INTERNATIONAL LAW APPLIES TO CYBER WARFARE! NOW WHAT?

Gary D. Brown*

INTRODUCTION

It's no longer controversial (if it ever was) to say international law applies to cyber warfare. The United Nations (UN) has said "[i]nternational law, and in particular the Charter of the United Nations, is applicable."[1] State Department Legal Adviser Harold Koh expressed existing U.S. policy in 2012 when he officially stated that "international law principles do apply in cyberspace."[2] And, expressing the unanimous view of the international group of experts gathered to develop the first comprehensive text on cyber international law, Rule 80 of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual*)—which gives away the ending with the title—notes that international law applies to cyber warfare.[3]

So, yes, international law applies to cyber warfare. But international law relevant to warfare comes in two flavors, as Harold Koh noted:

> Under international law, there are two distinct ways of looking at war—the reasons you fight and how you fight. In theory, it is possible to break all the rules while fighting a just war or to be engaged in an unjust war while adhering to the laws of armed conflict. For this reason, the two branches of law are completely independent of one another.

* Professor of Cyber Security, Marine Corps University, Quantico, Virginia.

1. U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 19, U.N. GAOR, 68th Sess., U.N. Doc. A/68/150 (June 24, 2013).

2. Harold Hongju Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference*, 54 HARV. INT'L L. J. ONLINE, at 3 (2012).

3. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 375 (2d ed. 2017).

> Jus (or ius) ad bellum is the title given to the branch of law that defines the legitimate reasons a state may engage in war and focuses on certain criteria that render a war just. . . . Jus in bello, by contrast, is the set of laws that come into effect once a war has begun.[4]

In contrast to the critical role played by *jus ad bellum*, this article suggests the *jus in bello* (law of armed conflict or LOAC) has little of interest to say specifically about cyber warfare.[5] Mr. Koh goes on to note specifically that the law of armed conflict applies in the context of armed conflict, and the principles of distinction, proportionality, and necessity are applicable in that context.[6] Although the legal overlap is significant, the places where actual cyber activities and the LOAC intersect are few and, in the scheme of things, not especially relevant. What is more, it could be damaging to attempt to flex LOAC to cover cyber operations not within the meaning of the law.

Again, this is not to say law is irrelevant to cyber operations. Law is a critical aspect of discussions about the cyber aspects of privacy rights, espionage, sovereignty, international norms of behavior, and more—but none of these things is within the realm of LOAC. LOAC applies only during armed conflict. In addition to there being ambiguity about what pure cyber armed conflict would look like, there are issues with how relevant LOAC would be regarding the use of cyber techniques in the context of traditional armed conflict when the techniques do not result in kinetic effects.[7]

Set out below are observations of what makes cyber conflict unique, followed by a discussion of law other than LOAC that is relevant to cyber operations and a case for an effects-based evaluation of cyber operations. The paper concludes with a look at why, for practical reasons, LOAC as a body of law has little relevance for cyber warfare, and the danger in trying to interpret it creatively enough to make it matter for cyber operations in armed conflicts.

4. Karma Nabulsi, *Jus ad Bellum / Jus in Bello*, CRIMES OF WAR, http://www.crimesofwar.org/a-z-guide/jus-ad-bellum-jus-in-bello/ (last visited Jan. 11, 2017).

5. The law applicable during armed conflict is referred to as both International Humanitarian Law (IHL) and the Law of Armed Conflict (LOAC). They refer to same body of law and are used interchangeably throughout this paper.

6. *See* KOH, *supra* note 3, at 4-5.

7. Of course, cyber activities that result in death or destruction would be analyzed according to the effect, just as bombs and bullets are. These events are not the subject of this article, and are analyzed precisely the same as their kinetic counterparts.

UNIQUENESS OF CYBER WARFARE

Despite assertions to the contrary, cyber-based warfare is *a lot different* from traditional kinetic warfare.[8] In the past, the introduction of new technologies into warfare hasn't caused LOAC to break a sweat.[9] It has been straightforward to apply traditional law to situations in which violence in warfare has been carried out by a new method. However armed conflict has been conducted, there haven't been significant debates about whether a given capability somehow eluded being governed by LOAC, although there have been issues around the edges about *how* LOAC would be applied.[10]

For example, airpower was introduced as a means of warfare in the 20th century but, even though it was new in many ways, it did nothing to challenge experts' intuitive understanding of warfare. Airpower still employed kinetic munitions, just like artillery and naval guns, both of which had been around for many years. The same basic rules applied. Later, precision-guided munitions (PGMs) were introduced but, again, there was not really anything new there. PGMs are simply more accurate than dumb bombs, creating some debate over whether their use is mandatory when they are available, but not controversy over whether LOAC governs explosions caused by PGMs.[11] The argument about nuclear weapons has generally focused on whether LOAC bans them entirely as indiscriminate, not whether the body of law controls their use in armed conflict.[12]

These new methods did little to interrupt the functioning of the *jus ad bellum*, either. Explosives and ballistic munitions, however delivered, are similar in effect. Whether a crater is caused by artillery or an air-delivered munition is of but little relevance when considering whether it constitutes an

8. *See* THOMAS RID, CYBER WAR WILL NOT TAKE PLACE (2013); Jerry Brio & Tate Watkins, *Cyberware is the New Yellowcake*, WIRED (Feb. 14, 2012, 6:30 AM), https://www.wired.com/2012/02/yellowcake-and-cyberwar/; Sean Lawson, *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History*, Mercatus Ctr. George Mason U., Working Paper No. 11-01 (Jan. 2011), http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

9. *See generally* BRYAN FREDERICK & DAVID E. JOHNSON, THE CONTINUED EVOLUTION OF U.S. LAW OF ARMED CONFLICT IMPLEMENTATION 41-48 (2015), http://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1122/RAND_RR1122.pdf

10. *See generally* RID, *supra* note 9.

11. Charles, J. Dunlap, Jr., *No, The Law of War Does Not Always Require the Use of Precision Munitions—and That's a Good Thing for the US*, DUKE LAW: LAWFIRE (Feb. 25, 2016), https://sites.duke.edu/lawfire/2016/02/25/no-the-law-of-war-does-not-require-the-use-of-precision-munitions-and-thats-a-good-thing-for-the-us.

12. Although with regard to *Add'l. Protocol I*, some States submitted declarations noting it was meant only to apply to conventional weapons. *See* Louis Maresca & Eleanor Mitchell, *The Human Costs and Legal Consequences of Nuclear Weapons Under International Humanitarian Law*, 899 INT'L REV. OF THE RED CROSS 621, 627 n.27 (2015).

armed attack. The analogies between territory and airspace, and space and the high seas, are strong and permit fairly straightforward solutions to the most vexing issues regarding sovereignty.[13]

Cyber armed conflict, on the other hand, has introduced a host of unique issues to the bodies of international law governing warfare. Time and geography offer few limits to cyber operations, which can happen in less than the blink of an eye anywhere on the globe.[14] Further, most of the modern LOAC developed when States had a monopoly on the means of warfare but, unlike tanks, ships, and bombers, cyber techniques are widely available to the public. Also, there are real questions about which cyberspace activities would violate "cyber sovereignty." For example, do electronic penetrations of computer systems violate territorial sovereignty as military invasions do?

Another difficult issue is that the infrastructure that is used to carry out legitimate and important civilian business and education is the same infrastructure used to engage in cyber espionage, carry out cyber aggression, to conduct strategic communications, and to do just about everything of importance a State government or its population would do.[15] This may have an unfortunate practical effect on the notion of protecting civilian infrastructure, because there really is no purely civilian cyber infrastructure. The commingling of military/security and civilian infrastructure tends to make the principle of distinction less relevant, if not altogether academic.

Perhaps the biggest issue facing States as they puzzle through how to govern cyber warfare is that crime, espionage, and warfare in cyberspace are all identical to a point. Unlike kinetic operations, which are different in kind and scale from crime and espionage, cyber warfare operations can be utterly indistinguishable from cyber crime and peacetime cyber espionage. This creates new issues for States trying to determine how they may, and how they should, react to adversary cyber operations they discover ongoing.

Despite the unique qualities of cyber capabilities, there should be no confusion about whether LOAC applies to cyber warfare—it does. There is no exception that would exempt cyber warfare from being governed by

13. *See generally* Eric Talbot Jensen, *Cyber Sovereignty: The Way Ahead*, 50 TEX. INT'L L.J. 273 (2015).

14. For a discussion on how the rapidity with which data moves on the internet has changed stock trading, *see* MICHAEL LEWIS, FLASH BOYS 56-82 (2014). On just how fast data travels, *see* Amy Nordrum, *Hibernia Networks Bets Speed of New Fiber Optic Cable Will Win Customers in Crowded North Atlantic Corridor*, INT'L BUS. TIMES (Aug. 12, 2015, 2:45 PM), http://www.ibtimes.com/hibernia-networks-bets-speed-new-fiber-optic-cable-will-win-customers-crowded-north-2050674.

15. *See generally* Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and The Protection of Civilians*, 886 INT'L REV. OF THE RED CROSS 533 (2012).

LOAC, but the details of the coverage can be elusive.[16] Before moving to a more in-depth discussion of LOAC, however, a look at other aspects of relevant international law is in order.

CYBER ACTIVITIES OUTSIDE THE CONTEXT OF ARMED CONFLICT

The most active area for international discussion relevant to cyber warfare is how cyberspace activities affect international relations and the possibility of resorting to cyber war or of cyber operations resulting in a war beginning.[17] Of course, lawyers would prefer to confine the discussion to the legal issues. There is a body of law that governs the resort to war, but politics and relations between States are much more the issue with cyber warfare. The dance among States as they carry out trade, diplomatic relations, espionage, etc. is delicate. In the end, although the UN Charter provides the only lawful means of resorting to armed conflict, i.e., when sanctioned under Chapter 7 or in response to an armed attack, political and military leaders tend to talk less about the law in the area and more in terms of what constitutes an "act of war."[18]

The determination that something is an act of war expands the discussion beyond the law. It concerns the relative strength of the involved States, the domestic political situation, alliances, intelligence analysis, and more. These factors greatly outweigh legal considerations in the actual calculus of States. This is easy to see when hypothetically reversing parties in some actual cyber incidents. For example, if Iran had damaged a nuclear facility in the U.S. as the U.S. is said to have done in Iran with the Stuxnet virus, the victim's public reaction to the operation would have been very different.[19]

Similarly, if Estonia had engaged in cyber aggression against Russia equivalent to what Russia did to Estonia in 2007, it is likely Russia would

16. The notion that declaring LOAC applicable to cyber warfare would legitimize cyber warfare has been put forward in some UN forums, but the idea has little support in the international legal community. *Report of the International Security Cyber Issues Workshop* 17 (2016), http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf.

17. The article uses the term "war" here rather than the legal formulation "armed conflict" because the point is that war is partly a political decision, informed rather than controlled by law.

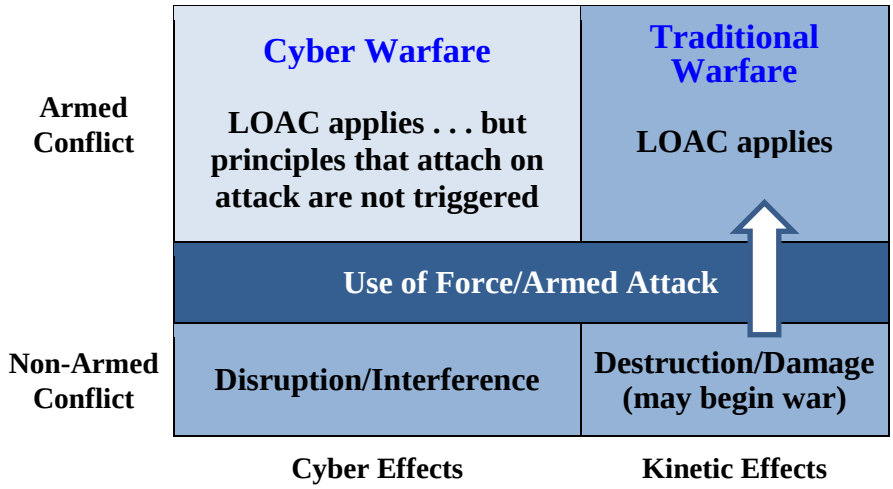
18. *See* Cyber Act of War Act of 2016, H.R. 5220, 114th Cong. (2016); *see also* Aaron Boyd, *When and How to Respond to Cyber Acts of War*, FED. TIMES (Jul. 13, 2016), http://www.federaltimes.com/story/government/cybersecurity/2016/07/13/cyber-acts-war/87044610.

19. *See generally* Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, 63 JOINT FORCES Q. 70 (2011). Israel was also implicated in the Stuxnet incident. For a full explanation of Stuxnet, see KIM ZETTER, COUNTDOWN TO ZERO DAY (2014).

have responded aggressively in self-defense.[20] Imagine Russia's reaction to having large numbers of its government and banking websites offline for hours at a time over a period of several days. Taking a position consistent with the relative sizes of the States involved, however, Estonia determined the activity would be better handled as a criminal matter rather than a breach of international peace.[21]

Ultimately, States' judgments on whether they are the victims of an act of war that provides sufficient cause to engage in national self-defense is circumscribed by political reality and, while the law may inform the decision, it does not compel it.[22]

To ensure clarity for the remainder of the paper, the following chart sets out a framework for the application of international law to cyber warfare. Although cyber means and methods are a part of warfare, war is also still caused and carried out by physical means. This article is meant to look at cyber-specific situations where there is little precedent and a great deal of ambiguity about how the law should operate.



20. ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS LEGAL CONSIDERATIONS 18-25 (2010).

21. *Id.* at 25-26.

22. U.N. Charter art. 39. UN. UN authorization to use force under Chapter 7 is straightforward if relatively rare. States must decide on a regular basis whether hostile activities directed against them constitute an act of war, which they would characterize as armed attacks for purposes of public justification.

The chart represents how the law applies to various effects. Below the ARMED CONFLICT band is peacetime (at least, non-armed conflict) operations.[23] However, most of the time kinetic operations during peacetime instantly elevate the situation above the line. That is, they trigger armed conflict, although the conflict may be quite brief if the victim decides not to respond. It's important to note that the applicable law is determined by the effects, not by the method. For example, if a cyber method causes a kinetic effect, it is treated no differently than if it were caused by a traditional kinetic means.

Operations below the line of armed conflict on the chart are not governed by the law of armed conflict. The bottom right box generally presents typical bellicose operations. If kinetic effects result (property destruction, injuries, or death), the situation may be pushed above the line to armed conflict—even if the kinetic effects are caused by cyber means or methods. The lower left box is the typical use of cyber techniques to annoy, harass, disrupt, and interfere outside of armed conflict. It's unclear when, if ever, such activity alone can create a state of armed conflict.

Above the line, the top right box is typical warfare, involving destructive and injurious effects. Even if kinetic effects in the context of armed conflict are created with cyber means and methods, the application of LOAC is clear, and no different than if the effects were created with kinetic means. Destroying civilian structures or directly injuring civilians (perhaps through manipulating medical devices), when the places and people are the target of the cyber attack, is unlawful, but there is little mystery there.[24] Some problems, like electrical power, are trickier, but the rules that have worked for bomb dropping should work equally well for cyber techniques. If anything, LOAC should operate to encourage cyber over kinetic operations because it's likely the civilian impact will be less when a system isn't destroyed as it is with kinetic options, but rather is rendered non-usable with cyber means and can be turned on again after the conflict. If LOAC operates to permit a broader range of cyber activities in war, civilian death and destruction will tend to be diminished. Rather than having only force to achieve national security goals during armed conflict, States could also have effective, lawful cyber options.

The unique aspect of the use of cyber means and methods in warfare is represented in the top left box. In the context of armed conflict, cyber

23. *See* discussion on different types of armed conflicts *infra* pages 363-65.

24. OFFICE OF GEN. COUNSEL DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 16.5, at 1003-9 (June 12, 2015).

techniques that do not result in kinetic effects create new issues for LOAC. It is this specific category of activities that this paper addresses.

GETTING TO CYBER WAR

LOAC, which is sometimes referred to as the law of war or international humanitarian law (IHL), is best defined as ". . . the controlling body of law with respect to the conduct of hostilities and the protection of war victims."[25] As might be obvious from the name, LOAC applies during an armed conflict.

LOAC is comprised of a specific set of principles that apply in a distinct situation that involves violence, destruction, injury, and death. It applies only when States or armed groups have broken the peace. At least one (and often more) of the parties involved in the armed conflict have already shown disdain for legal constraints on behavior by their resort to violence in the first place. Still, the body of law applies to all parties involved in an armed conflict, regardless of whether the conflict is just or unjust, and no matter who started it. In the context of this violent situation, certain basic rules have been found to apply: the principles of distinction, military necessity, proportionality, and humanity.[26]

LOAC is critically important for regulating conduct in warfare. It limits the use of inhumane weapons, prohibits the targeting of civilians and civilian property, and guards the wounded and captured, among other things.[27] However, it is limited in application to armed conflict. Relevant to this discussion, that means LOAC applies to cyber warfare, but not to cyber activities outside the context of armed conflict. As noted previously, those lesser activities are not ungoverned by law, but they are untouched by this particular body of law. Just as the body of Virginia traffic laws, while perfectly valid and important, does not govern driving in Canada, LOAC has no authority to regulate cyber conduct outside the context of armed conflict.[28]

25. Mary McLeod, Acting Legal Advisor, U.S. Dep't of St., *U.S. Affirms Torture is Prohibited at All Times in All Places*, Committee Against Torture, Opening Statement Before the Committee Against Torture (Nov. 12-13, 2014), https://geneva.usmission.gov/2014/11/12/acting-legal-adviser-mcleod-u-s-affirms-torture-is-prohibited-at-all-times-in-all-places/.

26. LAW OF WAR MANUAL, *supra* note 25.

27. *See generally id.* It also serves the vital function of governing the treatment of detainees, but that aspect of LOAC is beyond the scope of this article.

28. U.S. DEP'T OF DEF., DIR. 2311.01E, DOD LAW OF WAR PROGRAM para 4.1 (May 9, 2006). DoD notes its policy that DoD members "comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations." While this provision is the subject of discussion in other contexts, it does not change the outcome with regard to cyber activities. The primary principles would fail to attach to non-attacks in non-armed conflict situations, just as in armed conflict.

Although it is straightforward that LOAC applies during armed conflict, it is not always easy to determine the existence of an armed conflict. Not every occurrence of violence is "armed conflict." Attempts to define precisely armed conflict have been unsatisfactory, such as this one from Uppsala Universitet: "An armed conflict is a contested incompatibility which concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths."[29] Although it was a noble effort, it is apparent that a specific definition like this raises as many questions as it answers. Why must a government or territory be involved? Why not 24 deaths? What if there are thousands of injuries but no deaths? How can massive property damage and destruction not result in a state of armed conflict?

Armed conflict can be subdivided in various ways. Uppsala Universitet's creative definition lumps it all together, but international law requires armed conflict to be divided into two parts. That is because LOAC is comprised of two similar but legally distinct sets of rules. One governs international armed conflict (IAC) and the other non-international armed conflict (NIAC).[30]

The first is simple to define. An international armed conflict is a resort to armed force between States.[31] This is the classic case of warfare—the government of one territorial State waging war against the government of another territorial State. There is generally not considered to be any specific threshold of death or destruction. A single shot fired in anger between two States results in a state of IAC.[32]

It is challenging to conceive of a cyber-only IAC that did not include a large-scale kinetic effect. Cyber techniques that are used to cause fires, flooding, or mass transit accidents, for example, seem sufficient to meet the single shot threshold, just as the same event caused by kinetic actions (bombs, saboteurs, and assassins) would. To start an armed conflict without kinetic effects would be breaking new ground, but one focused on UN Charter law, i.e., the *jus ad bellum* rather than LOAC.

29. DEPT. OF PEACE & CONFLICT RESEARCH, http://www.pcr.uu.se/research/ucdp/definitions/definition_of_armed_conflict (last visited Jan. 11, 2017).

30. 31st International Conference of the Red Cross and Red Crescent, Nov. 28-Dec. 1, 2011, Geneva, Switz., *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 31IC/11/5.1.2, at 3 (Oct. 2011). In the LOAC discussion, this paper considers only principles common to both IAC and NIAC law.

31. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE GENEVA CONVENTIONS (III) OF 12 AUGUST, 1948, RELATIVE TO THE TREATMENT OF PRISONERS OF WAR, 22 (Jean S. Pictet ed., 1960).

32. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE GENEVA CONVENTIONS (III) OF 12 AUGUST, 1948, FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN ARMED FORCES IN THE FIELD, 32 (Jean S. Pictet ed., 1952).

Turning to non-international armed conflict, it is unhelpfully defined as "armed conflict not of an international character."[33] In addition to being an armed contest between entities that include at least one non-State, to be classified as armed conflict non-international clashes require some level of organization on the part of the non-State group, as well as some level of intensity in the violence to qualify as armed conflicts.

Various tribunals have considered the level of intensity required for armed conflict through evaluating a number of factors, some of which are particularly ill-suited to address groups of cyber actors, such as displacement of people due to the conflict and the number and type of weapons used.[34] Other factors aren't much better; they include the gravity of attacks and their recurrence, the expansion in territory, and duration of violence.[35]

If anything, the analysis gets harder when considering the organization of cyber actors. The law requires the non-state actors to be armed enough so that they have the capacity to mount attacks.[36] Organizational factors assessed include whether the group has internal regulations; whether it can issue orders and coordinate attacks effectively; the establishment of disciplinary rules and enforcement mechanisms; the ability to recruit members; and the use of uniforms.[37]

It seems unlikely these factors would be present sufficiently for there to be a cyber-only NIAC. Much of the nefarious activity on the internet is undertaken by hacktivists and loose collections of actors such as Anonymous, the Chaos Computer Club, and LulzSec, which hardly qualify for the moniker "group," much less "organized group."[38]

33. Geneva Convention (III) Relative to the Treatment of Prisoners of War, art.3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135. To make matters even more confusing, the ICRC recognizes six different types of NIAC, and takes note of a seventh type recognized by some. This level of discussion is well beyond the scope of this paper, but is set out in 31st International Conference of the Red Cross and Red Crescent, Nov. 28-Dec. 1, 2011, Geneva, Switz., *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 31IC/11/5.1.2, at 9-10 (Oct. 2011).

34. *See* Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, ¶ 40-49 (Int'l Crim. Trib. for the former Yugoslavia Apr. 3, 2008).

35. *See id.*; Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, ¶ 135-67 (Int'l Crim. Trib. for the former Yugoslavia Nov. 30, 2005).

36. *See* LAW OF WAR MANUAL, *supra* note 25, at 74-76.

37. *Limaj*, Case No. IT-03-66-T at ¶ 94-129

38. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 49, June 8, 1977, 1125 U.N.T.S. 3; Some hacker collectives are described in Rob Nightingale, *4 Top Hacker Groups And What They Want*, MAKE USE OF (Mar. 4, 2015), http://www.makeuseof.com/tag/4-top-hacker-groups-want; *Techopedia* defines hacktivism as "the act of hacking a website or computer network in an effort to convey a social or political message," TECHOPEDIA, https://www.techopedia.com/definition/2410/hacktivism (last visited Jan. 13, 2017).

Whether a state of armed conflict is triggered by cyber activities and effects or, as seems more likely, by kinetic events,[39] once a state of armed conflict exists, combatant activities are governed by LOAC. The principles that make up the essential body of LOAC are noted above. This paper will focus on two of them, distinction and proportionality.

CONDUCT OF HOSTILITIES WITH CYBER MEANS: A LIMITED ROLE FOR LOAC

"Distinction requires parties to a conflict to discriminate in conducting attacks against the enemy. . . . parties may not make the civilian population and other protected persons and objects the object of attack."[40]

What is referred to as the proportionality rule would prohibit "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[41]

Note the word "attack" in both principles. Proportionality and distinction only apply in cases of "attack" in the context of armed conflict. So, as simple as seems, the principles cannot be applied properly without a definition of attack.

The obvious question to be answered, then, is what exactly is a cyber attack? The definition of attack in international law is "acts of violence against the adversary."[42] Cyber operations that lack direct physical effects are not violent and so cannot be classified as attacks. The Tallinn Manual's definition for cyber attack is "a cyber operation . . . that is reasonably

39. *See* Chart, *supra* page 360.

40. LAW OF WAR PROGRAM, *supra* note 23, at para 2.5.2. The DOD's definition, rather than an international definition, is used here for reasons discussed *infra* at pages 371-72.

41. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3; The U.S. is not a party to *Add'l. Protocol I* but considers large parts of it, including this provision, to be accurate statements of customary international law.

Martin D. Dupuis, John Q. Heywood & Michèle Y.F. Sarko, *The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. INT'L L. REV. 415, 426-427 (1987); The U.S. sets out the rule in the Department of Defense Law of War Manual "Combatants must refrain from attacks in which the expected loss of life or injury to civilians, and damage to civilian objects incidental to the attack, would be excessive in relation to the concrete and direct military advantage expected to be gained." *See* LAW OF WAR MANUAL, *supra* note 21, at 242 n.304.

42. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 49, June 8, 1977, 1125 U.N.T.S. 3.

expected to cause injury or death to persons or damage or destruction to objects."[43]

So, even though it is clear LOAC applies to cyber activities inside an armed conflict, its relevance is limited. The two most important principles of LOAC, distinction and proportionality, both attach on attacks. That is to say, activities that are something other than attacks do not trigger application of the principles.[44]

Cyber attack must be distinguished from cyber disruption. The term "cyber disruption" is used here to refer to cyber only operations that cause inconvenience, even extreme inconvenience, but no direct injury or death, and no destruction of property. There have been many examples of these kinds of effects caused by computer malfunctions. Considering how such events would be characterized if they had been intentionally caused may help illustrate why they should not be categorized as attacks.

In 2016, both Delta Airlines and Southwest Airlines suffered major disruptions of service when computer systems malfunctioned.[45] Both airlines were forced to ground hundreds of flights, losing millions of dollars in revenue.[46] There was no injury or damage, but major financial losses.[47] If the computer systems were destroyed by bombing in an armed conflict, they would be considered attacks, of course. What if instead the problems were caused, during an armed conflict, by hiring all the competent computer operators away from the airlines, or by stealthily changing the cipher lock combinations on the doors to the computer facilities? Both of these could result in the same disruptions to the computer networks, but would not be classified as attacks. Neither should the same result caused by a non-

43. *See* TALLINN MANUAL 2.0, *supra* note 4, at 415.

44. *See generally*, MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 239-40 (2014). The author there does, however, take a contrary view on the application of *Add'l. Protocol I*, Art. 57, Precautions in Attack.

45. Analyn Kurtz, *Delta Malfunction on Land Keeps a Fleet of Planes From the Sky*, N.Y. TIMES, Aug. 8, 2016, http://www.nytimes.com/2016/08/09/business/delta-air-lines-delays-computer-failure.html.

46. Lauren Gensler, *Delta's Computer Outage to Cost Them $150 Million*, FORBES (Sep. 7, 2016, 10:36 AM), http://www.forbes.com/sites/laurengensler/2016/09/07/delta-computer-outage-flight-cancellations-eats-into-profits; *see also* Bill Hethcock, *Southwest Airlines Computer Outage Costs Could Reach $82M*, DALLAS BUS. J. (Aug. 12, 2016, 11:34 AM), http://www.wfaa.com/news/local/southwest-airlines-computer-outage-costs-could-reach-82m/296158194.

47. Kurtz, *supra* note 45; *Delta Malfunction on Land Keeps a Fleet of Planes From the Sky*, N.Y.TIMES, Aug. 8, 2016, http://www.nytimes.com/2016/08/09/business/delta-air-lines-delays-computer-failure.html; Bill Hethcock, *Router at Root of Southwest Airlines' Computer Systems Outage; Delays, Cancellations Persist*, DALLAS BUS. J., July 21, 2016, http://www.bizjournals.com/dallas/news/2016/07/21/router-at-root-of-southwest-airlines-computer.html.

destructive cyber operation be defined as an attack, despite its deleterious effect on the civilian population.

Similar actions could be designed to aid in a military campaign, without the actions themselves being attacks. Compromised networks controlling transportation systems, such as railroad switching and air traffic control, might be manipulated so they become buggy and unreliable. This would likely force the authorities to halt or curtail traffic to prevent accidents. Similarly, military operators might cause networked traffic lights in a major city like Los Angeles to work only sporadically, or set them all to red, snarling traffic. Software controlling ship traffic in Houston, New York, Long Beach, and other major seaports could be caused to crash, tangling the unloading of ships and causing shortages of items across the country. Penetrated financial networks might be manipulated to delete, modify, or transfer balances in individual bank accounts. None of these activities would cross the threshold of an attack, just as the same results caused with non-destructive physical means would fall short of an attack. For example, if an extension cord were unplugged causing equipment to go to a battery backup with limited functionality, or if phone calls were placed to harbormasters to trick them into sending ships away without unloading, there would be no military attack, but the result of the activity would be disruptive to an enemy in its war efforts.[48]

The unique aspects of cyber warfare—speed, ubiquity, and lack of geographic constraints—have brought this issue to the forefront. The principles of LOAC were agreed to and have been practiced in a pre-cyber warfare world. The introduction of cyber capabilities does not change the basic principles of LOAC, which continue to require attacks for the principles to apply.

The mischief that can be caused with cyber disruption, while still falling below *in bello* attack, illustrates how the time-honored LOAC principles, while very useful in a traditional kinetic situation, fail to provide the same level of protection for civilians who might be victims in cyber war. Experts in the field take for granted that the principles will be relevant in every situation that might be averse to the interests of civilians caught in armed conflict. Actually reading the words of the concepts reveals that this is not so.

Observing the gap cyber warfare techniques appear to have opened in civilian protections during armed conflict, some international law experts have suggested the definition of attack, with regard to cyber, should be

48. Of course, any or all of these activities might be criminalized under domestic law as sabotage or some other crime. The point here is that such actions are not limited by the LOAC principles of distinction and proportionality.

expanded to include loss of functionality.[49] This would not merely be an application of existing law to a new method of warfare. This would be a redefinition of a term of art beyond anything it has previously been found to mean.

The *Tallinn Manual* breaks the functionality issue into three basic scenarios.[50] A cyber operation can physically damage a component of a computer system, can cause it to cease functioning until the operating system is reinstalled, or can cause it to cease functioning by deleting or interfering with data on the system (e.g., the targeted computer still functions as a computer, but isn't functional as a communications node because the communications program has been deleted).[51]

The ICRC would like to see it expanded this way. "[I]t is clear that the damage to be taken into account comprises not only physical damage, but also the loss of functionality of civilian infrastructure even in the absence of physical damage."[52] More specifically, the ICRC argues:

> [T]he fact that a cyber operation does not lead to the destruction of an attacked object is also irrelevant. Pursuant to article 52(2) of Additional Protocol I, only objects that make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage, may be attacked. By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is immaterial whether an object is disabled through destruction or in any other way.[53]

The preeminent legal scholar in the field of cyber warfare offers a somewhat different view. "I am nevertheless now persuaded by the foundational premise of the restrictive approach, i.e., that the notion of cyber attacks cannot be limited to injurious or physically destructive cyber operations . . . My own view is that a system has lost functionality when it is no longer able to perform its intended function without some repair. This would include reloading the operating system or any software essential to its operation, but would not include replacing data that was merely stored on the system."[54] Although this is a reasoned position, it is still an expansion of existing law.

---

49. *See* TALLINN MANUAL 2.0, *supra* note 4, at Rule 92, para 10, at 417.

50. *Id.* at Rule 92, paras. 10-12, at 417-19.

51. *Id.*

52. Droege, *supra* note 15, at 571.

53. *Id.*

54. Michael N. Schmitt, *Rewired Warfare: Rethinking the Law of Cyber Attack*, 96 INT'L REV. OF THE RED CROSS 189, 202-03 (2014), https://www.icrc.org/en/international-review/article/rewired-warfare-rethinking-law-cyber-attack. As noted in his article, although

Under the terms of the *Tallinn Manual* taxonomy discussed above, the ICRC advocates for the broadest definition, which would define any cyber event causing a loss in functionality as an attack. Professor Schmitt argues for the middle option. Both of these approaches create issues under current law, although the ICRC approach is more problematic.

CONSEQUENCES OF APPLYING A FUNCTIONALITY STANDARD

The definition of function is "the kind of action or activity proper to a person, thing, or institution; the purpose for which something is designed or exists."[55] For example, the primary function of cell phones is to act as communications devices, the primary function of a bridge might be to provide a path across a river, and the primary function of car is to transport a person between two places.[56] In kinetic operations, the method of preventing the function of these items might be to bomb cell towers, blow up the bridge, and crush the car by driving over it with a tank. Clearly, all these options are attacks, and the principles of LOAC would apply. The attacks would have to be discriminate, necessary, proportionate, etc. to pass legal muster.

On the other hand, what if a military commander decided to approach the problem differently, by buying up all the cell phone service provider's bandwidth to prevent the operation of local cells phones, by parking military vehicles on the bridge to prevent the passage of civilian traffic, and by taking the car keys from the car. All of these techniques prevent the function of the civilian objects. However, none of them looks like an attack, and none would be analyzed as such under the principles of the law of war.[57] Why should cyber activity be treated differently? If a denial of service against the cell phone service provider, a hack that raises a drawbridge, and reprogramming car key fob to render it inoperable all can have the same effect as non-destructive kinetic events, why should they be analyzed differently?

If the ICRC approach were the law, other fairly innocuous actions in the physical realm would also be considered "attacks," because they similarly interfere with the functionality of an object without damaging it. The

Professor Schmitt agrees to some extent with ICRC's argument, he rejects its basis for the conclusion.

55. Function, DICTIONARY, http://www.dictionary.com/browse/function (last visited Jan. 30, 2017).

56. Each of the examples has other functions, as well, but it cannot be the case that every possible function of a device must operate lest the activity that ended that function be considered an attack. A cell phone may function as a paperweight, but picking it up from a stack of papers does not damage its functionality.

57. That's not to say the actions wouldn't be analyzed for policy and strategic reasons. Actions in and out of warfare are often avoided if they are "lawful but awful."

expansion in the law wouldn't be limited to cyber activities, it would also extend to kinetic activities with similar effects. Activities in wartime such as hiring civilian truck drivers, using roadways, or letting the air out of tires all reduce the functionality of civilian trucks, but none of these activities is an attack, and there would be no consideration given as to whether hiring civilian drivers violates the proportionality principle or whether driving on a roadway violates the principle of distinction, for example. The ICRC approach would appear to render all of them attacks, which is simply not the law.

Professor Schmitt's approach specifies that some sort of repair would be required before a loss of functionality would equal an attack.[58] This is closer to what the law requires, but still appears to expand it from its current state. For example, draining a battery necessitates recharging the battery, a type of repair. Would turning on a truck's lights, which might result in draining the battery, constitute an attack *in bello*? If a cyber attack could remotely drain a system battery by causing a screen to stay on at full brightness, for example, would that be an attack? It is difficult to think of a good kinetic analog to reloading system software, but perhaps it's akin to stealing an instruction book so that equipment can't be operated. Would such a theft be considered an attack? Referring to the previous paragraph, is adding air to a deflated tire a repair?

If these examples seem absurd, it is because they are. LOAC was designed to provide broad legal coverage of destructive wartime activities to protect civilians from death, injury, and property destruction, not to prohibit disruptions or inconveniences. As discussed earlier, LOAC should encourage non-destructive, non-lethal cyber activity in order to hasten a return to normalcy post bellum.

The role of cyber operations in national security is important, and growing in importance, but once an armed conflict begins, generally cyber warfare fades to the background in the white heat of kinetic battle. Cyber operations are in support, providing options to help degrade the adversary's ability to counter actions. Now and for the foreseeable future they will be the smallest concern when weighed against death, injury, and destruction.

58. Schmitt, *supra* note 54, at 203.

THE FUTURE

LOAC is a real body of law. Without new treaties or established custom, it won't change.[59] In the area of cyber warfare, it is generally considered that a treaty is unlikely to the point of impossible because of international disagreement over basic principles such as free speech and privacy.[60] Cyber warfare also presents an especially difficult case study for the development of norms, as States have to date kept their cyber operations concealed. That means there has been no progress toward developing common practice.

As the two common methods of changing the law are unlikely to result in change with regard to cyber warfare, any unique issues that arise must be dealt with by interpreting existing law, rather than writing new. The problem with creatively trying to adjust LOAC to fit the situation is that it could make it more difficult to apply and thus less effective for kinetic warfare.

Until there is a change in the political landscape, which could happen very quickly if there is a catastrophic cyber event, there will remain a gap in the protection of civilians from inconvenience in warfare. Despite this gap, the risk nondestructive cyberspace operations pose to civilians is outweighed by the risk of damaging LOAC's application in traditional armed conflict.

RED HERRINGS: EXPANDED DISTINCTION, THE MARTENS CLAUSE, AND TELEOLOGY

The discussion above did not use the most common international statement of the principle of distinction, which is found at *Add'l. Protocol I*, Art. 48: "Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[61] This definition of the principle is misleading, in that it uses the phrase "operations" rather than attacks when all the examples *Add'l. Protocol*

59. States develop new international law through their custom and practice, followed by eventually believing they are legally bound to act in certain ways because it is the practice. This can be aggravating for scholars, who would prefer open discussion and full transparency regarding the development of international law. This issue is fully discussed in Michael N. Schmitt & Sean Watts, *State* Opinio Juris *and International Humanitarian Law Pluralism*, 91 INT'L L. STUD. 171 (2015), http://stockton.usnwc.edu/ils/vol91/iss1/6.

60. Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INSTITUTION, 8 (2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf; Sean Lyngaas, *Cyber Treaty Not in the Cards*, FCW (Apr. 27, 2015), https://fcw.com/Articles/2015/04/27/Cyber-treaty.aspx.

61. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 597 (1987), http://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf.

I provides are, in fact, attacks. [62] Some scholars argue that it should be read to cover actions that would not qualify as attacks.[63] Actions suggested for coverage are "all the movements and activities carried out by armed forces related to hostilities."[64]

Despite the complex academic rationale in favor of this interpretation, two compelling arguments run counter. First, if the *Add'l. Protocol I* drafters intended the terminology to apply to situations broader than attacks, they would have offered examples of what those situations might be. Instead, all the examples provided concern attacks, which is consistent with the way the Protocol defines proportionality.

Second, and even more compelling, the broad interpretation is simply not how States have applied this provision in practice. When reviewing military activities in the context of operations, logistics, communications, and other support activities are not reviewed for compliance with the principle of distinction. The effect of such operations on civilians may be reviewed for practical or policy reasons, such as compliance with rules of engagement, but no legal review is authored to determine if the act of landing cargo planes on a civilian runway or using a civilian radio frequency to transmit military supply communications violates the principle of distinction, even though both fail to distinguish between civilian and military objects in the same way analogous cyber operations would.

For these reasons, the U.S. statement of the principle more accurately reflects the reality of the law than *Add'l. Protocol I*, and so the U.S. statement was used in the main body of this article.[65]

It has been similarly argued that another provision of *Add'l. Protocol I* might be relevant here.[66] Supplemental to, or in addition to (it is unclear which), the principle of distinction is *Add'l. Protocol I*, Art. 51, which provides civilians "general protection against dangers arising from military operations."[67] This provision has been a topic of discussion among international legal experts, but ultimately fails to change the conclusion that civilians and civilian objects may be targeted by cyber operations that fall below the level of an attack.

62. *Id.* at 600.

63. INT'L COMM. OF THE RED CROSS, *supra* note 61.

64. A summary of this position may be found in HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 196-202 (2012).

65. It certainly more accurately reflects customary law, and the section on *Add'l. Protocol I*, Art. 51 that follows, suggests it better represents the law of Art. 48, as well.

66. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, *supra* note 62, at 617.

67. *Id.* at 613.

The provision does not alter the conclusion about cyber warfare because, based on the examples given in the rest of Art. 51, it was not included to add restrictions to non-attack military operations.[68] Rather, it was written to emphasize that certain types of egregious attacks on civilians are prohibited.[69] These include attacks to cause terror and indiscriminate attacks.[70] The lack of clarity in the wording of the provision is noted by eminent international jurist Yoram Dinstein. "It is not clear what dangers arising from military operations—other than attacks—the drafters of AP/I had in mind."[71] The ICRC Commentary asserts the language should apply to all the activities armed forces carry out pursuant to armed conflict.[72] Although the sentiment is laudable, it reflects neither the language of the provision nor State practice in this regard. Troop movements, billeting, and security measures often inconvenience the civilian population, but States do not apply the principles of warfare to make decisions about these operations. For example, military leaders do not attempt to determine if driving a convoy on a road is "indiscriminate" just because the road is a civilian object whose functionality will be impaired while it is being used for military purposes.[73]

After discussing possible interpretations of the *Add'l. Protocol I*, Art. 51 language, Professor Dinstein ultimately concludes the provision must be read to apply only to attacks, expressing concern that it leaves open the door for sub-attack cyber operations to be directed against the civilian population.[74]

Neither Art. 48 nor Art. 51 of *Add'l. Protocol I*, as noted above, moderate adverse cyber warfare effects on civilians satisfactorily.[75] When something appears to fall outside the jurisdiction of LOAC, especially if there is ambiguity in the situation, scholars sometimes turn to the Martens Clause.[76] The Martens Clause, from the Preamble to the 1899 Hague Convention, is

68. *Id.* at 613.

69. "To give effect to this protection, the following rules . . . shall be observed." INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, *supra* note 62, at 613.

70. *Id.* at Art. 51(2) and (4) at 613.

71. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 143 (3d ed. 2004).

72. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, *supra* note 62, at 617.

73. The issue is discussed in the context of battlefield biometrics, but is not brought to a definitive conclusion in Alison Mitchell, *Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics*, 50 CAN. Y.B. INT'L L. 289, 309-10 (2012).

74. DINSTEIN, *supra* note 71.

75. There is a nearly identical argument with regard to Art. 57. *See* DINNISS, *supra* note 49, at 200-02.

76. *See, e.g.*, Erki Kodar, *Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I*, 15 ENDC PROCEEDINGS, 107, 107-32 (2012).

named for its author, Russian Professor von Martens. "Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience."[77] Although it is a valuable tool in some contexts, with regard to cyber warfare, the Martens Clause adds nothing to the mix. LOAC already applies,[78] so the Clause is unnecessary to ensure legal coverage. The big question is exactly how the law applies to cyber operations, and the language of Martens, being quite general, adds no clarity to that.

Finally, it may be argued that failing to apply LOAC principles to cyber disruption targeted at civilians violates the purpose of LOAC. [79] After all, ICRC defines IHL as "a set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare."[80] This definition, however, is overly restrictive in that it reflects only one rationale for LOAC, and notes only its limiting function, which is why this paper used another definition for its analysis.[81]

From the earliest attempts to develop a formal body of law to govern warfare there was a recognition that implementing general protective rules would facilitate a return to peace.[82] A practical body of wartime law facilitating a return to peace is more likely to motivate States to comply than would a protective code created without a recognition of the unfortunate reality of war. States desire peace not only because it benefits civilians, but also because it generally serves the security interests of States.

77. Hague II Convention with Respect to the Laws & Customs of War on Land, Preamble, July 29, 1899, 32 Stat. 1803, http://avalon.law.yale.edu/19th_century/hague02.asp#art1.

78. Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1, 2-3 (2010) (discussing how the LOAC applies to cyber warfare).

79. Byron D. Green, *Bridging the Gap that Exists for War Crimes of Perfidy*, 2010-AUG. ARMY L. 45, 3.2 (2010) (explaining that the purpose of the LOAC is to "humanize warfare to the maximum extent possible.").

80. Int'l Comm. of the Red Cross: Advisory Service on International Humanitarian Law, *What Is International Humanitarian Law?* (2004), https://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf.

81. *See* McLeod, *supra* note 20 (explaining that the LOAC is "the controlling body of law with respect to the conduct of hostilities and the protection of war victims").

82. EMMERICH DE VATTEL, THE LAW OF NATIONS; OR PRINCIPLES OF THE LAW OF NATURE, APPLIED TO THE CONDUCT & AFFAIRS OF NATIONS & SOVEREIGNS § 173, at 369 (Joseph Chitty ed., 6th ed. 1844) (stating that "the sword will never be sheathed till one of the parties be utterly destroyed.").

A restrictive definition of LOAC, which would result in the application of principles that would limit cyber disruption during armed conflict, does not reflect the law or State practice. Further, although it may seem to reflect a kinder legal regime, in the long run it might be less humane. If States are permitted to employ a broad range of disruptive cyber options, even against civilian objects, in many cases it could offer a rationale alternative to the collateral damage and casualties likely to result from lawful kinetic attacks.

As John Fabian Witt notes in his book on the law of war, *Lincoln's Code*, the original U.S. law of war code was "not just a humanitarian shield . . . [i]t was also a sword of justice."[83] That code, as is the case with the modern LOAC, was intended to be a realistic guide, recognizing the unfortunate inevitability of war while crafting rules limiting violent effects on the civilian population to those necessary to wage the war. In other words, it is overly reductionist to confine the purpose of LOAC to a humanitarian-driven quest to limit effects. LOAC's remit is broader, providing a legal framework for warfare while constraining its effects for the benefit of civilians and, ultimately, the parties to the armed conflict.

CONCLUSION

There are many challenges in applying international law to cyber activities. The least of these are concerns that arise during armed conflict. The critical issues are those surrounding cyber operations outside existing armed conflict. Uncertainty outside the context of existing armed conflict could cause international miscalculation, breaking of the peace, and a rapid escalation of aggression. There is work to be done to increase confidence among States, develop norms of appropriate cyber behavior, and to provide privacy guarantees to citizens, among other things. None of these issues is within the ambit of LOAC.

As discussed previously, LOAC has always covered cyber warfare.[84] The issue has been concern over *how* it does so.[85] LOAC, being a practical body of law, recognizes civilians will be adversely affected by war. Inconvenience and bother are the smallest concerns in warfare. LOAC addresses death and devastation, including that caused by cyber warfare. It just does not prohibit nonviolent actions that would cause civilians to drive

83. JOHN FABIAN WITT, LINCOLN'S CODE: THE LAWS OF WAR IN AMERICAN HISTORY 4 (2012).

84. *See* Huntley, *supra* note 79, at 2 (explaining that while the LOAC may not be completely effective when applied to cyber warfare, the LOAC, nevertheless, applies to cyber warfare).

85. *See id.* at 2-3 (discussing concern over the ineffectiveness of LOAC to deter cyber warfare).

the long way around to work, to lose cable TV, to be deprived of their favorite soda . . . nor does it protect them from being cut off from social media. In other words, what have to date been the most common uses of cyber capabilities operate below the level at which LOAC would restrict them. No attack means no proportionality or distinction analysis. When cyber attacks cause kinetic effects, by damaging a piece of industrial equipment, for example, analyzing the damage is the same regardless of whether it was caused by a saboteur, air-delivered ordnance, an artillery shell, or by a cyber attack. No cyber-specific analysis is required, or helpful.

The functionality gap discussed here has caused consternation in the international legal community, with some members fearing civilians might suffer as a result.[86] So far, even without LOAC governing disruptive cyber activities, civilians have not suffered greatly as a result of cyber warfare.[87] It may be that States have determined as a matter of policy not to carry out such activities, that they think wartime cyber disruption of civilians would not advance their strategic interests, or that warring States simply lack the capacity for an effective disruption campaign. Particularly if one of the first two is the explanation, there are grounds for hope that customary law might develop that would offer the civilian community more formal protection.

Although LOAC has little to offer in controlling unique aspects of cyber operations in the context of armed conflict, it continues to play a vital and irreplaceable role in regulating kinetic operations in warfare. LOAC is fragile by nature because it is designed to affect behavior between warring parties, who do not like each other to start with, and may perceive major advantages in violating the law. The body of the law of armed conflict has proven resilient through the years, but it is important to avoid stretching it to the breaking point.[88] Broadening definitions for the purpose of achieving more direct coverage of cyber activities during armed conflict risks undermining LOAC and losing its application to kinetic operations, where it is a critical and historically proven stay on the lethal and destructive activities of States.

It may be that permitting non-attack cyber operations to target civilian objects in armed conflict is not the best answer. In that case, States must

86. *See, e.g.*, Ariana L. Johnson, *Cybersecurity for Fin. Institutions: The Integral Role of Info. Sharing in Cyber Attack Mitigation*, 20 N.C. BANKING INST. 277, 303-04 (2016) (discussing how cyber warfare can cause physical harm and economic harm, including identity theft).

87. *See, e.g.*, *id.* at 277-81 (explaining that while banks are consistent victims of cyber warfare, banks constantly manage to recover and build new technologies to fight cyber warfare; thus, they avoid long-term financial damage or collapse).

88. *See, e.g.*, Ryan J. Vogel, *Drone Warfare & the L. of Armed Conflict*, 39 DENV. J. INT'L & POL'Y 101, 137 (2010) (discussing how the LOAC has been successful in regulating sophisticated technology, like drones).

determine whether non-attack cyber effects in armed conflict are best governed by the aggressively creative interpretation of LOAC critiqued here, or rather by some other body of law or norms. Until *States*, the masters of international law, decide to change the law, it will remain what it is—adaptable and effective in its rules protecting civilians from the effects of attacks in warfare, and ambivalent about activities that fall below that level.