage of troops or convoys).

[102] TALLINN MANUAL 2.0, *supra* note 22, at 557.

[103] LAW OF WAR MANUAL, *supra* note 21, § 16.4.1 (stating that relaying information through neutral communications infrastructure generally would not violate the law of neutrality and that this rule appears applicable even if that information "may be characterized as a cyber weapon or otherwise could cause destructive effects in a belligerent State (but no destructive effects within the neutral State or States)").

[104] Hague V, *supra* note 28, art. 8.

[105] *Id.*

[106] THE HAGUE REPORTS, *supra* note 94.

[107] *Id.* at 539.

provisions.[108] The majority approach also ignores its practical implications and the importance of intent when proscribing state conduct, ultimately contravening the law of neutrality's purposes.

A. Misapplication of Hague V Provisions

The majority view distinguishes between belligerent cyber communications and cyber weapons in evaluating belligerent transmissions through neutral cyberinfrastructure and applies two Hague V articles by analogy to cyber transmissions to support its position.[109] Applying Article 8, which permits belligerent use of neutral public communications structure, the majority concludes that belligerent transmissions with a communicative purpose do not violate the law of neutrality when transmitted through a neutral, open, and publicly accessible network.[110] However, transmissions of cyber munitions violate the law of neutrality, even when said munitions are broken into packets; the application of Article 2's prohibition of transporting belligerent supplies and munitions across the neutral territory is the basis for this conclusion.[111] The majority thus believes that the *character* of a transmission is dispositive.[112]

There are several problems with the position that the character of a transmission determines whether the law of neutrality is violated. Reports from Hague V clarify that the Article 8 exception results from the impracticality of preventing belligerent use of neutral communications towers.[113] It is not clear that this exception is based, in any way, on the purpose or character of communications. The same reports indicate that Article 2's explicit prohibition of the transport of belligerent supplies and munitions across a neutral state relates to the physical intrusion of such operations.[114] Indeed, the fact that the prohibition applies equally to *supplies* and *munitions* is instructive and suggests that the character of the transported items is less relevant than the nature of the intrusion itself.[115]

---

[108] *Id.* at 539, 543.
[109] TALLINN MANUAL 2.0, *supra* note 22, at 556–57.
[110] *Id.*
[111] *Id.* at 557.
[112] Another way to describe the majority's distinction would be the "purpose" of the transmission. A transmission could, however, have multiple purposes. For example, the purpose of transmission between a headquarters element and a forward operating unit that communicates the command to fire a weapon could be classified as a communication or the first step in an attack. The word "character" was selected as there is no evidence in the *Tallinn Manual 2.0* clearly indicating that the majority adopted an effects-based approach.
[113] THE HAGUE REPORTS, *supra* note 94.
[114] *Id.* at 539.
[115] Hague V, *supra* note 28, art. 2; THE HAGUE REPORTS, *supra* note 94, at 539.

Considering Articles 2 and 8 together, the degree and magnitude of the belligerent intrusion is essential. Belligerent communications via radio waves above neutral territory are far less physically invasive to a neutral state than a convoy of vehicles maneuvering over its terrain. In cyberspace, all data transmissions result in the same relative degree of intrusiveness, irrespective of whether a transmission qualifies as a communication or a weapon.[116] Even if the majority accounted for this reality and distinguished the character of transmissions using an effects-based approach, its analysis remains flawed. Cyber communications, like radio transmissions, can directly contribute to achieving physical effects on a target. It is not difficult to imagine a situation wherein military communication—transmitted over radio waves or through cyberinfrastructure—serves as the command signal to execute an attack, gaining a measurable military advantage as compared to delivering foodstuffs via convoy across the neutral territory. Whether founded in the character or likely effects of a particular transmission, the *Tallinn* majority view is flawed. The better view is that no belligerent cyber transmission, regardless of its character or purpose, violates the law of neutrality when transmitted through neutral cyber infrastructure without affecting the neutral state.

B. Untenable Practical Implications

The Hague Conventions account for the intent and capabilities of both belligerent and neutral parties through exceptions and domain-specific adaptions to ensure that the rules are practical. Article 8's exception is one such example, recognizing a neutral state's limited ability to stop belligerent use of their communications towers and, equally, the limited ability of belligerents to manipulate the direction of radio waves.[117] Neutral detection and attribution of belligerent conduct in radio communications is challenging due to a transmissions' high speed and invisible nature.[118] If a neutral state became aware of belligerent radio transmissions and was obligated to stop them, its failure to do so may invite a response from the aggrieved belligerent.[119] This would impose an unreasonable requirement on neutral states to detect and stop unintentional belligerent conduct, likely without success. Like radio transmissions, the speed and nature of all cyber transmissions make them nearly impossible for a neutral

---

[116] *See* McCormack, *supra* note 25, at 223 (explaining that all digital data is reduced to strings of 1s and 0s).
[117] Hague V, *supra* note 28, art. 8; THE HAGUE REPORTS, *supra* note 95.
[118] THE HAGUE REPORTS, *supra* note 94.
[119] LAW OF WAR MANUAL, *supra* note 21.

state to detect or reliably attribute to a belligerent party.[120] Imposing a duty on neutral states to stop belligerent use of their cyberinfrastructure fails to account for states' limited capabilities and ignores the futility of a rule designed to deter unintentional belligerent conduct.

Another example of flexibility in the law of neutrality exists in its application to the maritime environment; specifically, Hague XIII is replete with situations wherein belligerent vessels may penetrate a neutral state's sovereign waters or dock in its ports without violating the law of neutrality.[121] These adaptions acknowledge that the sea often presents unforeseen challenges to the deliberate maneuver of forces, as conditions and *force majeure* may compel a belligerent vessel along an unintended path.[122]

So long as a belligerent vessel moves expeditiously through a neutral state's territorial waters and docks only for harmless purposes, it has not violated the law of neutrality.[123] This right of belligerent vessels to move expeditiously through neutral waters is known as "innocent passage."[124] It stems in part from the features of the maritime regime that limit the number of available paths through which vessels may transit safely.[125] Characteristics of the cyber domain resemble features of the maritime environment. The automated, uncontrollable manner by which data moves through the internet may cause belligerent transmissions to unintentionally enter a neutral state's cyberinfrastructure, similar to maritime *forces majeure*. Similarly, internet architecture may present limited pathways between points; if all paths utilize neutral cyberinfrastructure, the sender

---

[120] TALLINN MANUAL 2.0, *supra* note 22, at 115 (explaining that "it is often difficult to attribute cyber activities to a particular State or actor with unqualified certainty" and providing examples of domain-specific operations that serve to "mask or spoof" the originator of a transmission).

[121] *See* Hague XIII, *supra* note 28. Examples where the domain of the sea proves less restrictive toward belligerent conduct include: (1) Article 7, which does not require neutral states to prevent the export or transit of "anything which could be of use" to belligerent forces in the maritime regime; (2) Article 10, which clarifies that the "mere passage" of belligerent vessels through a neutral power's territorial waters does not violate the law of neutrality; (3) Article 11, which permits a neutral power's licensed pilots to be employed by, and thus assist, belligerent vessels transiting through its waters; and (4) Articles 14–20, which relate to the conditions under which belligerent vessels may dock and make use of neutral ports.

[122] *Id.* art. 14 (mentioning the "stress of weather" as a reason for a belligerent ship to prolong its stay in a neutral port).

[123] *Id.* art. 10.

[124] LAW OF WAR MANUAL, *supra* note 21, § 13.2.2.4.

[125] THE HAGUE REPORTS, *supra* note 94, at 847 (discussing the "special condition of straits which might be situated within the area of territorial waters" and recognizing that straits which serve to connect open seas may never be closed).

has no option save to send a transmission through it. The proclamation that transmitting any variety of belligerent code through neutral cyber infrastructure violates the law of neutrality represents a departure from its historical flexibility, which adapts to other domains and provides exceptions recognizing states' limitations to control their conduct within them.

VI. Conclusion: Preserving the Law of Neutrality's Key Purposes

In addition to its imprecise application of Hague V's articles to cyberspace and its failure to account for the realities of state capabilities and domain features, the *Tallinn* majority view also results in consequences that undermine the very purposes of the law of neutrality.[126] In light of states' limited capabilities to detect and characterize belligerent transmissions, an obligation to prevent belligerent use of cyberinfrastructure is impractical and burdensome. More importantly, incapable states' failure to uphold this obligation begets the right of aggrieved belligerents to respond themselves.[127] Post-cyberattack, an aggrieved belligerent could then justify the destruction of a neutral state's cyberinfrastructure based on the assumption that the malicious code transited through its networks. The neutral state is thus drawn into the hostilities, resulting in an escalation of the conflict: the very consequence the law of neutrality seeks to prevent.[128] Finally, to prevent an aggrieved belligerent from responding, a neutral state may be forced to shut down its networks; considering modern society's reliance on the internet for basic functions such as banking and commercial activities, communication, commerce, and the management of critical infrastructure, the negative impact to neutral governments, persons, and commerce could prove colossal.[129] The majority view thus contravenes the aim of protecting commerce, the neutral state, its functions, and its people.

---

[126] LAW OF WAR MANUAL, *supra* note 21, § 15.1.3.

[127] *See* Augustine, *supra* note 2, at 82 (discussing the risk that a neutral state will be dragged into a conflict as the result of impermissible use of its cyber infrastructure).

[128] *See* Horace B. Robertson, Jr., *The "New" Law of the Sea and the Law of Armed Conflict at Sea*, 68 INT'L L. STUD. 263, 302 (1995) (explaining that the overtaxing of neutral states to enforce their duties to prevent belligerent conduct in an expansive maritime environment may result in "increased tension between neutral and belligerent states," thus "widening the area of conflict and drawing neutral states into it). Importantly, the exceptions for belligerent vessels at sea significantly reduce a neutral state's obligation to monitor and address belligerent conduct in its waters, thus decreasing the identified risk. *Id.*

[129] Stahl, *supra* note 19, at 248 ("The advent of the Internet has brought with it a fundamental change in the way nations and their citizens engage in global economic activity, manage critical infrastructure, and communicate with one another. Although the Internet is ubiquitous in modern society and plays a critical role in many aspects of everyday life, it was never intended to be used by so many and for the vast number of functions it performs today.").

The superior position is that the transmission of any belligerent data through neutral cyberinfrastructure, whether constituting communications or malicious code, does not violate the law of neutrality. The anarchy of cyberspace is analogous to the maritime domain, which is unpredictable and defies human control, necessitating exceptions to account for unintentional belligerent conduct and the impracticality of obligating neutral states to regulate it. Cyber transmissions are unique, but they are more similar by analogy to radio transmissions than a convoy of supplies regarding intrusiveness and neutral states' ability to detect and attribute them to belligerent actors. If belligerent transmissions through neutral cyber infrastructure do not violate international law, neutral states will not incur an obligation to prevent or stop them. Aggrieved belligerents will not derive a right to target neutral states' cyberinfrastructure from their failure to act. Neutral states will not become ensnared in the conflict due to events they could not foresee or affect and will not be forced to take action that may impair their economies, communications systems, and basic government functions.

In absence of international consensus, the United Nations maintains that "case-by-case" assessments will determine whether cyber operations violate state sovereignty,[130] and by implication, the law of neutrality. This unacceptable solution allows inconsistent legal interpretations to govern state practice, thus eroding the law of neutrality's normative force. Unpredictable state behavior undermines deterrent efforts that rely on the certainty of state responses to real or perceived provocation. The United States should highlight the shortcomings of the United Nations' case-by-case approach in international forums and urge formulation of clear rules that promote stability in cyberspace via foreseeable consequences for state behavior. They should equally argue against impractical legal frameworks that declare belligerent transmissions through neutral cyber infrastructure *per se* violations of international law. Universal application of an exception—like that of Article 8 in Hague Convention V—to *all* belligerent transmissions is the superior solution and preserves the law of neutrality's central purposes. The United States has wisely adopted this minority position[131] and now must advocate for other states to do the same.

---

[130] U.N. Secretary-General, *supra* note 22, at 26/142.
[131] LAW OF WAR MANUAL, *supra* note 21, § 16.4.1.

THIS PAGE INTENTIONALLY LEFT BLANK