Challenges in Applying the Law of Armed Conflict to Cyberspace

Richard W. Aldrich[1]

On June 17, 2010 a small antivirus company established in Belarus discovered what would later come to be known as the Stuxnet worm. Later research would reveal that a variant of the worm existed at least a year earlier. Stuxnet reputedly caused the physical degradation of some 1000 centrifuges at the Natanz facility in Iran, based on data of the International Atomic Energy Agency (IAEA).[2] While the identity of the perpetrators is still unknown almost two years later, some have suggested nation-state involvement due to the sophistication of the malware. The heavily hardened Natanz facility was built to withstand "bunker buster" bomb attacks, but apparently not cyber-attacks. The incident has created new impetus for examining the law of armed conflict in cyberspace.

On the 5th of February of this year, several senior government officials, including Secretary of State Hillary Clinton, Prime Minister David Cameron, Chancellor Angela Merkel and others, participated in the 47th Munich Security Conference to address, among other issues, how the Geneva and Hague Conventions should be applied in cyberspace. A joint US-Russian bilateral document presented at the conference offered recommendations in five key areas:

1. Detangling Protected Entities in Cyberspace
2. Application of the Distinctive Geneva Emblem Concept in Cyberspace
3. Recognizing New Non-State Actor and Netizen Power Stature
4. Consideration of the Geneva Protocol Principles for Cyber Weaponry
5. Examination of a Third, 'Other-Than-War' Mode

This paper will examine the merits and challenges of each recommendation, as well as the overarching challenge of attribution in cyberspace.

I. Detangling Protected Entities in Cyberspace

The aim of this recommendation is to "promote the preservation of the observed principles of the [Geneva and Hague] Conventions that protect humanitarian critical infrastructure and civilians."[3] The concern seems to be how to disentangle internet communications that support protected civilian functions from those that would be legitimate military targets. It is widely estimated that at over 95 percent of military Internet communications ride over the commercial backbone,[4] which shows just how

---

[1] Mr. Aldrich is a Lead Associate at Booz Allen Hamilton and the Senior Computer Network Operations Policy Analyst for the Information Assurance Technology Analysis Center.

[2] David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," ISIS, Dec. 22, 2010 (available at http://www.isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/).

[3] Karl Frederick Rauscher & Andrey Korotkov, "Working Towards Rules For Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace," at 7 (Jan. 2011) [hereinafter "EastWest Proposal"].

[4] Science Applications International Corporation, "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance," research report for the chief, Information Warfare Division

entangled they currently are.[5] The segregation of military communications from protected civilian communications is further complicated based on how the Internet is currently architected. Internet communications are broken up into "packets" which are then automatically routed based on best-routing information. Thus a single communication may consist of a large collection of packets, each of which may take a separate route to the destination, where they are reassembled. Rearchitecting the Internet to segregate protected civilian communications from other communications would be a challenge, but something similar was proposed in the wake of the Stuxnet worm.

General Alexander, Commander of the new Cyber Command, has proposed the establishment of a "a secure zone, a protected zone," which has been dubbed by others as "dot-secure" network for essential services.[6] It would attempt to provide fenced off protection for "essential networks like those that tie together the banking, aviation, and public utility systems," but Gen. Alexander did not expound on "where the fence should be built between the conventional Internet and his proposed secure zone."[7] The goal is to provide the type of protection currently enjoyed by the military's classified networks or the State Department's classified diplomatic network. He also did not explain how it would be done, though presumably it would quite expensive and have a host of challenges. Even the military's classified network "suffered a significant compromise," in 2008 via an infected flash drive, according to Deputy Secretary of Defense Lynn.[8] The essential industries would also have incentives to share information between the secure and insecure networks creating a similar problem, and connecting disparate industries would provide significant challenges in itself. Additionally, the dot-secure protection would presumably only provide added protection against electronic attacks. Kinetic attacks on the physical infrastructure would still be as effective as pre-dot-secure.

II. Application of the Distinctive Geneva Emblem Concept in Cyberspace

"The Geneva and Hague Conventions direct that protected entities, protected personnel and protected vehicles be marked in a clearly visible and distinctive way. This recommendation proposes analogous markers in cyberspace to designate protected entities, personnel and other assets."[9] The bilateral group suggested one approach may be to add a new generic Top-Level Domain (gTLD) extension, "such as '.med' or '.+++' or '.nsz' for 'no strike zone.'"[10] While an interesting approach, there are several potential problems with this proposed solution. First it would only identify protected entities via their long Uniform Resource Locator (URL), not their many other cyberspace presences, such as on social networking sites, their extended medical telepresence relationships and the like. Second,

---

(J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, Washington, D.C., 4 July 1995.

[5] "The fact that a country's military uses civilian communications for a large portion of its message traffic increases the justification for claiming such a target is a military target." Richard Aldrich, "The International Legal Implications of Information Warfare," Airpower Journal (Fall 1996).

[6] Tom Shanker, "Cyberwar Chief Calls for Secure Computer Network," N.Y. Times, Sep. 23, 2010 (available at http://www.nytimes.com/2010/09/24/us/24cyber.html).

[7] Id.

[8] William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," Foreign Affairs (Sep./Oct. 2010).

[9] EastWest Proposal, *supra* note 3, at 30.

[10] Id.

it's unclear who would pay for, manage and monitor this gTLD. Third, it's unclear what incentive hospitals would have to move from their proven brands on .com and .org sites to the new extension.

III. Recognizing New Non-State Actor and Netizen Power Stature

"The digital revolution has unleashed non-state actors and individuals to occupy, control and operate in cyber territory. This creates new power asymmetries and magnifies the clout of new participants who can violate Convention principles on a massive scale."[11] This observation of the bilateral group is very true, but the more significant issue is what can be done about it. The EastWest Proposal makes no recommendation on a solution, rather it only recommends it be studied. While the law of armed conflict has traditionally applied to nation-states, as early as 1949, in common Article 3 of the Geneva Conventions, relating to non-international armed conflict, legal obligations have been imposed on non-state entities. The terms of common Article 3, however, do not transfer well to the cyber realm. Of additional significance, there has been a shift in the right of a state to exercise self-defense against an armed attack by a non-state actor. In the wake of the terrorist attacks against the United States of September 11, 2001, the United States declared it was at "war" with Al-Qaida, a stateless, but well-funded terrorist entity. The international legal community has largely accepted this approach.[12] It seems far less clear that the international legal community would be willing to extend this further to netizens.

IV. Consideration of the Geneva Protocol Principles for Cyber Weaponry

"Russian and U.S. governments must be open to the possibility that some weapon attributes may be unacceptable because they are offensive to the principles of humanity and from dictates of public conscience." The prohibition on the use of certain weapons under the law of armed conflict is premised on the prevention of unnecessary suffering or widespread, long-term and severe damage to the natural environment. Only a few weapon-types have been explicitly recognized as prohibited: asphyxiating, poisonous or other gases; bullets which explode, expand or flatten easily in the human body; certain explosive projectiles; conventional weapons that would result in non-detectable fragments; anti-personnel mines, booby traps and incendiary weapons. These specific weapons seem to have no clear analogues in cyberspace. Nevertheless, it is conceivable that cyber weapons could have impacts that would result in unnecessary suffering or severe damage to the natural environment. The United States destroyed power plants during the Iraq war, which some alleged resulted in unnecessary suffering. This was because water treatment and sewage relied on the power from those plants, so raw sewage was dumped in the Tigris River from which many civilians drew their water, ultimately resulting in widespread dysentery, dehydration and death. One could easily conceive of a Stuxnet-like worm accomplishing much the same. Interestingly, however, the International Committee of the Red Cross

[11] EastWest Proposal, supra note 3, at 7.

[12] "[V]arious international bodies, such as the North Atlantic Treaty Organization (NATO), the Organization of American States (OAS), and the remaining parties to the Security Treaty between the United States, Australia, and New Zealand (ANZUS), have all concluded that the September 11 attacks activated the mutual self-defense clauses of their treaties involving the United States. John Yoo and James Ho, "The New York University-University of Virginia Conference on Exploring the Limits of International Law: The Status of Terrorists," 44 Va. J. Int'l L. 207, 212-213 (2003) (internal footnotes omitted).

(ICRC) found the attacks on Iraq's power plants was not a war crime, because power plants have been long-justified targets.

Of importance is the fact that Article 36 of Additional Protocol I to the Geneva Conventions[13] already sets out a requirement to conduct legal reviews of weapons, and the United States has long complied with this Protocol even though it never signed or ratified the Protocol:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[14]

V. Examination of a Third, 'Other-Than-War' Mode

"There is no clear, internationally agreed upon definition of what would constitute a cyber war. In fact, there is considerable confusion."[15] Within the United States former Director of National Intelligence Mike McConnell says, "The United States is fighting a cyber-war today, and we are losing."[16] Howard Schmitt, the White House Cyber Czar, concludes the U.S. is not in a cyber war.[17] A US-Russian bilateral commission on cybersecurity has proposed a definition,[18] but it is unclear it will resolve the issue. Most legal scholars divide the law of armed conflict into two phases, jus ad bellum ("right to wage war") and jus in bello ("law in war"). It's not clear that establishing a third mode, with its own criteria and rules would fare any better.

VI. Attribution

An overarching problem that spans all of the above issues is the problem of attribution in cyberspace. As long as nations believe they can act anonymously refined rules of behavior may have little practical effect. Currently nation states can quite easily create plausible deniability in cyberspace by a variety of means, including discretely delegating the task to sophisticated cybercrime organizations or bot herders, or employ a combination of obfuscating techniques, such as anonymizers, spoofing, and/or a wide variety of other obfuscation techniques. The crippling cyber attacks against Estonia in 2007, the massive cyber attacks against Georgia in 2008, the Stuxnet attack against Iran in 2009-10 are just three noteworthy attacks that have still never been definitively attributed to their sponsors. While all of the above efforts are admirable, without reliable attribution, they are unlikely to forward the cause meaningfully.

---

[13] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 [hereinafter Additional Protocol I].
[14] Id. at Article 36.
[15] EastWest Proposal, supra note 3, at 8.
[16] Mike McConnell, "Mike McConnell on how to win the cyber-war we're losing," Wash. Post, Feb. 28, 2010.
[17] Ryan Singel, "White House Cyber Czar: 'There Is No Cyberwar,'" Wired.com, Mar. 4, 2010.
[18] "Cyber War is an escalated state of cyber conflict between or among states in which cyber attacks are carried out by state actors against cyber infrastructure as part of a military campaign (i) Declared: that is formally declared by an authority of one of the parties. (ii) De Facto: with the absence of a declaration." Karl Frederick Rauscher & Andrey Korotkov, "Critical Terminology Foundations," at 30 (Apr. 2011).