Toward Criteria for International Cyber Weapons Bans

Merritt Baer
Merritt Rachel Baer, LLC
Washington, DC USA
mbaer@post.harvard.edu

Abstract**—This paper considers the possibility and envisions some of the limitations in applying arms control measures to cyber weapons. It surveys weapons bans in other forms of weapon including chemical, biological, and nuclear, and points to characteristics that are associated with a basis for a ban. Based on those characteristics, it then presents some criteria that are likely to surface in a discussion of whether and how to institute a cyber weapons ban.**

Keywords—arms control, cyber, weapons ban

I. INTRODUCTION

"[S]cience does not…answer the question: 'What shall we do, and, how shall we arrange our lives?'"

Max Weber, quoting Tolstoy [1]

In this paper, I examine the possibility of creating a subset of cyber weapons that can or should be subject to an international arms control treaty. I explore the application of international humanitarian law principles and the law of war, given existing bans on chemical, biological and nuclear weapons.

International law has enforced a number of rules surrounding war. These usually fall into the categories of why you fight (jus ad bellum), and how you fight (jus in bello). There has been some movement in the area of applying to cyber the principles of jus ad bellum—delineating when violent action is justified in the cyber landscape. The debate surrounding the use of preemptive force is particularly ripe and uncharted.

International dialogue has remained vague on the subject of whether there are certain cyber weapons that ought to trigger international humanitarian regulations. While the Tallinn Manual provided a lengthy international law discussion, it did not deal specifically with weapons classes. Moreover, while the Manual is an important step in the academic conversation about cyberwar, it is guiding and not binding. The discussion that is happening between and among governments seems to be largely separate from that of the intellectual conversations. So to the extent that an issue exists in potential cyber weapons bans, the Tallinn Manual has not settled it.

II. BRIEF OVERVIEW OF ARMS CONTROL MEASURES

Codification of international norms about weapons began in 1899. A Conference of 50 countries [2] at The Hague banned projectiles "the sole object of which is the diffusion of asphyxiating or deleterious gases," [3] among other forms of weapon. That being said, this agreement "was evaded or violated during World War I—first by the Germans at Ypres in April 1915, and then by all the major powers." [4] A quarter century later, the 1925 Geneva Protocol reinforced the prohibition, outlawing first use of chemical and biological weapons. [5] Current proscriptions include chemical, biological and nuclear weapons as well as certain conventional weapons such as landmines. [6]

The use of weapons bans has sometimes elicited criticism as a political tool masquerading as a moral imperative. In recent US-Syria tensions, Atlantic writer Dominic Tierney accused Obama of political gaming [7] because the US is dominant in conventional weapons, while chemical, biological and nuclear weapons could allow a small actor to enact disproportionately large damage. Critics suggest that rather than uplifting standards of human decency, weapons bans target "equalizers."[8] Cyber weapons bans might fall within the same set of critiques: perhaps attempts to standardize norms shroud a desire to disarm countries that would otherwise hold power disproportionate to their international clout. The context of cyber weapons is especially politicized and a weapons ban would likely elicit international resistance or noncompliance. That being said, applying international humanitarian proscriptions to cyber weapons predates current political agenda. I explore the possibility of applying the underlying principles to the cyber context.

III. INTERNATIONAL NORMS AND LAWS AROUND CYBER WEAPONS

Research on the applications and effects of a cyber weapon, current technological capabilities and possible effects, is a critical area for study. Technology is a moving target and will continue to evolve. The capabilities themselves are not the focus of this paper. Rather, this list describes features of weaponized uses of cyber technology that might trigger international humanitarian concerns enough to justify a ban on that technology as a weapon.

Cyber weapons are young in the timeline of war, and there is less empirical evidence upon which to draw. I leave for another day the insertion of specific examples into this framework. Most technologists can imagine examples of cyber uses—current or future—that might fall within these restricted categories. In this article I provide a synopsis of some traits that are likely to form the criteria for determining which cyber weapons are beyond the pale.

IV. Plausibility of Diplomatic Approaches

There are three basic principles in the law of war: 1) distinction, 2) proportionality and 3) military necessity. Weapons that have been banned by international law are those that not only do not fall within these principles, but in their envisioned uses, can not.

Some have scoffed at cyber treaty-making as an unrealizable goal. Indeed, I have presented research on technological and practical barriers to cyber disarmament diplomacy [9]. It is certainly true, as Christopher Capozzola points out, that "treaties and protocols have been unsigned, unratified or violated by some countries." [10] However, that does not detract from the relevance of establishing in the context of cyber an "international norm against forms of warfare that have devastating effects on soldiers, civilians and natural environments." [11]

I disagree with those who claim that diplomacy is not possible because "All you need is training in computer software engineering and some talent." [12] I grant that it may require minimal resources to execute ongoing attacks— even persistent, sophisticated attacks targeting significant payloads. Recent sources confirm that cyber weapons of many scales are for sale on a black market. But the class of action I target in this paper is a different mode of weapon. It is a confined subset of extraordinary as-applied technologies, perhaps ones that do not exist yet. The vast majority of cyber attacks do not and should not trigger strong international normative response.

Martin Libicki, who points out that "No person has ever died from a cyberattack," [13] advocates for establishment of "international norms" as an alternative to treaty-making. [14] I view international norms and treaty-making as functionally interrelated, particularly with the understanding that the role of international treaties is to formalize accepted terms rather than to enforce them. (Enforcement requires a separate architecture, though of course it lends weight to the restrictions.)

Academic Mary Ellen O'Connell asserts, "Moving away from military analogy in general and Cold War deterrence in particular, will result in the identification and application of rules with a far better chance of keeping the Internet open and safer for all." [15] She sees potential to apply to cyber the international law of economics and communications, and discusses the usefulness of architectures that exist in international law as an alternative channel for codification of cyber norms. Whether or not international law can be effective at regulating ongoing lawless actions online, international leaders might consider independently a contained cyber weapons ban for high-level violent technology that triggers humanitarian concerns.

V. Criteria for Potential Cyber Arms Control

The following are factors that are likely to be considered (all will need to be accompanied by damage that potentially rises to fatality):

- They target civilians intentionally or collaterally.

The need to focus force on military targets with appropriate precision and intent is a fundamental principle of the law of war.

- They have few or no civilian uses.

Like cyber, chemicals that are used in chemical attacks may have a dual use. But when the international community witnesses stockpiling of resources to a degree only justified by a weaponized use, there may be cause to take note. Context is supremely relevant, and this factor is likely to be paired with other concerns.

- They create extraordinary amounts of suffering.

Because of the nature of cyber, this might take the form of an as-applied weapon: an attack on critical infrastructure SCADA systems or a hack of a medical device company. (In accordance with this as-applied focus, chemical weapons are categorized by their effects upon humans. [16])

- They have "indiscriminate effects" or cannot be accurately tailored to their target.

This is a principle that has been raised but is not universally agreed upon. International Committee of the Red Cross (ICRC) lists the international treaties and various country-specific laws that formalize the customary international humanitarian law prohibiting weapons that are by nature indiscriminate. [17]Eugene Kaspersky has taken to calling for a ban on certain cyber weapons because "A targeted attack on one piece of critical infrastructure could easily spiral out of control, resulting in damage that would be nothing short of cataclysmic in an age where just about everything relies on access to a network to perform a critical function." [18] In other words, even targeted attacks cannot be contained in cyber and effects may end up being indiscriminate because of collateral damage.

VI. Barriers to Implementation of Cyber Arms Control

As I have described, there may be promise to apply a weapons ban to cyber weapons as they trigger international humanitarian concerns. There are also, however, certain unique barriers to establishing a framework for cyber weapons ban. These include:

- Difficulty in isolating the harm.

Can there be a humanitarian concern for harm that is not directly kinetic? How kinetic need the harm be? How direct need the connection be from the cyber weapon to the kinetic outcome?

- We lack some of the experiential aspect.

Weapons bans arose after WWI, and were revisited after WWII. Just War Theory is old but the distinction between jus ad bellum and jus in bello emerged 10 years after WWII. [19] Chemical weapons were banned before they were used, but much of the force of their normative proscription derives from witnessing the use of those weapons. [20] Can we speak authoritatively about what a normative response may feel like, when we have not experienced a cyber intrusion of this scale?

- Government has traditionally held sole responsibility for national security, yet private industry owns the architecture of cyber.

It is government's role to make decisions about and possibly authorize the use of certain weapons. In the case of cyber weapons, it is possible that the technology and its targets are not directly within the control of government. Can we control who creates new cyber weapons or new uses for cyber weapons to ensure that they do not violate international law? If a cyber weapon is deployed against an industry target and not a government entity, would it trigger the same concerns?

- Enforcement is unclear.

While Obama recently declared the existence of a "red line" [21] in Syria's stockpiling of chemical weapons supplies, in fact there is not international consensus upon where those lines lay, and what should happen if a state (or non-state actor) were to cross that line.

VII. Conclusion

While the criteria outlined above may not yet describe any existing technology, it is a worthwhile thought experiment to consider whether there are certain cyber tools that might be applied as weapons in violation of international law. Concerns about enforcement, moral perimeter drawing, and pragmatic applications are not unique to cyber, and have been brought into conversation and confronted internationally in the context of chemical, biological and conventional weapons bans. There is room to contemplate a cyber weapons ban, and we ought to revisit the possibility as use of technology in weapons evolves.

References

[1] H.H. Gerth and C.W. Mills (eds), "Science as a Vocation," in *From Max Weber : Essays in Sociology*. New York: Oxford Univ. Press, 1946, part 1, sec. 5, pp. 144.

[2] Int. Committee of the Red Cross, "Customary International Humanitarian Law," [online], http://www.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=150 (Accessed 20 October 2013).

[3] Yale Law School, "The Laws of War," *The Avalon Project*, [online], http://avalon.law.yale.edu/subject_menus/lawwar.asp (Accessed: 28 September 2013). There were a handful of weapons bans earlier than the 1899 Convention, including the St. Petersburg Declaration of 1868, prohibiting the use of exploding projectiles that weigh less than 400 grams.

[4] C. Capozzola, as interviewed by P. Dizikes, "Christopher Capozzola on the history of chemical-weapons bans," *MIT News*, http://web.mit.edu/newsoffice/2013/3q-christopher-capozzola-chemical-weapons-bans-0910.html (Accessed: 18 October 2013).

[5] United Nations, Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, 17 June 1925. Available online, http://www.un.org/disarmament/WMD/Bio/pdf/Status_Protocol.pdf (Accessed: 20 October 2013).

[6] The Ottawa Treaty, sometimes referred to as the Mine Ban Treaty, took effect in 1999.

[7] D. Tierney, "Civilian Syrians Better Hope They Die in the Right Way," *The Atlantic*, [online], 4 December 2012. http://www.theatlantic.com/international/archive/2012/12/syrian-civilians-better-hope-they-die-in-the-right-way/265848/ (Accessed: 21 October 2013).

[8] [7]

[9] M. R. Baer, "Cyber Disarmament Treaties and the Failure to Consider Adequately Zero-Day Threats," in *International Conference on Information Warfare and Security*, 2013, pp. 255-259. J. Goldsmith, "Cyber Disarmament Treaties: A Skeptical View," Hoover Institution, [online], http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf (Accessed 30 September 2013).

[10] [4].

[11] [4].

[12] C. Bronk and D. Wallach,"Cyber Arms Control? Forget About It," [online] 26 March 2013, http://www.cnn.com/2013/03/26/opinion/bronk-wallach-cyberwar/index.html (Accessed: 30 September 2013).

[13] M.C. Libicki, "Don't Buy the Cyberhype: How to Prevent Cyberwars from Becoming Real Ones," *Foreign Affairs*, 14 August 2013.

[14] "Setting International Norms on Cyberwar Might Beat a Treaty," *US News*, [online] 8 June 2012, http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/setting-international-norms-on-cyberwar-might-beat-a-treaty (Accessed: 28 September 2013).

[15] M. E. O'Connell, "Cyber Security Without Cyber War," *Journal of Conflict Security Law*, vol. 17, no. 2, pp. 187, Summer 2012.

[16] http://www.opcw.org/about-chemical-weapons/types-of-chemical-agent/

[17] "Practice Relating to Rule 71. Weapons That Are by Nature Indiscriminate," [online], http://www.icrc.org/customary-ihl/eng/docs/v2_rul_rule71 (Accessed: 20 October 2013).

[18] "Kaspersky Renews Call for Ban on Cyber Weapons," [online] 11 February 2013, http://www.itbusinessedge.com/blogs/it-unmasked/kaspersky-renews-call-for-ban-on-cyber-weapons.html (Accessed: 20 October 2013).

[19] ICRC, "IHL and other legal regimes—jus ad bellum and jus in bello, [online] 29 October 2010, http://www.icrc.org/eng/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm (Accessed: 20 October 2013).

[20] R.M. Price, *The Chemical Weapons Taboo*, Ithaca: Cornell University Press, 1997, pp. 12.

[21] Pres. Obama, "Remarks to the White House Press Corps," [online], 20 August 2012, http://abcnews.go.com/Politics/video/president-obama-draws-red-line-syria-2012-20117362 (Accessed: 30 September 2013).