INTERNATIONAL LAW APPLIES TO CYBER WARFARE! NOW WHAT?

Gary D. Brown*

INTRODUCTION

applies to cyber warfare. The

[1] State Department Legal Adviser Harold Koh expressed existing U.S. policy in inciples do apply in

[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

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 [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

capability somehow eluded being governed by LOAC, although there have been issues around the edges about *how* LOAC would be applied.[10]

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

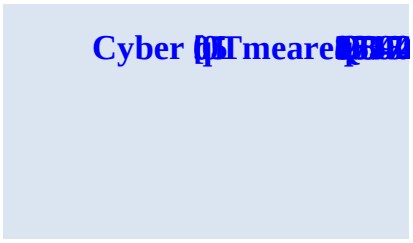
The most active area for international discussion relevant to cyber warfare is how cyberspace activities affect international relations and the possibility of resorting to cyber war or of cyber operations resulting in a war beginning.[17] Of course, lawyers would prefer to confine the discussion to the 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 Sta erane,292(Sta)iut fe561.91 0 7r warfare.

have responded aggressively in self-defense.[20]
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]

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.

Armed Conflict



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

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

2017]

expected to cause injury or death to persons or damage or destruction to [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

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]

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 networ[m0 gfaks. 367kwih,h(t)-4(9nW*

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*

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

person between two places.[56] In kine792 reBT/F3 11] TJET1.07 12.96 /F[(( )s,ns)7(t)-4(w)5h (i)-4(ch)9(od

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.

ies 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

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

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

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 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

ising from military

operations other than attacks t

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 [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,

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 [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 nBT/F1 8.52 Tf1 0 0 1 159.86 175.82 Tm0 g.d reWdW- 13f 0 1 -rghssibl1 0 3T2 reW* nBT/F1 6.96 Tf1 0 0 1 284.57 217.8

2017]

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]