LIEUTENANT COLONEL CHARLES C. POCHÉ, U.S. ARMY*

This Means War! (Maybe?)—Clarifying Casus Belli in Cyberspace

ABSTRACT

This paper argues current international legal norms and constructs do not adequately address what constitutes casus belli in the cyber domain. Consequently, an initiating state may unintentionally invite a responsive use of force through cyber actions it considers far short of

* Judge Advocate, U.S. Army. Presently assigned as Staff Judge Advocate, U.S. Army Maneuver Center of Excellence, Fort Benning, Georgia. Master of Strategic Studies, 2013, U.S. Army War College, Carlisle, Pennsylvania; LL.M., 2003, The Judge Advocate General's Legal Center and School, U.S. Army, Charlottesville, Virginia; J.D., 1999, University of Virginia School of Law, Charlottesville, Virginia; B.S., 1991, United States Military Academy, West Point, New York. Member of the bars of Virginia, U.S. Court of Appeals for the Armed Forces, and the Supreme Court of the United States. This Article was submitted in partial completion of the Master of Strategic Studies requirements of the 2013 U.S. Army War College Resident Course. The author would like to thank Commander John J. Patterson VI, U.S. Navy, and Colonel (Retired) Michael A. Marra, U.S. Air Force, for their invaluable assistance. The views expressed in this Article are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

the triggering threshold. Within the current ambiguity, however, the target state might consider those actions as well beyond that threshold. Such divergent viewpoints may result in open warfare between the two states. After applying emerging international analytical legal norms in two illustrative case studies, this paper recommends the United States adopt certain practices to reduce this dangerous ambiguity. These practices include more open acknowledgement of cyber actions and maintaining a clear separation between a state's cyber attack/defense and espionage functions. They also include asserting sovereign control over certain portions of the cyber domain, vigorously protecting those areas, and increasing the reporting of incidents.

> Of course, you realize, this means war!
>
> –Bugs Bunny[1]

When the long-eared hero of animation utters the above-borrowed[2] phrase or a similar one,[3] it is always in response to a provocation whose magnitude leaves no doubt concerning the appropriateness of a forceful response. The statement is declaratory and final. It invites no argument, because no argument is possible. The invariably clear casus belli—"an occurrence giving rise to or justifying war"[4]—by the offending character provides the required justification for the ensuing retaliatory mayhem.

This is entertaining and lighthearted in the imaginary context of cartoons, where no amount of force is ever permanently harmful or lethal. However, the requirement to identify adequately acts justifying a state's responsive use of force is a very real one with potentially lethal consequences. In stark contrast to the bright hues of cartoons, though, this analysis often occurs in a gray zone of uncertainty.

---

1 BULLY FOR BUGS (Warner Bros. 1953).

2 DUCK SOUP (Paramount Pictures 1933), *available at* http://movieclips.com/5xZ2y-duck-soup-movie-this-means-war/ (last visited June 9, 2013) (using the declarative, "This means war!" twice in the scene).

3 WET HARE (Warner Bros. 1962), *available at* http://www.youtube.com/watch?v=KvVyfgiN3ow (last visited June 9, 2013) (proclaiming, "Of course you know, this means war!"); *see also* A NIGHT AT THE OPERA (Metro-Goldwyn-Mayer 1935), *available at* http://www.youtube.com/watch?v=fvh1PdNJ2-8 (last visited June 9, 2013) (making the same declaration).

4 BLACK'S LAW DICTIONARY 247 (9th ed. 2009).

Nowhere is this uncertainty more prevalent than in the newest war fighting domain[5] of cyberspace.[6]

This paper argues current international legal norms and constructs do not adequately address what constitutes casus belli in the cyber domain. Consequently, an initiating state may unintentionally invite a responsive use of force through cyber actions it considers far short of the triggering threshold. Within the current ambiguity, however, the target state might consider those actions as well beyond that threshold. Such divergent viewpoints may result in open warfare between the two states.

This paper recommends the United States adopt certain practices to reduce this dangerous ambiguity. These practices include more open acknowledgement of cyber actions and maintaining a clear separation between a state's cyber attack/defense and espionage functions. They also include asserting sovereign control over certain portions of the cyber domain, vigorously protecting those areas, and increasing the reporting of cyber incidents.

The paper begins with an examination of the current norms concerning the use of force between states. It then details the emerging views concerning the application of these norms to the cyber domain. The paper goes on to apply these norms to the facts surrounding recently alleged state-level actions in the cyber domain. Based upon the conclusions drawn, the paper then presents recommendations for the United States to help remove some of the uncertainty surrounding assessments of cyber operations under international law.

---

5 U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5 (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf ("Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD's national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests.").

6 STEVEN A. HILDRETH, CONG. RESEARCH SERV., RL30735, CYBERWARFARE 1 (2001) ("Cyberspace is often used as a metaphor for describing the non-physical terrain created by computer systems. . . . Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse.").

I
USE OF FORCE AND INTERNATIONAL LAW

Since its adoption in 1945, the Charter of the United Nations (U.N.) has served as the aspirational framework for relations between states. That it has often failed to restrain the conduct of certain states does not make considering, in the words of Michael Walzer, "the precise meaning of the Charter . . . a kind of utopian quibbling."[7] To the contrary, its provisions and those of other customary international law, such as the Hague[8] and Geneva[9] conventions, have a very real effect. As Nye and Welch put it, "[S]uch rules put a burden of proof on those who break them."[10]

Indeed, the very reason for attempting to clarify casus belli in cyberspace is to provide a clear standard against which states may measure their own behavior and that of other states when initiating or responding to cyber actions. While states may use force to act on their interests in ways contrary to defined international norms, they do so at a cost to their legitimacy and prestige.[11] They also run the risk of drawing the collective ire of the international community, which may opt for group action to punish or to restore the status quo ante to ensure the offending state does not profit from its rule breaking.[12]

---

7 MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS xviii (3d ed. 2000).

8 Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulation Concerning the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, 205 Consol. T.S. 277.

9 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, T.I.A.S. No. 3362, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members, Aug. 12, 1949, T.I.A.S. No. 3363, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, T.I.A.S. No. 3364, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, T.I.A.S. No. 3365, 75 U.N.T.S. 267.

10 JOSEPH NYE & DAVID WELCH, UNDERSTANDING GLOBAL CONFLICT AND COOPERATION: AN INTRODUCTION TO THEORY AND HISTORY 25 (2011) ("Law and norms did not stop Saddam from invading Kuwait, but they did make it more difficult for him to recruit support, and they contributed to the creation of the coalition that expelled him from Kuwait.").

11 HANS MORGENTHAU, POLITICS AMONG NATIONS: THE STRUGGLE FOR POWER AND PEACE 80–81 (1985) ("Whatever the ultimate objectives of a nation's foreign policy, its prestige—its reputation for power—is always an important and sometimes a decisive factor in determining success or failure of its foreign policy. . . . Two factors make that triumph [of prestige] possible: reputation for unchallengeable power and *reputation for self-restraint in using it*.") (emphasis added).

12 *See* Thomas L. Friedman, *The Iraqi Invasion; Bush, Hinting Force, Declares Iraqi Assault 'Will Not Stand'; Proxy in Kuwait Issues Threat*, N.Y. TIMES, Aug. 6, 1990, *available at* http://www.nytimes.com/1990/08/06/world/iraqi-invasion-bush-hinting-force

Consequently, the first order question is, "What are the baseline rules?"

In Article 2, the U.N. Charter clearly removes the use of force from the repertoire of legitimate state actions in the normal course of international relations. It requires U.N. members to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[13] Recognizing, however, noncompliance by some states is possible (if not inevitable), the Charter details two currently relevant[14] circumstances when a responsive use of force is acceptable.

The first circumstance occurs when the U.N. Security Council determines "the existence of any threat to the peace, breach of the peace, or act of aggression"[15] and authorizes under Article 42 "such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."[16] Authorization for this type of action occurs only after careful deliberation. This mechanism is ill suited to match the speed at which cyber attacks can occur and at which an effective response must sometimes occur.[17] Of greater relevance to the cyber domain than this deliberative process is the Charter provision allowing acts in self-defense.

Article 51 of the U.N. Charter permits "individual or collective self-defense if an armed attack occurs against a Member."[18] In his volume, *Striking First*, Doyle characterizes this as "[t]he first and clearest case of just war. . . The country that is attacked and others

---

-declares-iraqi-assault-will-not-stand-proxy.html?pagewanted=all&src=pm (quoting President Bush, "'I view very seriously our determination to reverse this aggression. There are an awful lot of countries that are in total accord with what I've just said. We will be working with them all for collective action,' the President added. 'This will not stand. This will not stand, this aggression against Kuwait.'").

13 U.N. Charter art. 2, para. 4.

14 *Id*. art. 53, 107 (referencing in an obsolete manner an "enemy state" of World War II).

15 *Id*. art. 39.

16 *Id*. art. 42.

17 Chris Strohm, *Questions Unanswered in Pentagon Cyber Strategy*, NATIONAL JOURNAL DAILY A.M., July 14, 2011, *available at* ProQuest, Doc. No. 877037297 (quoting Deputy Defense Secretary William Lynn, "Lynn also acknowledged the woes of dealing with such high-paced threats. 'It's difficult because there's no real sovereignty in the Internet. It crosses borders. The effects of the actions on the Internet can take place in a matter of microseconds so there's no time to have a deputies meeting and decide how to react,' he added.").

18 U.N. Charter art. 51.

may join in the defensive war in order to repel, and perhaps also to punish, an unjust attacker."[19] This response need not await Security Council authorization, though states must apprise the Security Council of the exercise of the inherent right of self-defense. The Council may then take "such action as it deems necessary in order to maintain or restore international peace and security."[20]

Springing from this right of self-defense is the very narrow category of pre-emptive attack. In the words of Walzer, it is a "right recognized . . . in the legalist paradigm for international society." It holds "states can rightfully defend themselves against violence that is imminent but not actual; they can fire the first shots if they know themselves about to be attacked."[21] A commonly cited example of the application of this norm is Israel's attack to open the Six-Day War in 1967.[22]

Secretary of State Daniel Webster articulated the requirements for an acceptable preemptive attack during an exchange of letters with British authorities concerning the *Caroline* Case of 1837.[23] Secretary Webster asserted the requirement "to show a necessity of self-defence [sic], instant, overwhelming, leaving no choice of means, and no moment for deliberation." Additionally, the preempting attacker must do "nothing unreasonable or excessive; since the act justified by the necessity of self-defence [sic], must be limited by that necessity, and kept clearly within it."[24] The British agreed with Webster's assertions and they have become customary international law.

---

19 MICHAEL DOYLE, STRIKING FIRST: PREEMPTION AND PREVENTION IN INTERNATIONAL CONFLICT xiii (2008).

20 U.N. Charter art. 51.

21 WALZER, *supra* note 7, at 74.

22 *See also* DOYLE, *supra* note 19 at xiv (describing Israel's attack as "[a] classic example of justified preemptive war—at least in the judgment of many commentators"); *but see* JOE BARNES & RICHARD STOLL, PREEMPTIVE AND PREVENTIVE WAR: A PRELIMINARY TAXONOMY 13 (Mar. 2007), *available at* http://bakerinstitute.org /publications/Preemptive%20and%20Preventive%20War-1.pdf (arguing "the Israeli attacks of June 5 fall short of a strict definition of preemptive war" and "[t]hus, the Six-Day War contains elements of both preemption and prevention").

23 *See generally* Louis-Philippe Rouillard, *The Caroline Case: Anticipatory Self-Defence in Contemporary International Law*, 1 MISKOLC J. INT'L L. 104, 104–20, *available at* http://www.uni-miskolc.hu/~wwwdrint/20042rouillard1.htm#_ftn1 (providing a detailed background of the case).

24 *See generally* THE AVALON PROJECT: DOCUMENTS IN LAW, HISTORY, AND DIPLOMACY, BRITISH-AMERICAN DIPLOMACY: THE CAROLINE CASE (2008), *available at* http://avalon.law.yale.edu/19th_century/br-1842d.asp (providing the full text of the exchange of letters between Secretary Webster and Lord Ashburton of Great Britain).

In his work, Walzer questions whether the right to anticipatory self-defense articulated in the *Caroline* rules "has any substance at all."[25] As he puts it, the right allows one "to do little more than respond to an attack once we had seen it coming but before we felt its impact. Pre-emption on this view is like a reflex action, a throwing up of one's arms at the very last minute."[26] Walzer does not see this as a useful right because "[t]here is often plenty of time for deliberation" which makes 'Webster's reflex' unnecessary.[27]

To be fair, Walzer is not specifically addressing cyber actions in his analysis. However, whatever the relative merits of "Webster's reflex" are in the conventional war fighting domains, it appears exceptionally appropriate in the cyber domain. In fact, Webster's 175-year-old formulation provides succinct, well established, and recognized international law authority for the concept of active defense discussed later.

II
GENERAL APPLICATION OF INTERNATIONAL LAW TO CYBERSPACE

Having laid out the most relevant customary norms justifying a state's resort to force, it is appropriate to examine the general applicability of these norms to the cyber domain. The International Court of Justice (ICJ) has stated the self-defense provisions of Article 51 of the Charter, as well as Security Council enforcement measures under Article 42, "apply to any use of force, regardless of the weapons employed."[28] On its face, this brings cyber actions within the scope of the Charter.

Additionally, it is U.S. policy to apply existing international norms in cyberspace. The White House's *International Strategy for Cyberspace* states, "[C]yberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state

25 WALZER, *supra* note 7, at 74.

26 *Id.* at 74–75.

27 *Id.* at 75.

28 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

behavior—in times of peace and conflict—also apply in cyberspace."[29]

While the overall applicability of these norms is certainly not in doubt from a U.S. perspective,[30] how to apply them is much less settled. It is far from obvious how the standards of the *Caroline* case and the U.N. Charter, formulated before the widespread use of electricity and electronics, respectively, factually apply to acts in the cyber domain. In the words of one author, "In fact, the entire field of international cyber law is still murky."[31] This uncertainty provides the very concerning risk of miscalculation this paper seeks to address.

III
THE TALLINN MANUAL AND CYBER WARFARE

A substantial first step towards lifting some of this fog occurred in March 2013 with the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* [hereinafter the Tallinn Manual].[32] The Tallinn Manual represents an attempt by a group of nineteen international experts "to produce a non-binding document applying existing law to cyber warfare."[33] The experts involved adopted the rules of the Tallinn Manual by "employing the principle of consensus."[34] While the authors admit "any claim that

29 BARACK OBAMA, INTERNATIONAL STRATEGY FOR CYBERSPACE 9 (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf ("The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace.").

30 Harold Hongju Koh, Legal Advisor to the U.S. Dep't of State, Address at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm (stating, "Question 1: Do established principles of international law apply to cyberspace? Answer 1: Yes, international law principles do apply in cyberspace. Everyone here knows how cyberspace opens up a host of novel and extremely difficult legal issues. But on this key question, this answer has been apparent, at least as far as the U.S. Government has been concerned. Significantly, this view has not necessarily been universal in the international community. At least one country has questioned whether existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace. But the United States has made clear our view that established principles of international law do apply in cyberspace.").

31 JEFFREY CARR, INSIDE CYBER WARFARE 31 (2010).

32 MICHAEL N. SCHMITT ET AL., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013) [hereinafter THE TALLINN MANUAL].

33 *Id.* at 16.

34 *Id.* at 19.

every assertion in the Tallinn Manual represents an incontrovertible restatement of international law would be an exaggeration,"[35] it carries sufficient persuasive force to warrant its use.

Indeed, given the accepted methods of determining international law on a particular subject, the Tallinn Manual may be the only available cyber warfare source for the near future. Article 38 of the Statute of the International Court of Justice [hereinafter ICJ] details the generally accepted sources of international law. These include international conventions, international custom, general principles of law, as well as the subsidiary means of "judicial decisions and the teachings of the most highly qualified publicists of the various nations."[36]

Applying these sources to cyber warfare, one quickly exhausts the list. There currently are no applicable international conventions or treaties.[37] Cyber warfare is a relatively new state capacity and customs emerge slowly (over decades, not years). General principles of law may be timeless, but they still require expert application. There are not yet any international judicial decisions on the topic. This leaves only the subsidiary means of highly qualified publicists as a currently available source. Consequently, the Rules and Commentary of the Tallinn Manual may be the best available lens through which to view the application of current international norms to the cyber domain.

As an initial matter, it is important to understand the general nature of the international legal environment. The *Lotus* case provides a succinct statement of the two overarching behavioral norms with which states comply. One is permissive, while the other is restrictive. First, "under international law everything which is not prohibited is permitted." Second, "[F]ailing the existence of a permissive rule to the contrary[, a state] may not exercise its power in any form in the territory of another."[38] The U.N. Charter harkens to these norms in its regulation of hostilities between states.

---

35 *Id*.

36 Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 1031.

37 Lawrence J. Muir, Jr., *The Case Against an International Cyber Warfare Convention*, 2 WAKE FOREST L. REV. ONLINE 5, 5 (2011) http://wakeforestlawreview.com/the-case-against-an-international-cyber-warfare-convention. ("Over the past five years, a number of academic articles have called for the creation of an international convention to govern the rules, rights, and responsibilities of nations in cyber warfare and information operations.")

38 The Case of the S.S. Lotus, Judgment (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 21 and 11 (Sept. 7), *available at* http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm (The first norm appears as a paraphrase in the dissent of M. Loder. The

As previously stated, Article 2 prohibits the "threat or use of force," removing those acts from the spectrum of unregulated state behavior. However, absent some other prohibition, actions below the use of force threshold are permissible under international law. The self-defense clause of Article 51 is a permissive rule suspending the previous prohibition in response to an "armed attack." Consequently, "use of force" describes what a state must refrain from doing until an "armed attack" occurs. Defining these two terms for the cyber domain is essential for avoiding state miscalculations.

In its Rule 11, the Tallinn Manual defines a cyber operation as "a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[39] On its face, this is not a very satisfying definition, as it uses the term "use of force" to define a cyber use of force. This would be less troubling if non-cyber "use of force" was well defined. Unfortunately, it is not. The Tallinn Manual acknowledges, "There is no authoritative definition of, or criteria for . . . 'use of force.'"[40]

Despite this shortcoming, the definition is not a nullity. It at least informs us the rules for the use of force in the cyber domain are no different from that of any other domain. Additionally, the term "scale and effects" carries some meaning. It appears in the ICJ's decision in the *Nicaragua* case. In this case, the ICJ held an act done by a proxy might constitute an armed attack by the sending state if its "scale and effects" would classify it as an armed attack if done by a state's regular armed forces.[41]

It is important to note the ICJ was addressing "armed attack," not "use of force." The drafters of the Tallinn Manual forthrightly acknowledge their intentional expansion of the term's application. They state, "[T]he Experts found the focus on scale and effects to be

---

actual holding of the case states, "The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.").

39 THE TALLINN MANUAL, *supra* note 32, at 47.

40 *Id*.

41 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 103 (June 27) [hereinafter The Nicaragua Case] ("The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.").

an equally useful approach when distinguishing acts that qualify as uses of force from those that do not."[42]

This equality of approaches, however, does not make "armed attack" and "use of force" terms that possess a distinction without a difference.[43] The ICJ makes this clear when it states, "[i]t will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[44] As Michael Schmitt so aptly puts it, "[i]n other words, whereas all armed attacks are uses of force, not all uses of force are armed attacks."[45] This is significant, as only an armed attack triggers the right to self-defense under Article 51 of the U.N. Charter.

The drafters of the Tallinn Manual were unanimous in their determination "some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack.'"[46] In defining "armed attack," the Tallinn Manual again calls upon the "scale and effects" language. Rule 13 states, "Whether a cyber operation constitutes an armed attack depends upon its scale and effects."[47]

If one uses the same "scales and effects" analysis for determining both "use of force" and "armed attack," it is worthwhile to define the threshold at which a use of force transitions into an armed attack. The Tallinn Manual characterizes this point as "unsettled" and "unclear."[48] Unfortunately, the Tallinn Manual provides little additional clarity and may actually confuse this issue further.

In discussing the armed attack threshold, the Tallinn Manual holds "some cases are clear."[49] The drafters "agreed that any use of force that injures or kills persons or damages or destroys property would satisfy the scale and effects requirement."[50] This seems to set a bright line rule. However, in the next comment, the Tallinn Manual removes this apparent clarity by stating, "[t]he law is unclear as to the precise point at which the extent of death, injury, damage, destruction, or

---

42 THE TALLINN MANUAL, *supra* note 32, at 47.

43 *But see* Abraham D. Sofaer, *International Law and the Use of Force*, 82 AM. SOC'Y OF INT'L L. PROC. 420, 422 (1988).

44 The Nicaragua Case, *supra* note 41, at 101.

45 Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13, 22 (2012).

46 THE TALLINN MANUAL, *supra* note 32, at 54.

47 *Id*. at 53.

48 *Id*. at 55.

49 *Id*.

50 *Id*.

suffering caused by a cyber operation fails to qualify as an armed attack."[51] It is difficult to discern how death, injury, damage, and destruction can both satisfy the scales and effects requirement and fail to qualify as an armed attack.

Beyond this one instance of confusion, the Tallinn Manual's inability to provide bright-line rules is understandable. After all, states have wrestled with the application of these terms to non-cyber activities for well over half a century and precise definitions are still elusive. Rather than fault the Tallinn Manual for failing to provide what may be impossible to provide, it is better to focus on what it does provide. It presents a compelling list of factors states "are likely to consider . . . when deciding whether to characterize any operation, including a cyber operation, as a use of force"[52] and, by extension, a possible armed attack.

IV
FACTORS FOR ASSESSING USE OF FORCE IN CYBERSPACE

The primary factors laid out by the Tallinn Manual are severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.[53] This is admittedly a non-exhaustive list.[54] Nonetheless, it provides a useful framework for analysis. A brief explanation of each primary factor is a necessary precursor for future application. It is helpful to categorize these factors under the headings of who, what, where, when, and how.

Both state involvement and military character address the question of "who." For state involvement, "[t]he clearer and closer a nexus between a State and cyber operations, the more likely" other states will see it as a use of force by the originating state.[55] Military character raises the question of "whom" both in terms of the originator and the target. If either are military forces, it "heightens the likelihood of characterization as a use of force."[56]

The first aspect of the question of "what" is perhaps the most obvious. What actually happened because of the cyber operation? The

---

51 *Id*.

52 *Id*. at 49 (drawing heavily upon the work of Michael N. Schmitt, *Computer Network and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914 (1999).

53 *Id*. at 49–52.

54 *Id*. at 52.

55 *Id*.

56 *Id*. at 51.

concept of severity addresses this question and holds the distinction of being "[s]elf-evidently the most significant factor in the analysis." Unless de minimis, any act "involving physical harm to individuals or property" will likely qualify as a use of force.[57] The question of "what" is also applicable to an analysis of presumptive legality. What kind of operation was it? Recall that absent a prohibition, acts in the international realm are presumptively legal. This includes such negative actions as "propaganda, psychological operations, espionage, or mere economic pressure," all of which are less likely rise to the level of a use of force.[58]

The question of "where" seems to be a strange fit in a domain with no physical boundaries. However, it does matter where in cyberspace the attack occurs and where the physical effects occur. The concept of invasiveness covers this question. "As a rule, the more secure a targeted cyber system, the greater the concern as to its penetration."[59] Operations against a highly classified military network are much more likely a use of force than those targeting commercial websites. Additionally, if the effects "are limited to a particular State," it increases the perceived invasiveness of those operations."[60] If either of these conditions are true, it raises the likelihood a cyber action constitutes a use of force.

The temporal question of "when" addresses the factor of immediacy. Immediacy holds that states are more likely to categorize "a cyber operation that produces immediate results as a use of force." This is due to the decreased window of opportunity to "seek a peaceful accommodation" or prevent the "harmful effects." Attacks that "take weeks or months to achieve their intended effects" are less likely in the use of force category.[61]

While immediacy addresses the timing of causation, "directness examines the chain of causation."[62] This is a question of "how" the cyber operation causes the effect. The more directly linked the cause and effect, the more likely the cyber action is a use of force.[63] The second aspect of the "how" question addresses measurability, as in "How bad was it?" It is easier "to characterize actions as a use of

57 *Id*. at 49.
58 *Id*. at 52.
59 *Id*. at 50.
60 *Id*.
61 *Id*.
62 *Id*.
63 *Id*.

force when the consequences are apparent." Having "quantifiable and identifiable" consequences, such as "amount of data corrupted, percentage of servers disabled, number of confidential files extracted," makes it more likely the operation will appear to be a use of force.[64]

V
APPLYING THE FACTORS

Having laid out the assessment factors proposed by the Tallinn Manual, it is illuminating to test their utility by applying them to actual cyber events. This paper uses two case studies. The first is the 2007 wave of cyber attacks aimed at Estonia, and the second is the Stuxnet malware attack in Iran made public in 2010.

A. Estonia—The Cyberwar That Wasn't

On 27 April 2007, a wave of distributed denial of service attacks[65] hit various websites in Estonia. Affected sites included those of "the president, parliament, ministries, political parties, major news outlets, and Estonia's two dominant banks."[66] The apparent precipitation of the attacks was the "decision to move a Soviet-era war memorial."[67] Some attacked sites were "defaced to redirect users to images of Soviet soldiers."[68] The attacks occurred during a time of protest riots

64 *Id*. at 51.

65 U.S. Computer Emergency Readiness Team, *Understanding Denial-of-Service Attacks* (Nov. 4, 2009), http://www.us-cert.gov/cas/tips/ST04-015.html (defining a denial-of-service attack as follows: "In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. . . . The most common and obvious type of DoS attack occurs when an attacker 'floods' a network with information. . . . The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a 'denial of service' because you can't access that site. . . . In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is 'distributed' because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.").

66 Johnny Ryan, *"iWar": A New Threat, Its Convenience–and Our Increasing Vulnerability*," NATO REV., Winter 2007, http://www.nato.int/docu/review/2007 /issue4 /English/analysis2.html.

67 *War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?* THE ECONOMIST July 1, 2010, http://www.economist.com/node/16478792.

68 Patrick Jackson, *The Cyber Raiders Hitting Estonia*, BBC NEWS, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665195.stm.

by ethnic Russian Estonians.[69] The attacks continued for over a month and, at times, included up to 100,000 networked machines bombarding the targeted sites.[70]

The Estonian response was to circle the wagons to fend off the attacks by closing down external server access, while attempting to continue to allow access by Estonian users. The head of information technology at the Estonian defense ministry stated the country was very dependent upon the internet due to the country's "paperless government" and web-based banking. In his words, "If these services are made slower, we of course lose economically."[71]

At the time, Estonia believed the Russian government was behind the attacks,[72] partially because the list of alleged offenders includes internet addresses "in the Russian government and presidential administration."[73] A Kremlin spokesman characterized the allegations as "completely untrue"[74] and stated an internet address "does not mean foreign governments are behind these attacks. Moreover, as you probably know, IP addresses can be fake."[75]

Concurrently, one Russian internet pioneer indicated there was "no reason to believe in Russian state involvement" beyond that of "Russian state propaganda" fueling "anti-Estonian sentiments."[76] A member of "a pro-Kremlin youth group" stated "he personally took part in cyber-attacks . . . [although] he denied that Moscow state offices were used."[77] Eventually, a 20-year-old ethnic Russian Estonian student was the first convicted and fined for participation in the attack. Prosecutors claimed the attack was an act of protest.[78]

One commentator characterized this incident as "more a cyber-riot than a war."[79] The below application of the Tallinn Manual's assessment factors supports this view. Very few of the factors, if any,

---

69 *Estonia Fines Man for "Cyber War,"* BBC NEWS, Jan. 25, 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm.

70 Ryan, *supra* note 66.

71 Jackson, *supra* note 68.

72 BBC NEWS, *supra* note 69.

73 Jackson, *supra* note 68.

74 BBC NEWS, *supra* note 69.

75 Jackson, *supra* note 68.

76 *Id*.

77 Victor Yasmann, *Monument Dispute With Estonia Gets Dirty*, RADIO FREE EUROPE RADIO LIBERTY, May 8, 2007, http://www.rferl.org/content/article/1347550.html.

78 BBC NEWS, *supra* note 69.

79 THE ECONOMIST, *supra* note 67.

weigh in favor of considering this incident a use of force, much less an armed attack.

Applying the questions of "who" to this case illustrates what one commentator has deemed the "single greatest challenge to the application of the law of armed conflict to cyber activity"[80]—that of attribution. As the Kremlin spokesman pointed out above, even the use of government originating addresses does not necessarily mean state involvement. Despite initial concerns, the eventual conviction in this case indicates state involvement was not a factor. Likewise, the attack also lacked a military character. There was no specific targeting of Estonian military capabilities, nor was there any indication of Russian military involvement in the attacks.

Answers to the questions of "what" also weigh against considering this a use of force. Despite the massive inconvenience, the attacks do not appear to have caused any physical harm or damage. The attacks lacked the severity necessary to cross the threshold of a use of force. Additionally, while the eventual conviction clearly indicates a violation of Estonian domestic law occurred, it is unclear the attacks violated any international legal norms. Even if Russia's spread of propaganda fueled the attacks, such spreading of propaganda is a presumptively legal act in the international context.

The question of "where" harkens to the invasiveness of the attack. While it is true the attacks were largely limited to Estonian sites, indicating a state-defined target set, they did not appear to target classified or secure networks. Even the government sites attacked were informational sites generally open to the public. No specialized access was necessary to reach these networks. Doors that are open to the public carry the risk of admitting unhappy members of that public.

The effects of the attack also lacked the immediacy that would support characterizing the attack as a use of force. Examining the question of "when" makes it apparent Estonia had time to react and mitigate the effects of the attacks. During the month-long duration of the attacks, Estonia had time to lodge protests and take the protective measure of closing its sites to requests originating outside of Estonia.

The use of force analysis for the attacks also fails on the question of "how." Although Estonia perhaps did "lose economically," the attacks lacked directness. The attacks did not actually destroy financial records or economic capacity. Instead, they simply made

---

80 Todd C. Huntley, *Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1, 34 (2010).

regular financial transactions more difficult. It is also difficult to assign a monetary figure to this loss of convenience. This causes the attacks also to fail in the measurability analysis.

The above analysis of the 2007 cyber attacks on Estonia using the factors proposed by the Tallinn Manual indicate any characterization of these attacks as cyber "warfare" is overblown. The attacks and their effects fail in nearly every instance to demonstrate the proposed characteristics of a use of force. Interestingly, however, the primary author of the Tallinn Manual's factors appears to reach a different conclusion. In his analysis, "[t]aken together as a single 'cyber operation,' the incident arguably reached the use-of-force threshold."[81]

This difference of opinion does not invalidate the analytic approach, but it does highlight the subjective and often uncertain nature of its outcome. In many cases, reasonable people may reach differing conclusions. The 2010 Stuxnet malware attack in Iran, however, is a much clearer case.

B. Iran—A Likely Cyberwar Salvo

In late 2009 or early 2010, Iran replaced approximately 1,000 of the centrifuges at its primary nuclear enrichment facility at Natanz, "implying that these centrifuges broke."[82] About that same time, however, a sophisticated piece of computer malware appeared "loose on the Internet"[83] and drew the attention of computer security experts. They christened the malware "Stuxnet."[84] In November of 2010, Iranian President Ahmadinejad confirmed the cause of Iran's centrifuge problems was some type of cyber attack. In his words,

---

81 Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILLANOVA L. REV. 569, 577 (2011).

82 David Albright, Paul Brannan & Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY REPORT 1 (Dec. 22, 2010), *available at* http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

83 Ellen Nakashima & Joby Warrick, *Stuxnet was Work of U.S. and Israeli Experts, Officials Say*, WASHINGTON POST ONLINE (June 1, 2012), http://articles.washingtonpost.com/2012-06-01/world/35459494_1_nuclear-program-stuxnet-senior-iranian-officials.

84 David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES ONLINE (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

someone "succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts."[85]

The Symantec computer security company characterizes Stuxnet as "a large, complex piece of malware . . . primarily written to target an industrial control system [ICS] or set of similar systems."[86] It does so by modifying the ICS's "programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment."[87] The malware is very precise in its targeting.

Stuxnet "covertly changes the frequencies of certain types of frequency converters, which control the speed of motors." Its intended targets are components associated with Iran's centrifuges.[88] Stuxnet ultimately causes the centrifuges to rotate out of their designed tolerances. Such rotations "could destroy large numbers of centrifuges."[89] As early as 2008, the malware was apparently active at Natanz and causing centrifuges to spin "at faster-than-normal speeds until sensitive components began to warp and break."[90] A third version of Stuxnet, implemented shortly after the outside detection of the malware, caused the destruction of the 1,000 centrifuges.[91]

The computer security community did eventually determine the software's functioning and specific targeting of Iranian enrichment processes.[92] However, it "came to no conclusions about who was responsible,"[93] even after Symantec reported the location of two "command and control servers" in Malaysia and Denmark.[94] Symantec did note, however, "Stuxnet is of such great complexity—

---

85 *Update 2–Iran Says Cyber Foes Caused Centrifuge Problems*, REUTERS (Nov. 29, 2010), http://www.reuters.com/article/2010/11/29/iran-ahmadinejad-computers-idAFLDE6AS1L120101129.

86 Nicolas Falliere, Liam O. Murchu & Eric Chien, *W32.Stuxnet Dossier*, SYMANTEC SECURITY RESPONSE 1 (Feb. 2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

87 *Id*.

88 Albright, Brannan & Walrond, *supra* note 82, at 1.

89 *Id*. at 4.

90 Nakashima & Warrick, *supra* note 83.

91 *Cyberattacks on Iran—Stuxnet and Flame*, N.Y. TIMES, Aug. 9, 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html.

92 Kim Zetter, *Report: Obama Ordered Stuxnet to Continue After Bug Caused It to Spread Wildly*, WIRED (June 1, 2012), http://www.wired.com/threatlevel/2012/06/obama-ordered-stuxnet-continued/.

93 N.Y. TIMES, *supra* note 91.

94 Falliere, Murchu & Chien, *supra* note 86, at 21.

requiring significant resources to develop—that few attackers will be capable of producing a similar threat . . . ."[95]

Although no government has openly acknowledged responsibility, subsequent news reporting based upon "leaks" in the U.S. government provides a possibility. According to news reports, the U.S. National Security Agency (NSA) developed the malware with the help of Israel as part of a classified effort code-named Olympic Games.[96] The operation "was geared toward damaging Iran's nuclear capability gradually while sowing confusion among Iranian scientists about the cause of mishaps at a nuclear plant."[97] The U.S. Central Intelligence Agency (CIA) and Israelis handled the problem of getting the software into the system. Because the plant's equipment was not attached to the internet, emplacing the software "depended on spies and unwitting accomplices" to connect an infected device to the system.[98]

The spread of the malware outside the Natanz system may have been the result of a coding error. However, as a testament to the targeting specificity of the malware, there was no damage resulting from the more than 100,000 computers unintentionally infected outside the plant.[99] The effects inside the Natanz facility, however, were significant. As one reporter noted, "Stuxnet appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives."[100]

Based upon the above facts, one cyber-expert opined, "Effectively the United States has gone to war with Iran and has chosen to do so in this manner because the effects can justify this means."[101] Could Iran consider this effort by the United States and Israel to be an armed attack justifying the use of force in self-defense? An application of the assessment factors proposed by the Tallinn Manual indicates such a conclusion is not only possible, but almost a certainty.

---

95 *Id*. at 55.

96 Nakashima & Warrick, *supra* note 83.

97 *Id*.

98 *Id*.

99 Zetter, *supra* note 92.

100 N.Y. TIMES, *supra* note 91.

101 Nakashima & Warrick, *supra* note 83.

Both the state involvement and military character aspects of the question of "who" in this case point towards the legitimacy of considering this an armed attack. Poor U.S. security in leaking the potential identity of the malware's originator may have solved the technical attribution problem. The importance of this cannot be overstated. Given the primacy of state action under international law, one frequent expert commentator was certainly correct when he noted, "the identity of the attacker may well determine if a state of war exists."[102] If other states assume the accuracy of public news stories not disavowed by the governments concerned, the creation and insertion of the malware were acts of state involvement by the United States and Israel.

The "who" issue of the military character of the attack is a slightly closer question. The U.S. agencies allegedly involved were the NSA and CIA. These are not technically military organizations. However, the CIA does sometimes go beyond strict espionage by taking a more direct role in hostilities. For example, a CIA-led military operation was largely responsible for the destruction of the Taliban regime in Afghanistan.[103] Given this, it is likely other nations would consider the CIA at least a paramilitary arm of the United States.

The target was also of a quasi-military character. Iran claims its uranium enrichment efforts are for peaceful purposes. However, the international community believes its true aim to be military—the development of nuclear weapons. A weapons-development program is more military than civil in nature. While it is not an unequivocal determination, the facts of this case weigh in favor of answering "yes" to whether the attack's origin and target possess a military character.

The answers to the questions of "what" are clearer determinations. When examining severity, acts causing physical harm cross the threshold as a use of force. Physical harm includes harm to property. The destruction of the centrifuges to necessitate their replacement meets this requirement. The attack also fails to qualify as an act of presumptive legality. Had the "spies and unwitting accomplices" only inserted information-gathering tools, this would have been an act of simple espionage presumed legal under international law. However,

---

102 Charles J. Dunlap, Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, 5 STRATEGIC STUD. Q. 81, 88 (2011), *available at* http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf.

103 *See* GARY C. SCHROEN, FIRST IN: AN INSIDER'S ACCOUNT OF HOW THE CIA SPEARHEADED THE WAR ON TERROR IN AFGHANISTAN (2005).

the aim was to produce destructive results akin to bombing or planting explosives. This nullifies any presumptive legality argument.

Turning to the question of "where," it is clear the attack was highly invasive. Given its nature, the Natanz facility is likely one of Iran's most secure facilities. The lack of connectivity between its systems and the internet supports this assessment. Additionally, the malware was highly engineered to target only specific components at this specific plant. Even when it unintentionally spread outside the plant, it had no real effects. The highly secure nature of the plant and the extreme specificity of the targeting both place the attack at the high end of the invasiveness scale.

The aspect of immediacy associated with the question of "when" is more complex. The first version of the malware apparently ran for months without causing alarm. The program, as designed, obscured the nature of the centrifuge failures in an attempt to damage Iran's capability gradually. This approach lacked immediacy.

Despite this lack of immediacy, however, the malware eventually gained outside notice. Perhaps fearful the Iranians would piece things together and close the window of opportunity, the attackers introduced a newer variant that caused the abrupt destruction of 1,000 centrifuges. This newer variant possessed the immediacy the original version lacked. Its entire purpose was to cause its effects before the Iranians could react to mitigate the harm.

Turning to the final question of "how," the attack appears to have both the requisite characteristics of directness and measurability. It is clear the malware's manipulation of the frequency controllers initiated the short chain of causation that led to the centrifuge failures. The 1,000 simultaneous failures are otherwise difficult to explain. Those same 1,000 failures are a distinctly measureable result one can attribute to the attack.

Given the above analysis, the consideration by "many experts" of Stuxnet as "the first cyber weapon in history" appears valid.[104] To call it a "State sponsored attack" aimed at "the critical infrastructures of a foreign country with the specific intent to destroy them" [105] is not an exaggeration. The operation possesses all of the characteristics suggested by the Tallinn Manual as indicators of a use of force, if not

---

104 Pierluigi Paganini, *The Rise of Cyber Weapons and Relative Impact on Cyberspace*, INFOSEC INSTITUTE RESOURCES (Oct. 5, 2012), http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/.

105 *Id.*

an armed attack, under international law. Although Iran cannot currently speak from a position of moral authority regarding international norms, it would appear justified in raising a complaint regarding this incident.

VI
RECOMMENDATIONS FOR INCREASING CYBERSPACE CLARITY

The two above case studies fall in at the opposing ends of the spectrum of analysis using the assessment factors proposed by the Tallinn Manual. The cyber attack on Estonia arguably possesses practically none of the characteristics of a use of force, while the attack on Iran demonstrates nearly all of them. It is fair to surmise future incidents will likely fall somewhere between these two extremes.

Applying a balancing test will be necessary in instances where some factors support the characterization of a use of force, while others mitigate against it. There is always a level of ambiguity associated with such analysis. Because the outcome of the analysis may provide justification under international law to go to war, it is in the interest of states to remove as much ambiguity as possible. The United States can lead this effort by taking a number of actions, both in the offensive and defensive contexts.

A. On the Offense

First, in the offense, the United States should demonstrate "secrecy" and "cyber" are not synonymous when it comes to state involvement. The United States does not have a history of launching surprise attacks and has an aversion to doing so. It was Robert Kennedy's likening a surprise invasion of Cuba to Pearl Harbor that "discredit[ed] the hawks" and enabled the "more prudent approach" of a naval quarantine during the Cuban Missile Crisis.[106] In this same vein, a non-attributable "cyber sneak attack" with widespread effects against another state appears distinctly un-American.

However, the United States may enjoy a significant technological advantage in the cyber domain that it has every right to exploit. The United States may choose to use cyber methods in self-defense or as an offensive use of force during already ongoing hostilities. When it

106 Mark White, *Robert Kennedy and the Cuban Missile Crisis: A Reinterpretation*, AMERICAN DIPLOMACY (Sept. 2007), http://www.unc.edu/depts/diplomat/item/2007/0709/whit/white_rfk.html.

does so, it should not attempt to mask the origin of these cyber actions and should take responsibility for them.

All U.S. weapons, including cyber weapons, undergo two legal reviews. As an initial matter, an examination ensures the weapon is not per se contrary to international legal norms before it even enters the U.S. weapons inventory.[107] Afterwards, any significant employment of the system undergoes another review to determine whether the intended use also complies with international law.[108] This prevents the use of otherwise legal weapons in illegal ways.

Cyber weapons undergo this same legal analysis.[109] If they pass, there is no reason to mask their use. The United States should be as hesitant to do so as it would be to send its regular forces into combat lacking the "fixed distinctive emblem recognizable at a distance"[110] embodied in their uniforms. Failure to take ownership of cyber attacks risks the target state responding too broadly and drawing others into the conflict. Additionally, if there is a question of the appropriateness of a cyber action, acknowledgement of that action allows target states recourse to international bodies that settle such disputes. This allows the building of a body of law and state practice that clarifies what is appropriate.

---

107 U.S. DEP'T OF DEF., DEP'T OF DEF. DIRECTIVE 5000.01, THE DEFENSE ACQUISITION at E1.1.15 SYSTEM (2003), *available at* http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf ("Legal Compliance. The acquisition and procurement of DoD weapons and weapon systems shall be consistent with all applicable domestic law and treaties and international agreements . . . , customary international law, and the law of armed conflict (also known as the laws and customs of war). An attorney authorized to conduct such legal reviews in the Department shall conduct the legal review of the intended acquisition of weapons or weapons systems.").

108 U.S. DEP'T OF DEF., DEP'T OF DEF. DIRECTIVE 2311.01E, DOD LAW OF WAR PROGRAM (2010), at 5.7.3, *available at* http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf ("The Heads of the DoD Components shall . . . [m]ake qualified legal advisers at all levels of command available to provide advice about law of war compliance during planning and execution of exercises and operations.").

109 *See, e.g.*, U.S. DEP'T OF THE AIR FORCE, AIR FORCE INSTRUCTION 51-402, LEGAL REVIEWS OF WEAPONS AND CYBER CAPABILITIES 1.6.2 (2011), *available at* http://www.fas.org/irp/doddir/usaf/afi51-402.pdf ("Ensure commanders/directors of Air Force components engaged in cyberspace operations provide their [Staff Judge Advocate] all the information required to accomplish a thorough and accurate legal review of each new or modified cyber capability.").

110 Convention (IV) Respecting the Laws and Customs of War on Land and its Annex, *supra* note 8, at art. 1 (requiring the "emblem" to qualify as a belligerent); *see also* Geneva Convention Relative to the Treatment of Prisoners of War, *supra* note 9, at art.4. (requiring the same "sign" to qualify as a prisoner of war, if captured).

This recommendation holds well for openly conducted conflicts. The Iran attack demonstrates, however, that states sometimes determine their interests require surreptitious actions. It would be Pollyannaish to assume this never happens or that one can prevent it from happening. In such cases, state involvement is still a significant issue. Should the non-attribution fail, the target state may have a legitimate recourse to open warfare. The gravity of this outcome makes the protection of that anonymity highly important. Consequently, the United States should actively investigate and prosecute "leaks" of the type that revealed the Olympic Games operation to the world. The release of such highly classified information is a crime and the potential for harm is enormous.

Second, in the offense, the United States should take care not to overly militarize its cyber capabilities. Doing so may inadvertently give a military character to actions that would otherwise enjoy presumptive legality as espionage. For example, a single U.S. General heads both the U.S. Cyber Command (USCYBERCOM) and the NSA. The organizations are even co-located. According to U.S. policy, this allows "these separate and distinct organizations . . . to maximize talent and capabilities, leverage respective authorities, and operate more effectively to achieve DoD's mission."[111] The separateness and distinctness of these organizations matters.

USCYBERCOM, "when directed, conducts full-spectrum military cyberspace operations . . . in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries"[112] As part of its Signals Intelligence (SIGINT) mission, the NSA, "collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations."[113] These missions carry an important distinction.

Target states will view any cyber attack or defense action under USCYBERCOM authority as having a clear military character. However, NSA's SIGINT mission falls squarely into a category most would consider traditional espionage. This categorization is important given the customary international norm that information-gathering espionage efforts do not amount to a use of force.

---

111 U.S. DEP'T OF DEF., *supra* note 5, at 5–6.

112 U.S. CYBER COMMAND FACT SHEET, U.S. STRATEGIC COMMAND, *available at* http://www.strat com.mil/factsheets/Cyber_Command/ (last visited June 10, 2013).

113 ABOUT NSA, U.S. NATIONAL SECURITY AGENCY, http://www.nsa.gov/about /mission/index.shtml (last visited June 10, 2013).

It is no doubt organizationally beneficial that USCYBERCOM "is charged with pulling together existing cyberspace resources."[114] However, the United States should take care not to blur functional lines too greatly. By doing so, it may inadvertently forfeit the useful protection of presumptive legality its cyber espionage efforts currently enjoy.

For example, consider the insertion of surreptitious information-gathering software into a sensitive foreign military system. Most would immediately characterize such an action by the NSA as simple espionage, and not necessarily a prelude to further escalation. These are extremely useful actions the United States can routinely undertake without risking recourse to war. This is true even when the information gathered may be of tremendous military value. However, it may give the recipient state greater concern to learn the perpetrator was the military's USCYBERCOM. This raises the question of whether the intrusion is part of a larger, perhaps more imminent, military effort.

The more closely these organizations align, the more difficult it is for states to draw this distinction. Should the distinction disappear in the reasoning of other states, the United States may have to self-limit its espionage for fear of others viewing it as an escalatory military action. This would result in a case where increased organizational efficiency actually led to decreased operational effectiveness.

B. On the Defense

The above recommendations pertain primarily to U.S. actions on the offensive end of the spectrum. The United States can also lessen ambiguities on the defensive end. Clear declarations concerning invasiveness can put opposing states on notice concerning what incursions the United States will treat as possible armed attacks.

One author calls cyberspace "the latest domain of commerce and globalization to emerge as a global common."[115] However, the entire globe is not a commons. States exercise recognized territorial sovereignty over portions of the land, air, and sea domains. There is no reason cyberspace must be treated as outer space, without any

---

114 U.S. STRATEGIC COMMAND, *supra* note 112.

115 Steven H. McPherson & Glenn Zimmerman, *Cyberspace Control*, *in* SECURING FREEDOM IN THE GLOBAL COMMONS 83, 83 (Scott Jasper ed., 2010).

assertions of territorial sovereignty.[116] Human beings create the networks and nodes that comprise the cyber domain. States sometimes go to great lengths to maintain separation between certain sensitive networks and nodes and the "open" cyber commons. When they do so, states should enjoy the equivalent of sovereign rights over that portion of the cyber domain.

This is more than just an academic concept. With sovereignty comes a recognized right of exclusion and defense. There is no expectation that a state stand idly by while thousands or millions of unknowns make unwanted and uninvited attempts to cross it borders in the air, land, or sea domains. Attempts in these numbers occur daily in the cyber domain.[117] In traditional domains, states might view the vast majority of cases as criminal acts appropriate for handling by immigration authorities. However, some attempts might occasionally fit the profile of an invasion, which would trigger the inherent right to self-defense. The analysis need not differ much for the cyber domain.

As a first defensive step, the United States should declare its most critical cyber networks and nodes as under its sovereign protection and state its intention to exclude all others, just as it would from its physical territory. It has already done so, in effect, by its declaration that it does "reserve the right to defend these vital national assets as necessary and appropriate."[118] Basing this right upon sovereignty is a logical step into an already-existing legal framework.

This acquisition of sovereignty by assertion is not without parallel in the land domain. "Acquisition of land traditionally was, and still remains, dependent on power processes, often backed by military strength . . . [T]he rules for allocating title to a particular state are heavily dependent on a showing of physical control."[119] In other words, the power to keep others away eventually becomes a recognized right to keep them away.

---

116 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, art. II, Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. 6347 ("Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.").

117 U.S. DEP'T OF DEF., *supra* note 5, at 3 (stating, "DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from U.S. networks and those of U.S. allies and industry partners").

118 *Id*. at 10.

119 Lea Brilmayer & Natalie Klein, *Land and Sea: Two Sovereignty Regimes in Search of a Common Denominator*, 33 N.Y.U. J. INT'L L. & POL. 703, 705–06 (2001).

As a second defensive step, the United States should employ active cyber defenses in those portions of the cyber domain over which it claims sovereignty. Active defenses involve detecting, tracing, and performing some type of cyber counter-attack against the intruder.[120] This can occur in an automated mode at network speed, typically after the intruder bypasses passive defenses.

It is here that "Webster's reflex" detailed in the *Caroline* rules has remarkable applicability for the 21st century.[121] After breaching passive defenses, damage may occur faster than humans can react, making an electronic reflexive action necessary to prevent harm. The U.S. Department of Defense has already declared it "will employ an active cyber defense capability to prevent intrusions onto DoD networks and systems."[122] Such measures should defend all critical systems, whether DoD or otherwise.

Finally, the United States should commit to reporting instances in which its active defenses actually deploy. This is consistent with its obligation under the U.N Charter to inform the Security Council of measures taken in the exercise of the right of self-defense in response to an armed attack.[123] Because an active defense mechanism typically has a destructive component, it is likely a use of force. Only an armed attack justifies a use of force in response.

Laying out the circumstances of the use of force (though certainly not its technical means) and the perception of the armed attack that precipitated it provides two benefits. First, it helps deters future attacks, as effective deterrence requires a certain level of knowledge and common understanding about the possible response. Drawing on the work of Thomas Schelling in *Arms and Influence*,[124] one commentator refers to this as having "a shared idiom of action" in which "countries interpret military actions and reprisals similarly."[125] This "shared understanding of limits, norms, and expected responses

120 Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self Defense and Deterrence in Cyberspace*, 25 HARV. J. L.AW & TECH. 415, 419 (2012).

121 Matthew J. Sklerov, *Responding to International Cyber Attacks as Acts of War*, *in* INSIDE CYBER WARFARE 45, 45–75, (Jeffrey Carr ed., 2010) (providing a detailed analysis of the specific application of international law to active defenses).

122 U.S. DEP'T OF DEF., *supra* note 5, at 6.

123 U.N. Charter art. 51.

124 THOMAS SCHELLING, ARMS AND INFLUENCE (2008).

125 Vincent Manzo, *Deterrence and Escalation in Cross Domain Operations: Where Do Space and Cyberspace Fit?*, 66 JOINT FORCES Q. 8, 10 (3d Quarter, 2012).

creates a necessary frame of reference by which actors distinguish between proportionate and escalatory behavior."[126]

Second, it also helps to lessen quickly the ambiguity currently surrounding the application of international law to the cyber domain. It is difficult to clarify this legal regime when there is no acknowledgement or discussion of current state practice. Open information allows legal commentators, practitioners, and judicial authorities to build a body of accepted international law.

CONCLUSION

To summarize, this paper first detailed the international legal norms currently governing the use of force between states. The key components of the regime are the overall prohibition against the use of force and the exception for force used in self-defense, to include anticipatory self-defense, against an armed attack. It then examined the factors proposed by the Tallinn Manual as indicators a cyber action qualifies as a use of force. These factors included state involvement and military character (who), severity and presumptive legality (what), invasiveness (where), immediacy (when), and directness and measurability of effects (how).

Applying these factors to the 2007 cyber attack against Estonia indicated the attacks did not qualify as a use of force or armed attack. The application to the 2010 Stuxnet attack against Iran reached the opposite finding. That particular cyber action likely did qualify as an armed attack under the proposed Tallinn Manual analysis. Recognizing a vast grey area exists between these two extremes, the paper recommended several steps the United States could take to reduce dangerous ambiguities and lessen the risk of state miscalculation.

First, the United States should take responsibility for its clearly justified offensive uses of force in the cyber domain. As a corollary, it should vigorously seek to prosecute those who compromise its anonymity in special cases where national interests preclude such open acknowledgement. Second, to protect the presumptive legality of cyber espionage, the United States should not blur the distinction between it and cyber attack/defense by allowing functions to intermingle too closely between organizations. Third, the United States should draw a bright line as to its invasiveness tolerance by asserting sovereignty over some portions of the cyber domain. Fourth,

---

126 *Id*. at 11.

the use of active defenses is the most effective means of asserting and protecting these U.S. sovereignty claims. Fifth and finally, U.S. reporting of active defense deployments will help customary international legal norms develop more quickly.

The cyber domain is a relatively new environment. As with all such environments, a certain amount of discovery learning must take place. However, it is in everyone's interest to reduce the ambiguities in the domain as quickly as possible to ensure no one blunders into war. It is towards this aim that this paper directs the above recommendations. One hopes the phrase, "Of course, you realize, this means war!" will never be necessary between states. However, if it ever is, it would unspeakably tragic if the alleged offending state could legitimately disagree.