Fordham International Law Journal

Volume 35, *Issue* 3 2012 *Article* 2

Sovereignty and Neutrality in Cyber Conflict

Eric Talbot Jensen*

*Brigham Young University Law School

SYMPOSIUM

CYBER ATTACKS: INTERNATIONAL CYBERSECURITY IN THE 21ST CENTURY

ARTICLE

SOVEREIGNTY AND NEUTRALITY IN CYBER CONFLICT

Eric Talbot Jensen[*]

INTRODUCTION 816
I. CYBER OPERATIONS AND THE LAW OF NEUTRALITY IN INTERNATIONAL ARMED CONFLICT 818
A. The Law of Neutrality 819
B. Neutrality and Cyber Operations 824
1. Belligerents and Cyber Neutrality 824
2. Neutrals and Cyber Neutrality 826
C. Applying Neutrality Law to the Scenario 827
II. CYBER OPERATIONS AND NON-INTERNATIONAL ARMED CONFLICT 830
A. Cyber Crime or Armed Conflict 832
B. The Law in NIAC 833
C. The Modified Scenario 835
III. APPLYING THE PRINCIPLES OF NEUTRALITY TO CYBER OPERATIONS IN NON-INTERNATIONAL ARMED CONFLICTS 838

* Associate Professor, Brigham Young University Law School. The Author wishes to thank Ryan Fisher for his exceptional research and editing assistance. This Article was initially prepared for presentation at the *Fordham International Law Journal* Symposium, Cyber Attacks: International Cybersecurity in the 21st Century. While writing this Article, the Author was engaged with other experts from around the world in writing the *Manual on Cyber Warfare in International Armed Conflict*, otherwise known as the *Tallinn Manual*, which is forthcoming from Cambridge University Press. Hence, the Author benefitted greatly from the discussions, which occurred during the writing of the neutrality provisions of the *Tallinn Manual*.

A. The Benefits 839
B. The Process 840
CONCLUSION 841

INTRODUCTION

> *Longstanding notions of sovereignty fall apart when it comes to cyber operations.*[1]
>
> Lieutenant General Robert Schmidle,
> Deputy Commander of US Cyber Command

As stated in the quote that begins this Article, cyber activities in general, and cyber warfare in particular, place stress on the traditional notions of sovereignty, challenging both belligerent nations and neutral nations in the application of law to cyber operations during international armed conflict. As cyber capabilities increase both at the national level and at the nonstate actor level, the principle of sovereignty will continue to come under increasing pressure to provide clarity to a paradigm that eschews attributability of actors and characterization of actions.[2]

Despite these apparent difficulties, the law of neutrality is still a binding legal doctrine in the cyber age. It can have increasing utility by incorporating modern understandings of its applicability to international armed conflicts and by extending its coverage to parties and nonparties in noninternational armed conflicts.

Consider the following scenario. State *G* and State *X* are in an international armed conflict. State *G* wants to conduct a cyber attack on State *X*, but avoid attribution of the attack. To facilitate this, State *G* takes the following actions:

An agent of State *G* uses his tourist passport to lawfully enter neutral State *H*, carrying a cyber tool on a thumb drive.

---

1. David Perera, *Schmidle: Cyber Ops Might Require New Combatant Command Structure*, FIERCEGOVERNMENTIT (May 15, 2011, 4:29 PM), http://www.fiercegovernmentit.com/story/schmidle-cyber-ops-might-require-new-combatant-command-structure/2011-05-15.

2. Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397–404 (2011).

Once within State *H*, *G*'s agent enters a cyber café and plugs the thumb drive into one of the computers. Upon activation, the cyber tool is copied to the hard drive and establishes a signaling beacon that then broadcasts across the Internet and awaits contact by another prearranged cyber tool.

Shortly thereafter, another agent of State *G* offers free thumb drives under the guise of a promotional gimmick from a local business to customers boarding a commercial cruise ship flagged in neutral State *M*, leaving from a port in neutral State *R*. Once the cruise ship leaves the port (and has likely entered the high seas), any customer who plugs the thumb drive into the ship's passenger computers will upload a malicious malware that will become resident on the ship's computer system. The ship's computers connect to the Internet through a commercial carrier satellite operated by a company registered in neutral State *F*. Once the computer is connected to the Internet, the malicious malware on the ship's computer sends a signal across the Internet, seeking the beacon that is now resident on the computer in State *H*.

Once the shipboard cyber tool has connected with the beacon, a code is executed that sends a malicious cyber program to the beacon. Upon arrival at the computer in State *H*, it combines with the cyber tool at the beacon and creates cyber malware that is then forwarded to a computer in State *X*. State *G* previously gained access to that computer through the work of a citizen of neutral State *J*, which State *G* had hired for that purpose. Once the cyber malware reaches the computer in State *X*, it initiates an action that amounts to an attack on State *X* that causes death and destruction.

Part I of this Article analyzes this scenario and its wider implications. It determines that the law of neutrality applies in most instances to cyber operations during international armed conflict and supplies an adequate framework for responding to such actions. This Part also highlights some key points where it does not. While nations still have the legal obligation to both respect the doctrine of neutrality while in international armed conflict and to abide by it when not a belligerent, some elements of the Internet and its infrastructure require an evolved application of neutrality by both belligerents and neutrals.

Now consider the following modification to the above scenario. Rather than international armed conflict between two states, assume a scenario where a nonstate actor, such as a terrorist organization, takes these actions against State *X*. This modified scenario creates perplexing questions as to the application of the law and certainly does not implicate the laws of neutrality since there is no international armed conflict occurring.

Part II of this Article analyzes a modified scenario involving the terrorist organization and demonstrates that traditional principles of sovereignty, including neutrality, have limited application as a matter of law to noninternational armed conflicts against transnational organizations such as terrorist organizations. Part III proposes that borrowing the doctrines of neutrality and applying them more fully to noninternational armed conflicts will facilitate states' ability to adequately respond to situations similar to the modified scenario and provide an additional legal paradigm that states that are not a party to the noninternational armed conflict ("NIAC") can apply to help prevent escalation and maintain their lack of involvement.

I. *CYBER OPERATIONS AND THE LAW OF NEUTRALITY IN INTERNATIONAL ARMED CONFLICT*

The scenario in the Introduction assumes that State *G* and State *X* are involved in an international armed conflict ("IAC"). As a result of that assumption, the law of armed conflict, or LOAC, applies to their conflict.[3] The LOAC contains robust provisions governing the interaction and use of force between State *G* and State *X*, including the Geneva[4] and Hague Conventions.[5]

---

3. *See* Geoffrey S. Corn, Hamdan*, Lebanon, and the Regulation of Hostilities: The Need to Recognize a Hybrid Category of Armed Conflict*, 40 VAND. J. TRANSNAT'L L. 295, 300–09 (2007); Geoffrey S. Corn & Eric Talbot Jensen, *Untying the Gordian Knot: A Proposal for Determining Applicability of the Laws of War to the War on Terror*, 81 TEMP. L. REV. 787, 796–98 (2008).

4. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention), Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention), Aug. 12, 1949, 6

The LOAC also provides rules on the interactions between belligerent states, *G* and *X*, and states that are not involved in the conflict, otherwise known as neutral states. The interaction with these states is governed by the law of neutrality.[6]

A. *The Law of Neutrality*

The law of neutrality has ancient origins[7] and is one of the most fundamental and longstanding principles of the LOAC. Substantially codified in the 1907 Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land ("Hague V")[8] and Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War ("Hague XIII"),[9] the principle of neutrality serves two primary functions. First, it prohibits certain activities by belligerent nations that might detrimentally impact the neutral nation and draw the neutral nation into the conflict either unwillingly or unwittingly.[10] Second, it requires neutral nations to take certain actions and refrain from taking other actions in order to enforce and maintain that neutrality, including treating all belligerents equally.[11] These two principles provide

---

U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

5. Hague Convention (II) with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803 [hereinafter Hague II]; Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277 [hereinafter Hague IV]; 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].

6. *See, e.g.*, Hague V, *supra* note 5.

7. PHILIP C. JESSUP & FRANCIS DEÁK, 1 NEUTRALITY, ITS HISTORY, ECONOMICS AND LAW 1, 4 (1935).

8. *See* Hague V, *supra* note 5.

9. *See* Hague XIII, *supra* note 5.

10. *See, e.g.*, *id.* arts. 5, 18; *see also* OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, NWP 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ch. 7 (2007), *available at* http://www.usnwc.edu/getattachment/a9b8e92d-2c8d-4779-9925-0defea93325c/1-14M_(Jul_2007)_(NWP).

11. *See* HUMANITARIAN POLICY & CONFLICT RESEARCH, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE ¶¶ 166–67, at 52 (Program on Humanitarian Policy & Conflict Research, Harv. Univ. ed., 2009). The *Commander's Handbook on the Law of Naval Operations* states: "The law of neutrality serves

belligerents with predictability, knowing that they generally need not worry about hostile activities coming from neutral nations.

Exhaustive commentaries on the law of neutrality have been written elsewhere,[12] making detailed analysis unnecessary here. It is important to note, however, that the law of neutrality has survived the formation of the United Nations ("UN") and the promulgation of the UN Charter[13] and continues to be applied both in practice,[14] in recent manuals and commentaries on the LOAC,[15] and in the writings of scholars on cyber operations.[16]

---

to localize war, to limit conduct of war both on land and sea, and to lessen the impact of war on international commerce." OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., *supra* note 10, ¶ 7.1.

12. *See, e.g.*, VIITH CONGRESS OF THE INT'L ASS'N OF DEMOCRATIC LAWYERS, LEGAL ASPECTS OF NEUTRALITY: PROCEEDINGS OF THE THIRD COMMISSION (1960); ERIK J. S. CASTRÉN, THE PRESENT LAW OF WAR AND NEUTRALITY (1954); ELIZABETH CHADWICK, TRADITIONAL NEUTRALITY REVISITED: LAW, THEORY AND CASE STUDIES (2002); ROBERT W. TUCKER, THE LAW OF WAR AND NEUTRALITY AT SEA (1955); George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079 (2000).

13. As a result of Articles 25 and 103 of the United Nations Charter, every member nation agrees to follow the determinations of the Security Council with respect to issues of international peace and security. Thus, if the Security Council takes binding actions under Chapter VII, no nation could rely on the law of neutrality to avoid compliance with its obligations under the Charter of the United Nations. *See* U.N. Charter art. 25, 103.

14. *See, e.g.*, Georgios C. Petrochilos, *The Relevance of the Concepts of War and Armed Conflict to the Law of Neutrality*, 31 VAND. J. TRANSNAT'L L. 575, 599–601 (1998) (discussing the application of the law of neutrality during the Falklands Conflict).

15. This is confirmed by recent manuals written to reflect the current law of armed conflict ("LOAC"). For instance, Rule 165 of the *Humanitarian Policy and Conflict Research Manual on Air and Missile Warfare* reads:

> Where the Security Council takes binding preventive or enforcement measures under Chapter VII of the Charter of the United Nations—including the authorization of the use of force by a particular State or group of States—no State may rely upon the law of neutrality to justify conduct which would be incompatible with its obligations under the Charter of the United Nations.

HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶ 165, at 52. Additionally, Paragraphs 7 and 9 of the International Institute of International Humanitarian Law's *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* state:

> (7) Notwithstanding any rule in this document or elsewhere on the law of neutrality, where the Security Council, acting in accordance with its powers under Chapter VII of the Charter of the United Nations, has identified one or more of the parties to an armed conflict as responsible for resorting to force in violation of international law, neutral States: (a) are bound not to lend assistance other than humanitarian assistance to that State; and (b) may

Several basic provisions of the law of neutrality deserve specific mention with relation to cyber operations. First of all, assuming that State *G* and State *X* are involved in an IAC, for a nation to be neutral, the nation must not be a party to the IAC.[17] No formal declaration of neutrality is required by uninvolved states.[18] However, there is no room for either "qualified neutrality" or for "non-belligerency."[19] States are either neutrals, or they are participants.

The law of neutrality, combined with the doctrine of sovereignty, enshrines the inviolability of neutral nations and places belligerents under a strict obligation to respect the territorial sovereignty of the neutral.[20] In this sense, the territory of a neutral state comprises "the land territory of Neutrals as well as sea areas which are under the territorial sovereignty of the neutral costal State, i.e. internal waters, territorial sea and, where applicable, archipelagic waters, and the airspace above

---

> lend assistance to any State which has been the victim of a breach of the peace or an act of aggression by that State;
>
> (9) Subject to paragraph 7, where the Security Council has taken a decision to use force, or to authorize the use of force by a particular State or States, the rules set out in this document and any other rules of international humanitarian law applicable to armed conflicts at sea shall apply to all parties to any such conflict which may ensue.

INT'L INST. OF HUMANITARIAN LAW, SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA ¶¶ 7, 9, at 7–8 (Louise Doswald-Beck ed., 1995).

16. *See, e.g.*, Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 56 (2009); Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 90 (2009); Walker, *supra* note 12, at 1182.

17. *See, e.g.*, HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶ 1(aa), at 6; INT'L INST. OF HUMANITARIAN LAW, *supra* note 15, sec. V, ¶ 13(d), at 9; OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, *supra* note 10, ¶ 7.1; U.K. MINISTRY OF DEFENCE, JSP 383, THE JOINT SERVICE MANUAL ON THE LAW OF ARMED CONFLICT ¶ 12.11 (Joint Doctrine & Concepts Ctr. ed., 2004).

18. *See* OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS, ET AL., *supra* note 10, ¶ 7.2; OFFICE OF THE CHIEF OF NAVAL OPERATIONS, DEP'T OF THE NAVY, NWIP 10-2, LAW OF NAVAL WARFARE ¶ 231, at 2–5 (1955).

19. *See* Wolff Heintschel von Heinegg, *"Benevolent" Third States in International Armed Conflicts: The Myth of the Irrelevance of the Law of Neutrality*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 543, 543–68 (Michael Schmitt & Jelena Pejic eds., 2007) (providing a recent analysis on this issue).

20. *See* Hague V, *supra* note 5, art. 1; OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, *supra* note 10, ¶ 7.2.

those areas."[21] Objects located within the territory of a neutral state are both subject to that neutral state's jurisdiction and also protected by that state's neutrality irrespective of public or private ownership and irrespective of the nationality of the owners.[22]

The requirement to respect neutral territory prohibits belligerents from conducting hostilities within neutral territory[23] and should be understood in a broad sense. It is not limited to "attacks" as defined under the law of armed conflict.[24]

For example, Article 3 of Hague V makes it unlawful for belligerents to:

> a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;
>
> b) Use of any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages.[25]

In order to preserve its neutrality, the neutral state also accepts obligations to affirmatively prevent the use of its territory by belligerents. This obligation is found in Article 5(1) of the 1907 Hague Convention V, which states: "A neutral Power must not allow any of the acts referred to in Articles 2 to 4 to occur on its territory."[26] This includes an obligation on the neutral state to monitor activities on its territory, to the extent that the means

---

21. HUMANITARIAN POLICY & CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE 307 (Program on Humanitarian Policy & Conflict Research, Harv. Univ. ed., 2010).

22. *See* INT'L INSTITUTE OF HUMANITARIAN LAW, *supra* note 15, sec. I, ¶ 16, at 11.

23. *See, e.g.*, Hague V, *supra* note 5, art. 2; Hague XIII, *supra* note 5, art. 1; OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, *supra* note 10, ¶ 7.3; MANUAL OF HUMANITARIAN LAW IN ARMED CONFLICT ¶¶ 1108, 1149 (Federal Ministry of Defense of the Federal Republic of Germany ed., VR II 3, 1992); HUMANITARIAN POLICY AND CONFLICT RESEARCH, *supra* note 11, ¶¶ 166–67, at 52; INT'L INST. OF HUMANITARIAN LAW, *supra* note 15, ¶ 15, at 11; Hague Rules of Air Warfare, art. 39, drafted Dec. 1922–Feb. 1923, *reprinted in* THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 153, 153 (Dietrich Schindler & Juří Toman eds., 1981).

24. *See, e.g.*, Hague XIII, *supra* note 5, art. 2; HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶ 171(d), at 54.

25. Hague V, *supra* note 5, art. 3.

26. *Id.* art. 5; *see also* HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶¶ 167(a), 168(a), at 52.

at its disposal allow, in order to prevent the violation of its neutrality by the belligerents.[27] It would also allow the use of force in response to any attempted violation of its neutrality by a belligerent.[28]

Article 8 of Hague V provides an important exception to this rule. It states: "A neutral Power is 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."[29]

Another key point is clearly stated in the US Navy's *Manual of the Law of Naval Warfare*. It states that "if the neutral nation is unable or unwilling to enforce effectively its right of inviolability, an aggrieved belligerent may take such acts as are necessary in neutral territory to counter the activities of enemy forces, including warships and military aircraft, making unlawful use of that territory."[30] This makes sense, as the alternative would require a belligerent nation to receive attacks without any form of recourse, thus undercutting the foundational rationale for neutrality law.

Actions by a belligerent in response to a neutral nation's inability or unwillingness to maintain its neutrality would most certainly constitute a violation of the neutral state's sovereignty. Thus, not every action that might technically violate neutrality would allow belligerent response, but only those that "constitute[] an immediate threat to the security of the opposing belligerent."[31] Further, when a belligerent deems that self-help is required, any actions taken by the belligerent are

---

27. *See, e.g.*, Hague XIII, *supra* note 5, art. 8; Hague Rules of Air Warfare, *supra* note 23, arts. 42, 47, at 154; MANUAL OF HUMANITARIAN LAW IN ARMED CONFLICT, *supra* note 23, ¶¶ 1109, 1125, 1151; OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, *supra* note 10, ¶ 7.3; INT'L INST. OF HUMANITARIAN LAW, *supra* note 15, sec. I, ¶¶ 15, 18, 22, at 11–12; HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶¶ 168(a), 170(b), at 52–53.

28. *See* Hague V, *supra* note 5, arts. 5, 10; HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶¶ 168–70, at 52–53.

29. Hague V, *supra* note 5, art. 8.

30. OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, *supra* note 10, ¶ 7.3; JUDGE ADVOCATE GEN., CANADIAN MINISTRY OF NAT'L DEFENCE, B-GJ-005-104/FP-02, LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS ¶ 1304(3), at 13-1 (2001).

31. INT'L INST. OF HUMANITARIAN LAW, *supra* note 15, sec. I, ¶ 22, at 11.

subject to a prior notification and a reasonable time for the neutral state to terminate the violation.[32]

While these traditional principles of the law of neutrality are fairly well-accepted, their application to cyber activities is not necessarily so clear and deserves analysis.

B. *Neutrality and Cyber Operations*

The nature of the Internet and cyber activities raises questions about the application of the law of neutrality to cyber conflict. For example, when an email is sent across the Internet, it is broken into smaller "packets" of information, which are disseminated across the Internet in an undetermined and undirectable fashion.[33] This virtually ensures that malicious code sent by a belligerent will traverse cyber infrastructure in neutral nations. Does this mean that the belligerent has violated the laws of neutrality by sending something across the Internet?

Additionally, those who monitor neutral cyber infrastructure have limited ability with current technology to detect malicious packets and either stop or redirect them.[34] Do neutral nations potentially forfeit their neutrality because they are incapable of preventing potentially hostile packets from traversing their Internet infrastructure? Answering these and other similar questions will determine the continuing validity of the law of neutrality to cyber operations.

1. Belligerents and Cyber Neutrality

The starting point for analyzing belligerent obligations with respect to cyber activities under the law of neutrality is the basic premise that belligerents are prohibited from conducting cyber operations against an enemy from within neutral territory.[35] The same prohibition applies to the use of neutral cyber infrastructure that is located outside neutral territory in two cases. The first is if it enjoys the benefits of neutrality because of sovereign immunity. The second is if it is the private computer

---

32. OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, *supra* note 10, ¶ 7.3.

33. *See* Walker, *supra* note 12, at 1094–99.

34. *See id.* at 1158.

35. *See* Hague V, *supra* note 5, art. 1.

infrastructure or systems of a private entity or person from the neutral country that is not located within belligerent territory.[36]

In addition to a modernized version of the specific prohibitions discussed earlier from Article 3 of Hague V, "using" cyber infrastructure would include things such as initiating an attack or facilitating an attack within neutral territory. It would not include, as discussed further below, the mere passage of malware or malicious code over cyber infrastructure that was generally open for public use.

As stated above, the prohibition against belligerents conducting hostilities from neutral territory is to be understood in a very broad sense. In relation to cyber operations, this prohibition is not limited to "attacks" as defined under the law of armed conflict or to "'acts of cyber warfare" or to "cyber attacks." The use of neutral cyber infrastructure for intrusion into the enemy's cyber infrastructure to conduct actions harmful to the opposing belligerent would violate the law of neutrality.

As opposed to "using" a neutral's cyber infrastructure, "when Belligerent Parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a Neutral does not constitute a violation of neutrality."[37] A modern interpretation of Article 8 of Hague V seems to require this conclusion.[38] The same conclusion is supported by US government statements.[39]

In the event that a neutral nation's territory, including its cyber infrastructure, is being used for acts hostile to another belligerent, the targeted belligerent may respond proportionally to stop the hostile acts.[40] If the hostile actions were coming from

---

36. *See* Walker, *supra* note 12, at 1149–50.

37. HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶ 167(b), at 52.

38. *But see* Kastenberg, *supra* note 16, at 56–57; Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1442–45 (2008) (arguing that Article 8 does not apply to cyberspace); Todd, *supra* note 16, at 90–92.

39. *See* OFFICE OF GEN. COUNSEL, U.S. DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 23 (1999); Kelsey, *supra* note 38, at 1442.

40. *See* HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶ 168(b), at 53; OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, *supra* note 10, ¶ 7.3; INT'L INST. OF HUMANITARIAN LAW, *supra* note 15, sec. I, ¶ 22, at 12.

the neutral nation's cyber infrastructure, an appropriate response could include targeting the neutral nation's cyber infrastructure with either a cyber or kinetic response. Alternatively, a targeted nation could also respond to a noncyber hostile act from a neutral nation's territory with a cyber operation that would terminate the hostile act.

2. Neutrals and Cyber Neutrality

The basic responsibility of neutrals found in Article 5(1) of Hague V applies equally in cyber conflict.[41] Therefore, a neutral state must not knowingly allow acts of cyber warfare to be launched from cyber infrastructure located in its territory or under its exclusive control. This prohibition applies not only to instances where the organs of the state have actual knowledge of a belligerent act of cyber warfare, but also to cases of presumptive knowledge. For example, if the neutral state does not have sophisticated cyber infrastructure of its own and has therefore contracted with a commercial provider, the neutral state would be presumed to have knowledge possessed by that commercial provider.

In order to effectively maintain neutrality, a neutral state has a duty to effectively monitor, to the best of its ability, its own territory and infrastructure in order to prevent the launching of an act of cyber warfare from its territory or from cyber infrastructure it effectively controls. This duty to monitor is necessarily dependent upon the means and personnel available to the neutral state and upon the neutral state's level of technology, but a neutral nation must do everything feasible to maintain its neutrality by monitoring its cyber networks and precluding their use for hostile acts.[42] If, despite its best efforts, a belligerent act of cyber warfare is not prevented, the neutral state has violated its duty of prevention and leaves itself open to belligerent response as discussed above.[43]

The obligation for a neutral nation to not knowingly allow acts of cyber warfare from within its territory also necessarily

---

41. Hague V, *supra* note 5, art. 5(1); *see* HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 11, ¶ 168(a), at 52.

42. This is based on the requirement found in Hague V, *supra* note 5, art. 5.

43. *See supra* notes 30–32 and accompanying text.

authorizes the neutral state to take cyber actions (or kinetic actions, if necessary) to prevent such use. In other words, a neutral state would be absolutely authorized to strike back with cyber operations in an attempt to prevent a belligerent from using its territory or infrastructure for the commission of a hostile act.[44]

It is important to note once again that this obligation applies only to hostile cyber acts that are "launched" from within the neutral territory and not from hostile traffic merely transiting the neutral nation's cyber infrastructure. Therefore, the mere fact that military communications, including cyber attacks, have been transmitted via the cyber infrastructure of a neutral state may not be considered a violation of that state's neutral obligations.

C. Applying Neutrality Law to the Scenario

Having briefly reviewed the law of neutrality and analyzed its implications to cyber operations, it is now time to apply the law to the scenario proposed at the beginning of the Article. Remember that State *G* and State *X* are in an international armed conflict, meaning that the LOAC applies, including the law of neutrality. Further, State *G* wants to conduct a cyber attack on State *X*.

The first action taken by State *G* is to send an agent across the border into neutral State *H* carrying a cyber tool on a thumb drive. Once within State *H*, *G*'s agent enters a cyber café and plugs the thumb drive into one of the computers. Upon activation, the cyber tool is copied to the hard drive and establishes a beacon that waits until contacted by another tool.

Article 2 of Hague V prohibits the movement of "troops or convoys of either munitions of war or supplies across the territory of a neutral Power."[45] This has been interpreted to preclude moving "troops or war materials and supplies across neutral land territory."[46] A modern analysis requires a

---

44. Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 209 (2006).

45. Hague V, *supra* note 5, art. 2.

46. OFFICE OF THE CHIEF OF NAVAL OPERATIONS & HEADQUARTERS ET AL., DEP'T OF THE NAVY, *supra* note 10, ¶ 7.3.1.

determination of whether the cyber tool was "war material" or "supplies." Given the facts, it is likely that when *G*'s agent crosses the border into neutral *H* with the thumb drive containing software intended to facilitate a cyber attack on X, he is violating State *H*'s neutrality. The opposing argument is that software that merely establishes a beacon that attracts additional cyber software, or even combines with or supplements that software, is not a war material or supply. This position appears hard to support, as the insertion of the thumb drive and subsequent action from the computer are essential elements of the eventual attack. The better answer is that such an action during international armed conflict violates the neutrality of State *H*.

The next event occurs shortly thereafter. Another agent of State *G* offers free thumb drives under the guise of a promotional gimmick from a local business to customers boarding a commercial cruise ship flagged in neutral State *M*, leaving from a port in neutral State *R*. Once the cruise ship has left the port and entered the high seas, any customer who plugs the thumb drive into the ship's passenger computers will upload a malicious malware that will become resident on the ship's computer. The ship's computers connect to the Internet through a commercial carrier satellite operated by a company registered in neutral State *F*. Once the computer is connected with the Internet, the malicious malware on the ship's computer sends a signal across the Internet, seeking the beacon that is now resident on a computer in State *H*. When the shipboard cyber tool has connected with the beacon, a code is executed that sends a piece of a malicious cyber program to the beacon.

Multiple actions and neutral nations are involved in this action. For the same reasons discussed above, it is likely that *G* violates *R*'s neutrality when its agent entered *R*'s territory with the thumb drives since they contained the malicious malware. Based on Article 8 of Hague V, neither *M* nor *F* has an obligation to prevent *G* from using the privately owned shipboard computers or the privately owned satellite communication system to facilitate the attack on X.[47] However, because the privately owned cruise ship was flagged by neutral

47. While not the subject of this Article, these actions by State G likely raise significant LOAC issues concerning the principle of distinction and the role that civilians would unwittingly play in the attack.

State *M* and because the agent of State *G* intends to use the commercially owned network of a private company headquartered in State *F*, *G* has violated the neutrality of both of these states as well. The fact that the malware is not uploaded until the cruise ship is on the high seas removes any further violation of neutrality that would have occurred if the uplink would have happened while still in the territorial waters of State *R*. Because the high seas are not subject to any state's sovereignty, the geographic location of the ship does not implicate the doctrines of sovereignty or neutrality.

Upon arrival at the computer in State *H*, the malicious malware from the shipboard computer combines with the cyber tool at the beacon and creates cyber malware that is then forwarded to a computer in State *X* to which State *G* has previously gained access. State *G* gained access to the computer in State *X* through the work of a citizen of neutral State *J*, which State *G* had hired for that purpose. Once the cyber malware reaches the computer in State *X*, it initiates an action that amounts to an attack on State *X* causing death and destruction.

The neutrality issue here concerns the use of a private citizen from neutral State *J* to gain access to a computer system within State *X*, facilitating the eventual attack. Article 16 of Hague V states that "[t]he nationals of a State which is not taking part in the war are considered as neutrals."[48] However, Article 17 states:

> A neutral cannot avail himself of his neutrality (a) If he commits hostile acts against a belligerent; (b) If he commits acts in favor of a belligerent, particularly if he voluntarily enlists in the ranks of the armed force of one of the parties. In such a case, the neutral shall not be more severly [sic] treated by the belligerent as against whom he has abandoned his neutrality than a national of the other belligerent State could be for the same act.[49]

The civilian hired by the agent of State *G* enjoys protection based on State *J*'s neutrality until he decides to act for State *G* and performs an act hostile to State *X*. At the point that he makes that decision, he loses his protections as a neutral and,

48. Hague V, *supra* note 5, art. 16.
49. *Id.*, *supra* note 5, art. 17.

depending on the nature of his hostile act, may lose his protection as a civilian.[50] However, this has no effect on the neutrality of State *J*. Additionally, there are no further neutrality implications as these events occur within State *X*, the other belligerent in the armed conflict.

Therefore, in this IAC scenario, State *G* has violated the neutrality of States *H*, *R*, *M*, and *F*, but not *J*, although the specific individual citizen of *J* has forfeited his neutral protections. Despite the lack of complete precision, current neutrality law is fairly clear in its application to the IAC scenario. However, the vast majority of conflicts over the past six decades have not been IACs, but NIACs.[51] It is to this type of armed conflict that this Article will now turn to discuss.

II. *CYBER OPERATIONS AND NON-INTERNATIONAL ARMED CONFLICT*

Despite the convenience of having a clear set of laws that apply to cyber operations in IAC, the reality of the current world situation is that cyber attacks have seldom, if ever, occurred between nation states during armed conflict. The United States contemplated doing so during the invasion of Iraq in 2003[52] and again against Libya's el-Qaddafi regime in 2011.[53] Some have

---

50. There is currently a continuing debate on the actions that a civilian might take to be considered as directly participating in hostilities or targetable as a member of an organized armed group. *See* J. Ricou Heaton, *Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces*, 57 A.F. L. Rev. 155, 157–58 (2005); Richard S. Taylor, *The Capture Versus Kill Debate: Is the Principle of Humanity Now Part of the Targeting Analysis When Attacking Civilians Who Are Directly Participating in Hostilities?*, 2010 ARMY L. 103, 108–09 (2010).

51. The Uppsala University Department of Peace and Conflict Research has compiled extensive research on the issue of armed conflicts. *See Program Overview*, DEP'T PEACE & CONFLICT RESEARCH-UPPSALA UNIV., http://www.pcr.uu.se/research/ucdp/program_overview/ (last visited Feb. 20, 2012). For a graphic representation of the numbers of international armed conflicts ("IACs") and non-international armed conflicts ("NIACs"), see *Armed Conflict by Type, 1946–2009*, DEP'T PEACE & CONFLICT RESEARCH-UPPSALA UNIV., http://www.pcr.uu.se/digitalAssets/20/20864_conflict_types_2009.pdf (last visited Feb. 20, 2012).

52. Judi Hasson, *US Considered 2003 Cyber Attack on Iraq*, FIERCEGOVERNMENTIT (Aug. 2, 2009, 4:10 PM), http://www.fiercegovernmentit.com/story/u-s-considered-2003-cyber-attack-iraq/2009-08-02.

53. Eric Schmitt & Thom Shanker, *U.S. Wrestles with Cyberwar's Place; White House Refrained from Tactics in Libya, Fearful of a Precedent*, INT'L HERALD TRIB., Oct. 19, 2011, at 5.

argued that Russia coordinated activist attacks on both Estonia in 2007[54] and Georgia in 2008.[55] At latest report, more than 100 nations either currently have or are actively pursuing cyber capabilities.[56] However, to date, no state has either claimed to have executed cyber attacks on another government or claimed to have been the target of cyber attacks by another government during armed conflict.

This lack of official state-sponsored cyber attacks is not indicative of the amount of cyber activities that are occurring across the world, including those that either target nations or are conducted by nations.[57] The pervasiveness of cyber attacks have been well-documented elsewhere[58] and do not need to be repeated here. However, it is important to note that states are increasingly concerned about the prospect of cyber conflict

---

54. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 5 (2009); *A Look at Estonia's Cyber Attack in 2007*, MSNBC.COM (July 8, 2009, 2:24 PM), http://www.msnbc.msn.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/; President Ilves, Speech on the Occasion of International Cyber Conflict Legal and Policy Conference in Tallinn (Sept. 9, 2009) (transcript available at http://www.eesti.ca/?op=article&articleid=25139) [hereinafter President Ilves's Speech].

55. Sklerov, *supra* note 54, at 4–5; William Matthews, *China is Most Formidable Cyber Foe, Experts Warn*, FED. TIMES, Jan. 25, 2010, at 13; President Ilves's Speech, *supra* note 54.

56. Andrea Shala-Esa & Jim Finkle, *NSA Helps Banks Battle Hackers*, REUTERS (Oct. 26, 2011), http://www.reuters.com/article/2011/10/27/us-cybersecurity-banks-id USTRE79P5E020111027.

57. This is not to say that governments are not sponsoring or conducting a great deal of cyber activity. *See Cybersecurity Task Force Releases Recommendations, Rep. Mac Thornberry (R-TX) News Release*, FED. INFO. & NEWS DISPATCH, INC., Oct. 5, 2011, *available at* LEXIS. Recently, the US Congress has held a number of hearings on China state-sponsored theft of intellectual property. Douglas Birch, *US Lawmaker Slams China for Cyber Spying*, ASSOCIATED PRESS, Oct. 4, 2011, *available at* LEXIS. However, these cyber operations have generally been on defense contractors or other corporate entities and not on the US government itself, and certainly not during an armed conflict. Further, if "attack" were defined in accordance with the LOAC, it would require an "act of violence." Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1) art. 49, June 8, 1977, 1125 U.N.T.S. 3. *See generally* Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NAT'L SEC. L. BRIEF 33 (2011). For the purposes of this Article, it is sufficient to say that no attacks during armed conflict have occurred between nations.

58. *See generally* Hollis, *supra* note 2.

from other states, individuals, and nonstate actors.[59] In an environment where states, terrorist organizations, criminal enterprises, and individuals are all equally as likely to be "attackers" as they are to be targets, differentiating between cyber incidents and the law that they implicate is vital.

A. *Cyber Crime or Armed Conflict*

The determination of what law applies to a cyber event depends largely on how that event is characterized. Characterizing an event is aided by knowing the actor and activity that has occurred. For example, an intrusion into a government logistics system by recreational hackers[60] is almost certainly going to be considered a criminal activity, and any retributive action will likely be taken through the criminal law system of the hackers' nations, even if that event occurs during an on-going IAC. However, if the same intrusion was coming from state actors of another state, such an act would likely be understood in a different light and, depending on the seriousness of the event, might be considered an armed attack initiating hostilities[61] or part of the on-going IAC.

It is clear that most of the cyber events that occur are merely criminal events and should be handled under domestic criminal law. However, it is also clear that cyber operations are very likely to take place in armed conflicts, even those not involving interstate conflict. Acts that would be criminal and

---

59. Eric Talbot Jensen, *Ten Questions, Responses to the Ten Questions: President Obama and the Changing Cyber Paradigm*, 37 WM. MITCHELL L. REV. 5049 (2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1740904 (noting that

> [d]uring a time of significantly reduced budgets, the UK government made some difficult decisions on the allocation of defense resources. In a move that would shock most other nations, the United Kingdom opted to forego the production of aircraft capable aircraft carriers and allocate those resources to expanding and maintaining its cyber defenses).

60. *See* Hollis, *supra* note 2, at 400 (discussing a major hacking event of the US military logistics operations by two teenagers from California and their mentor from Israel).

61. This Article is concerned mainly with the *jus in bello*, but it is as of yet an undecided question as to what cyber activities would amount to a use of force or armed attack under the *jus ad bellum*. *See generally* OFFICE OF GEN. COUNSEL, U.S. DEP'T OF DEF., *supra* note 39; Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

handled by domestic criminal law in the absence of an armed conflict will invoke the LOAC applying to NIAC if done in connection with an armed conflict. The potential frequency of this possibility requires a closer look at the law in NIAC that applies to cyber events.

B. *The Law in NIAC*

Where IACs are governed by the full LOAC, NIACs are governed by a much less robust set of laws.[62] Most states,[63] courts,[64] and academics[65] agree that many LOAC provisions apply to NIACs, such as the principle of distinction in selecting and engaging targets. But it is clear that many LOAC principles, including the law of neutrality and its impact on sovereignty, are only applicable during an IAC.[66] This leaves states with limited

---

62. *See supra* note 3 and accompanying text.

63. *See* U.K. MINISTRY OF DEFENCE, *supra* note 17, ¶¶ 15.5–15.33, at 388–400. Both the United States and Canada have stated that they will apply the provisions of the LOAC during NIACs. *See* DEP'T OF DEFENSE, DIRECTIVE 2311.01E, DOD LAW OF WAR PROGRAM ¶ 4.1 (2006); JUDGE ADVOCATE GEN., CANADIAN MINISTRY OF NATIONAL DEFENCE, *supra* note 30, ¶ 1702.2, at 17-1.

64. *See* Prosecutor v. Tadic, Case No. IT-94-1-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 119 (Int'l Trib. for the Former Yugoslavia Oct. 2, 1995) ("What is inhumane, and consequently proscribed, in international wars, cannot but be inhumane and inadmissible in civil strife."). The same Court also stated: "If international law, while of course duly safeguarding the legitimate interests of States, must gradually turn to the protection of human beings, it is only natural that the [distinction between IAC and NIAC] should gradually lose its weight." *Id.* ¶ 97; *see also* Rome Statute of the International Criminal Court art. 8(2)(e), July 17, 1998, 2187 U.N.T.S. 90, 97–98.

65. *See, e.g.*, MICHAEL N. SCHMITT, CHARLES H.B. GARRAWAY & YORAM DINSTEIN, INT'L INST. OF HUMANITARIAN L., THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT: WITH COMMENTARY (2006); *see* 1 & 2 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (2005) (describing rules governing the law or armed conflict in Volume 1, which are supported by annotated state practice in Volume 2); J.M. Henckaerts, *Study on Customary International Humanitarian Law*, Annex, *available at* http://www.icrc.org/eng/assets/files/other/customary-law-rules.pdf (listing customary rules of international humanitarian law and designating which rules apply to IAC, NIAC, or both).

66. *See, e.g.*, von Heinegg, *supra* note 19, at 561 ("Some parts of the law of neutrality . . . become applicable in an international armed conflict only when and insofar as the belligerents resort to recognized methods and means by, for example, interfering with neutral shipping and aviation."); HUMANITARIAN POLICY & CONFLICT RESEARCH, *supra* note 21, at 305 ("The law of neutrality exclusively applies to Belligerent Parties, on the one side, and to Neutrals, on the other. Accordingly, Section X does not apply to non-international armed conflicts.").

guidance concerning the rights and duties with respect to cyber operations of both the belligerent state and states not involved in the NIAC.[67]

There is no clear analogy to the law of neutrality that specifically defines the interactions of states in a NIAC. There are, however, some principles that provide guidance to both belligerent and uninvolved states.

Article 2 of the UN Charter, which applies at all times, including a time of NIAC, essentially solidifies territorial sovereignty as one of the underlying principles of international law.[68] The Charter precludes the use of force against the territorial sovereignty of another state, especially in cases of purely domestic issues, except when initiated by the UN Security Council.[69] Therefore, a state involved in a NIAC would have to respect the territorial sovereignty of any other state, including states in which transnational terrorists or insurgent movements were harboured or at least not expelled. Of course, if the state was actually supporting or facilitating the insurgents, the NIAC might transform into an IAC, and the earlier discussion would be applicable.

There are also norms on state responsibility that preclude internationally wrongful acts and provide remedies in the case of injury or damage.[70] However, in the absence of something similar to the detailed LOAC provisions, there is limited guidance for what cyber actions would constitute a violation of a state's territorial sovereignty in a NIAC. Unlike the law of neutrality, which provides a fairly specific understanding of what states can and cannot do in neutral nations, there is no such clarity in a NIAC.

---

67. *See* SCHMITT, GARRAWAY & DINSTEIN, *supra* note 65 (containing thoughtful and extensive analysis on the laws applicable to the conduct of operations during a NIAC, but neither addressing the rights and duties of nonparticipants, nor the rights and duties of belligerent parties toward nonparticipants, analogous to the laws of neutrality during an IAC).

68. *See* U.N. Charter art. 2(4).

69. *See* U.N. Charter art. 2(7).

70. For example, the International Law Commission has proposed articles on state responsibility that are still in draft but are accepted by many states as restating customary international law. Rep. of the Int'l Law Comm'n, 53d sess, Apr. 23–June 1, July 2–Aug. 10, 2001, U.N. Doc. A/56/10 [hereinafter ILC 53d Report]; *see also* JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY 61–74 (2002).

The law applicable to uninvolved states is no clearer. Beginning early in the formulation of international law and becoming codified in a series of arbitrations and cases including the *Trail Smelter* arbitration[71] and the International Court of Justice's ("ICJ") *Corfu Channel* case,[72] the principle that a state cannot knowingly allow its territory to be used to the detriment of another state has become universally accepted. This is often referred to as the "no harm" principle and should be equally applicable to cyber operations in a NIAC.[73] This would mean that any state involved in a NIAC, and every state that is not a party to the NIAC, has an obligation to not allow its territory, including its cyber capabilities and infrastructure, to be used to harm another state.

While the law of neutrality applicable in IAC provides at least some definition on hostile acts and adds workable provisions on the use of public communications networks such as telephone and telegraph, simply precluding anything detrimental to another state lacks specificity sufficient to be a workable standard in the cyber context.

Perhaps most importantly, where the obligations of neutrality fell on all states involved in an IAC equally—whether neutral or belligerent—there is no such legal obligation upon the nonstate party to the NIAC. This leaves only the domestic laws of the various states to sort out the cyber actions of the nonstate participant in a NIAC, a situation that is highly problematic.

These difficulties can be illustrated by reviewing the "modified" scenario and attempting to determine the legality of nonstate Actor *G*'s actions.

C. *The Modified Scenario*

The scenario at the beginning of the Article set out a situation where State *G* was in an IAC with State *X* and took

---

71. Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1907 (1941).

72. The International Court of Justice ("ICJ") held that every state had an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States." Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

73. *See* Eric Talbot Jensen, *The International Law of Environmental Warfare: Active and Passive Damage During Times of Armed Conflict*, 38 VAND. J. TRANSNAT'L L. 145, 158–60 (2005).

certain cyber actions, involving parties and states that were not involved in the conflict but who were neutral. In the modified scenario, *G* is no longer a state but rather a nonstate actor—perhaps a transnational terrorist organization—and takes the same cyber actions against State *X* as part of an ongoing NIAC.

In the modified scenario, the first action taken is that an agent of nonstate actor *G* uses his tourist passport to lawfully enter neutral State *H*, carrying a cyber tool on a thumb drive. Once within *H*, *G*'s agent enters a cyber café and plugs the thumb drive into one of the computers. Upon activation, the malicious cyber tool is copied to the hard drive and establishes a beacon that then awaits contact by another tool.

When applying the laws of neutrality in an IAC, this action by the agent of State *G* is a violation of neutrality and therefore illegal; in a NIAC, there is no neutrality to violate. Because the agent is not an agent of a state, the UN Charter proscription on violating the territorial integrity of *H* is not implicated. Further, under the "no harm" principle, states are obligated to not knowingly allow their territory to be used to harm other states. Because the harm is done by a civilian member of a terrorist organization, there is no breach of the "no harm" principle, and State *H*'s legal response is likely limited to trying to capture the agent (if he is still in *H* or if *H* can get him through extradition if he is not) and apply *H*'s domestic criminal law response. As illustrated by the inability of the Philippines to prosecute the initiator of the "I Love You" malware, prosecution for the acts done by the agent of *G* may not even be possible in all states.[74]

Moving on in the scenario, soon after the previous event, another agent of *G* offers free thumb drives under the guise of a promotional gimmick from a local business to customers boarding a commercial cruise ship flagged in neutral State *M*, leaving from a port in neutral State *R*. Once the cruise ship entered the high seas, any customer who plugs the thumb drive into the ship's passenger computers will upload a malicious malware which then becomes resident on the ship's computer.

---

74. *See* MCCONNELL INT'L, CYBER CRIME . . . AND PUNISHMENT? ARCHAIC LAWS THREATEN GLOBAL INFORMATION 3–4 (2000), *available at* http://www. witsa. org/papers/McConnell-cybercrime.pdf.; Ann Harrison, *'Love Bug' Investigation Wrapping Up in Philippines*, COMPUTERWORLD, June 9, 2000, http://www.computerworld.com/s/article/45677/_Love_Bug_investigation_wrapping_up_in_Philippines.

The ship's computers connect to the Internet through a commercial carrier satellite operated by a company registered in neutral country *F*. Once the computer is connected with the Internet, the malicious malware on the ship's computer sends a signal across the Internet, seeking the beacon that is now resident on a computer in State *H*.

When the doctrine of neutrality applied because the conflict was an IAC, the agent's entrance into *R* and transport of the cyber weapon was a violation of *R*'s neutrality. As above with State *H*, this would not be the case here. The actions of *G*'s agent with respect to *R* would only be prosecutable if *R* had some domestic proscription to providing free thumb drives and if *R* could get jurisdiction for any potential criminal activity from the onboard actions of the passengers. Further, the use by State *G* of the neutral private ship's computer systems and the neutral commercial satellite system were also violations of the law of neutrality. Because these principles are based on the duties of states, the civilian agent of transnational terrorist group *G* is subject only to the domestic criminal laws of *M* and *F*, again assuming they can identify the agent and then gain custody in order to prosecute. As in the IAC scenario, the geographic location of the ship on the high seas removes any territorial claims of jurisdiction for the criminal acts, although other jurisdictional claims would still apply.

Finally, once the shipboard cyber tool has connected with the beacon on the computer in State *H*, a code is executed that sends a malicious cyber program to the beacon. Upon arrival at the computer in State *H*, it combines with the cyber tool at the beacon and creates cyber malware that is then forwarded to a computer in State *X* to which *G* has previously gained access. *G* gained access to the computer in State *X* by hiring a citizen of neutral State *J* to create an access for the specific malware that *G* created. Once the cyber malware reaches the computer in State *X*, it initiates an action that amounts to an attack on State *X* that causes death and destruction.

In the NIAC modified scenario, *J* is not a neutral and the hired citizen is merely a current resident of State *X*. He does not have any neutral protections to violate. He is most likely subject to the domestic law of *X* and can be prosecuted for any illegal

activity in which he participates. Hiring the civilian has no legal ramifications on *G*.

So, under the modified scenario, *G* as an organization is not legally constrained from taking any of the proposed actions. Further, in the case of the actions taken in States *H*, *R*, *M*, and *F*, members of *G* risk only the attenuated potential of criminal prosecution. *J*'s citizen who is working for *G* in State *X* also might be subject to criminal penalties.

III. *APPLYING THE PRINCIPLES OF NEUTRALITY TO CYBER OPERATIONS IN NON-INTERNATIONAL ARMED CONFLICTS*

For many who believe that domestic criminal law is the correct paradigm to deal with terrorism, the previous section will likely not raise many concerns. However, for those who want to create disincentives for terrorist organizations and other nonstate actors to use cyber activities to forward their ends, the lack of legal deterrence for the nonstate actor in the scenario will be troubling. Evolving the law to provide legal limitations on the actions of nonstate actors grounded in the LOAC should prove beneficial, if effectively accomplished.

In NIACs, where as a matter of definition the conflict is between a state bound by the LOAC and a nonstate actor who is not, international law creates an asymmetry that is likely to discourage lawfulness on the part of the nonstate actor. These groups, such as insurgent groups or terrorist organizations, who are almost always working at a logistical disadvantage because of a lack of resources and organization, will certainly see the lack of LOAC applicability to them as an advantage to be maximized.

In recent years, using the law to one's advantage during armed conflict has been termed "lawfare" and often implies illegal acts by a nonstate actor.[75] However, in the case of

75. *See* Charles J. Dunlap, Jr., *Is "LAWFARE" a Useful Term?: Does Lawfare Need an Apologia?*, 43 CASE W. RES. J. INT'L L. 121 (2010); Charles J. Dunlap, Jr., *Lawfare: A Decisive Element of 21st-Century Conflicts?*, 54 JOINT FORCE Q. 34 (2009), *available at* http:// www. dtic. mil/cgi-bin/GetTRDoc?AD=ADA515192&Location=U2&doc=GetTRDoc.pdf; Charles J. Dunlap, Jr., *Lawfare Today: A Perspective*, 3 YALE J. INT'L. AFF. 146, 146 (2008); Charles J. Dunlap, Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts* (Carr Ctr. for Human Rights, John F. Kennedy Sch. of Gov't, Harvard U., Working Paper, 2001), *available at* http://www.ksg.harvard.edu/cchrp/Web%20Working%20Papers/Use%20of%20Force/Dunlap2001.pdf.

applying neutrality in cyber conflict, the actions taken in the modified scenario above were not violations of the LOAC, even if some of them may have been violations of domestic law. Rather, it is the lack of applicable regulation in this area that encourages nonstate actors to take similar actions, knowing that the state they were engaging would have far more limited responses available to it to prevent or remedy the violation. For this reason, the law should be adapted to place legal constraints, such as the doctrine of neutrality, on nonstate actors in NIAC.

A. *The Benefits*

Applying the doctrines of neutrality to NIACs would have a number of benefits. First, it would level the playing field between parties to the conflict. Currently, states engaged in NIAC are also not bound by the doctrine of neutrality, but are bound by the doctrine of sovereignty and the UN Charter's preclusion of acts that violate another state's territorial integrity.[76] This legal limitation does not apply to nonstate actors and allows actions such as those in the modified scenario to occur. Having all parties bound by the same rules reduces the use of law as a weapon and adds to the predictability of actions within the conflict.

Additionally, applying the law of neutrality would add to the protections for states that are not involved in the NIAC. Requiring all parties, including nonstate actors, to refrain from taking any actions that were hostile to a party to the conflict from within a neutral state would provide neutral states with increased security and likely decrease the risk of escalation of the conflict through the actions of others.

Finally, giving nonparties the formal status of neutrals would also provide those states with another set of legal rights by which it could enforce its sovereignty. In other words, considering the modified scenario, turning the nonparty state into a neutral provides another legal paradigm (along with domestic criminal law) by which the nonparty state could prevent or punish the actions of both the nonstate actor and potentially the state party to the NIAC for cyber operations that violated its neutrality.

---

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

B. *The Process*

While these benefits would clearly advance the cause of international peace and security, they would only do so if parties were compliant. This is particularly difficult in the case of nonstate actors. As with all situations of lawfare, the problem is not only the law, but also seeking compliance.[77] Benefits would still accrue even if states only applied the doctrine of neutrality to NIACs. However, the real benefits of this initiative would be much greater if nonstate actors were also incentivized to comply.

Accomplishing the application of neutrality to NIACs would be difficult, but not insurmountable. The first step could be for states to make unilateral declarations that they would apply the law of neutrality to NIACs, not only binding them to apply the principles when they were involved in a NIAC, but also giving them the rights of neutrals toward NIACs in which they are not parties. At some future point, it might be useful to seek a formal treaty expanding the Hague Conventions to NIACs.

As part of the decision to apply the law of neutrality to NIACs, the international community would also have to determine methodologies to incentivize nonstate actors to commit themselves to the application of neutrality to the NIAC. Resolving this issue is an ongoing problem in international law and one that is beyond the scope of this Article. However, there are a number of scholars who have written on this issue and have proposed interesting ideas on how to pursue nonstate compliance.[78]

Some encouraging steps are already occurring. Nonstate actors are engaging in the legal process and voluntarily accepting obligations that they otherwise might not have.[79] This is a process that should be supported and expanded. It would

---

77. Jakob Kellenberger, President of the Int'l Comm. of the Red Cross, Speech on Strengthening Legal Protection for Victims of Armed Conflicts (Sept. 21, 2010), *available at* http:// www. icrc. org/eng/resources/documents/statement/ihl-development-statement-210910.htm.

78. *See, e.g.*, Anthea Roberts & Sandesh Sivakumaran, *Hybrid Sources of Law: Armed Groups and the Creation of International Law*, YALE J. INT'L L. (forthcoming).

79. *See id.* (detailing a number of recent statements and actions by nonstate organized armed groups indicating willingness and a commitment to voluntarily comply with the LOAC).

not only pave the way for the application of neutrality to NIAC, but also for the application of the LOAC more generally.

CONCLUSION

The doctrines of sovereignty and neutrality are some of the most difficult issues in cyber conflict due to the structure of the Internet and the protocols by which it operates, including the inability to direct the path over which Internet traffic travels. Cyber activities in general and cyber conflict in particular place stress on traditional LOAC notions, challenging both belligerent nations and neutral nations in the application of law to cyber operations. As cyber capabilities increase both at the national level and at the nonstate actor level, the principle of territorial sovereignty will come under increasing pressure, particularly during times of cyber conflict.

The current law of neutrality can continue to have meaning and provide clarity in the cyber age with few modifications and modernized understandings. For example, recognizing that Internet traffic that traverses the computer infrastructure of a neutral nation is not a violation of that nation's neutrality provides greater clarity to states planning cyber operations or desiring to maintain neutrality.

Additionally, applying neutrality to NIACs, where the traditional doctrine of neutrality is not currently applicable, would also prove extremely useful in preventing actions by both states and nonstate actors that might tend to escalate the conflict. Applying the law of neutrality to NIACs would provide nonparties to the NIAC an additional legal paradigm to prevent cyber actions within their territory. Admittedly, making neutrality apply as a matter of law would require actions by both states and nonstate actors, but these are not insurmountable difficulties.

The law of neutrality is still a binding legal doctrine in the cyber age and can have increasing utility by incorporating modern understandings of its applicability and by extending its coverage to parties and nonparties in NIACs.