Easier Said Than Done: Legal Reviews of Cyber Weapons

Gary D. Brown* & Andrew O. Metcalf**

Introduction

On June 1, 2012, author and *New York Times* reporter David Sanger created a sensation within the cyber-law community. Just over a year previously, *Vanity Fair*, among other media outlets, reported that a malware package of unprecedented complexity had effectively targeted the Iranian nuclear research program.[1] The malware, which came to be known as Stuxnet, was also discovered on many computer systems outside Iran, but it did not appear to do any damage to these other systems. Just as the discussions spurred by the discovery of Stuxnet had begun to die down, the *New York Times* published an interview with Mr. Sanger to discuss his newest book, in which he alleged that the Stuxnet malware had been part of a U.S. planned and led covert cyber operation. The assertion that a nation state had used a "cyber attack" in support of its national objectives reinvigorated the attention of cyber-law commentators, both in and out of government.

What makes Stuxnet interesting as a point of discussion is that the basic functioning of the software is easy to understand and easy to categorize. A piece of software was deliberately inserted into the target systems, and physical damage was the result. However, resulting physical damage is not characteristic of most cyber operations, and the legal analysis of Stuxnet is of limited utility when examining a broad range of cyber activities.[2] A distinct *lack* of physical effects is much more characteristic of cyber operations, and the absence of physical effects has continued to complicate the legal analysis of cyber in the context of military operations.

The terms "cyber attack" or "cyber warfare" imply the employment of cyber weapons. But the uncertainty in the term "cyber warfare" leads to equal uncertainty in identifying cyber weapons, and great confusion about when the use of a "cyber weapon" is a "cyber attack" that creates a state of "cyber warfare." There have been some excellent attempts to define "cyber weapon" with specificity and to use that discussion to gain a better understanding of cyber war.[3] These discussions are intellectually stimulating, but the purpose of

---

* Colonel, USAF (ret.). Senior Legal Advisor at U.S. Cyber Command, 2010-2012.

** Lieutenant Colonel, USMC. Senior Legal Advisor to U.S. Marine Corps Forces Cyberspace Command.

1. Michael Joseph Gross, *A Declaration of Cyber War*, Vanity Fair, Apr. 2011, at 152.

2. Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, Joint Forces Q., 4th Qtr., 2011, at 70.

3. Duncan Blake & Joseph S. Imburgia, *"Bloodless Weapons"? The Need to Conduct Legal Review of Certain Capabilities and the Implications of Defining Them as "Weapons,"* 66 A.F. L. Rev. 157

this paper is to highlight the difficulty in transforming these broad topics of academic discussion into practical legal advice for those few practitioners advising commanders on the impact of cyber law on operations. Military attorneys must translate academic and deeply theoretical discussions into concrete legal advice. That experience informs this article, which offers examples of how the practicalities of cyber war may collide with the academic discourse, in the hope of informing and shaping the debate. The actual examples of cyber capabilities and operations offered here highlight the practical issues involved in cyberspace operations, where attorneys are called upon to analyze cyber operations under the existing legal regime regarding weapons, and the means and methods of war. Ultimately, this article concludes that treating all cyber techniques as weapons is impractical. Rather, an assessment focusing on how a capability will be used in context, especially of the primary purpose of the capability, is more effective and consonant with international law. This approach will more clearly delineate cyber attacks, and permit a separate discussion of the great majority of cyber events – those that fall below the level of attack.

What this paper does not do is discuss the difference between state-sponsored cyber operations, including cyber warfare and cyber espionage, and cyber crimes. Distinguishing between state uses of cyberspace, and the operations of criminal groups by examining the technical details of cyber incidents is usually not possible. Ultimately, this can only be determined by learning and assessing the motivation of the responsible party, and issues of agency and attribution may make this a near-impossible task. Agency is a particularly thorny problem. The keyboard operator may think he is merely part of a criminal enterprise stealing intellectual property or assisting in an extortion scheme, but the entity paying the bills could as easily be a government pursuing a national security agenda. Conversely, agents of foreign intelligence services may occasionally moonlight as cyber criminals for a few extra bucks. In the end, it is the effect of the action that matters. If all the money is disappearing from a bank, it makes little difference to the bank and its customers whether the malevolent actor is a criminal or a spy – they just want the theft to stop.

I. ESPIONAGE VS. OPERATIONS

One of the first practical issues confronting a cyber operations lawyer is the artificial distinction between espionage and operations. While it's true there is a long-standing (and cynically named) "gentleman's agreement" between nations to ignore espionage in international law, determining exactly which cyber actions constitute espionage and not something of a different nature presents a real challenge. Despite the similarities between cyber-spying and more aggres-

(2010); Thomas Rid & Peter McBurney, *Cyber-Weapons*, RUSI J., Feb.-Mar. 2012, at 6; DEP'T OF THE AIR FORCE, AIR FORCE INSTRUCTION 51-402, LEGAL REVIEWS OF WEAPONS AND CYBER CAPABILITIES (2011).

sive activity in this operations space, cyber experts and policymakers seem intent on excluding espionage from the same consideration that other cyber operations receive.[4] While this firm distinction may have been workable in the age of microfilm, cameras and spies, there are significant challenges in applying this old paradigm to cyber operations.

First, espionage used to be a lot more difficult. Cold Warriors did not anticipate the wholesale plunder of our industrial secrets. Second, the techniques of cyber espionage and cyber attack are often identical, and cyber espionage is usually a necessary prerequisite for cyber attack. On the receiving end, there may be little or no ability to distinguish between cyber techniques used for espionage and those used for warfare. Once an adversary takes control of a computer, he can do what he wants. Initial actions might involve stealing information, but the adversary can use the same access to disrupt or destroy the system, as well. The treatment of espionage in international law may have made some sense prior to the advent of cyber espionage, but looks increasingly ill-suited for the modern world.

Cyber espionage, far from being simply the copying of information from a system, ordinarily requires some form of cyber maneuvering that makes it possible to exfiltrate information.[5] That maneuvering, or "enabling" as it is sometimes called, requires the same techniques as an operation that is intended solely to disrupt. Enabling operations themselves can – deliberately or accidentally – also be just as disruptive to a computer system as an action undertaken for the specific purpose of disrupting the system. For example, an enabling operation could set out to weaken encryption or disable a cyber capability to force the target into using an alternate system that provides easier access to his communications. And, once a system is compromised, the new "owner" of the system can take whatever action he chooses on the compromised system, from manipulating data, to destroying the software, to, in some cases, actually physically breaking the hardware. From the victim's perspective, if this unauthorized access is discovered prior to being used, there is no way to tell from mere observation whether the unauthorized user will choose to engage in espionage, system disruption or destruction.

Often, the only difference between military cyber operations intended to collect intelligence and those designed to deliver cyber effects is the intent – intelligence activities are done with the intent of collecting intelligence, while other military activities are done in support of operational planning or

4. It is inconceivable, for example, that no one in a position of authority would be aware of the military equivalent of the espionage operation that reportedly resulted in the long-term tapping of the German Chancellor's phone, resulting in an extraordinary flap when it was discovered. *US Bugged Merkel's Phone from 2002 Until 2013, Report Claims*, BBC (Oct. 27, 2013), http://www.bbc.co.uk/news/world-europe-24690055.

5. In the DoD definition of "computer network exploitation" this is referred to as "enabling," although the concept is not further explored. DEP'T OF DEF. DICTIONARY OF MILITARY AND ASSOCIATED TERMS, JOINT PUB. 1-02, at 73 (2013) (as amended through Feb. 15, 2013).

execution. The military regularly conducts a broad range of activities outside of cyber that support its ability to execute traditional military operational plans. Some of the support is direct, such as collecting intelligence on areas of interest and strategically pre-positioning forces or supplies so they are available during future crises. Other support is indirect, such as training partner nation militaries or entering into mutual support agreements with friendly countries. Most support activities outside the cyber realm are non-controversial from a legal perspective, though they may be conducted clandestinely and without the consent of the nation where they are being conducted.

This unnatural dichotomy in cyberspace activities makes providing legal advice a different and much more challenging activity than it is in traditional military operations. An activity in cyberspace may be entirely uncontroversial when the primary articulated purpose is intelligence, while the identical activity, conducted for a purpose other than collecting intelligence, may be defined as an "attack" with a "weapon" that requires an extensive analysis involving every branch of government.[6] As set out below, providing a proper definition of "cyber weapon" may provide a basis for a more objective determination of the nature of activities in cyberspace.

II. UNIQUE CHALLENGES OF CYBER OPERATIONS LAW

Military cyberspace operations mix issues of geography, sovereignty, criminal law, and civil rights in ways that may not be entirely new, but cut across some traditional boundaries of legal practice.

The U.S. Department of Defense (DoD) defines cyberspace as a "man-made domain."[7] Military legal analysts are comfortable discussing the concepts of warfare in the contexts of other domains, such as "land-warfare" or "air-warfare," but the common use of those terms and the distinct characteristics those terms convey do not seem to have carried over to discussion of "cyber warfare." In particular, the terms "warfare" and "attack," when used in a cyber context, are applied to a broader range of military operations than when they are used in the other domains. For example, the term "cyber warfare" is used to describe the use of the cyber domain to conduct military operations ranging from the cyber equivalent of logistical convoys to the delivery of violent military attacks.

Cyberspace operations, because of their nature, may be harder to pigeonhole within the range of military operations. The threshold question of when a national action violates either Article 51 or Article 2(4) of the United Nations

6. The Air Force dealt with this disconnect by simply excepting espionage and enabling activities from the definition of cyber weapons and capabilities, as discussed below – straightforward, but supported by no logical rationale.

7. Cyberspace is "[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." JOINT PUB. 1-02, *supra* note 5, at 92.

(U.N.) Charter continues to spur legal debate regarding military operations in the real world /"meatspace,"[8] and both the United States and the international community continue to analyze incidents on a case-by-case basis, focusing on whether a cyber activity constitutes a "use of force" – prohibited under Article 2(4) – or an "armed attack," which would engender a nation's right to engage in self-defense as articulated in Article 51.[9]

Relying on the work of the authors of the Tallinn Manual, and with Stuxnet as the prime example, it is easier to distinguish those cyber operations that deliver effects equivalent to an "armed attack" under Art. 51 of the U.N. Charter, and they fit relatively easily into the law of armed conflicts analysis.[10] The difficult questions arise with those operations that do not meet the armed attack threshold. Because of all that follows from the answer, the most critical question may be what constitutes a use of force under Article 2(4) of the U.N. Charter.[11]

The most complete analysis of how these thresholds apply to cyber operations is Professor Schmitt's seven-point test, with which he attempts to categorize clear cases.[12] In evaluating whether a use of cyber is a use of force under Art 2(4), Prof Schmitt considers elements like severity, immediacy, directness, invasiveness, measurability and legitimacy in an admittedly complex and context-dependent endeavor.[13] In applying the criteria, Prof Schmitt considers the consequences of cyber operations, and the threat of coercion to evaluate whether, under a holistic analysis, the cyber operations should be considered the equivalent of a traditional armed attack. In his paper there may be some range of cyber operations that are below an armed attack, but still constitutes a breach of the peace and may be subject to action by the United Nations Security Council.[14] The examples he uses to illustrate his arguments still are heavily focused towards kinetic damage. The number of factors in Prof Schmitt's test, and the challenge in evaluating them, both serve to highlight that there is still a broad range of military cyber operations that do not qualify as a use of force under

8. William Gibson made the term "cyberspace" famous in his 1984 book Neuromancer. In that volume, he also used the term "meatspace" to distinguish the real world from the virtual. WILLIAM GIBSON, NEUROMANCER (1984).

9. Article 51 of the U.N. Charter provides that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs." The U.S. interprets this language as permitting self-defense against uses of force that do not rise to the level of an armed attack, a position rejected in the *Nicaragua* case. Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MIL. L. REV. 89, 92-93 (1989). *See generally* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 12, 21-25 (2012), http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf.

10. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

11. It should be noted here that the U.S. maintains the terms "use of force" and "armed attack" are synonymous, but this is not the accepted position in international law.

12. Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

13. *Id.* at 914-915.

14. *Id.* at 927, 934.

international law. As in the physical world, where there are realms of state action which are coercive and unwelcome but clearly understood to fall short of a use of force, we should be able to legally justify cyberspace operations that may violate host-nation law, and may be the subject of diplomatic objection if identified, but can generally be thought of as never reaching either the threshold for use of force or intervening in the ability of a state to exercise sovereignty. For these cyber actions, in order to develop a rational legal foundation that enables military cyber operations, we need to be comfortable with the idea that there is a subset of cyber warfare activities that are not attacks, do not constitute a new form of warfare, and are otherwise consistent with international law. This line of reasoning is more commonly applied to espionage, but as we will discuss, when the actual techniques employed are considered, the distinction between cyber espionage and cyber operations is not as clear.

In particular, the failure to accurately describe what is and what isn't a "cyber weapon" may make it more difficult for law-abiding states to ascertain what, exactly, they should do to ensure their cyber activities comply with the law of war. A rational approach to cyber-warfare may also have the salutary effect of cutting through the hype surrounding the issue, as documented by sensational newspaper headlines and a seemingly endless parade of computer security companies flogging products to protect companies and governments from cyber Armageddon.[15]

These issues are discussed below in the context of operational attorneys trying to articulate the rules in a way that support military operations in cyberspace. This will include a discussion of the mechanism and techniques used in some open source cyber incidents, which will highlight the difficulty, and impracticality, of applying academic niceties in real world operations.

III. EXAMPLES OF CYBER TECHNIQUES

While details of any actual cyber operations may be classified, the examples below are of open-source and publicly available cyber tools, capabilities and operations. One might speculate how these operations could be similar to the actions of nation states in this arena. The examples are offered to highlight the difference between how discussions regarding cyber weapons are conducted in an academic setting and the discussions pertinent to real world operations.

A. Stuxnet

Supervisory Control and Data Acquisition (SCADA) systems are a primary area of national vulnerability to cyber interference. SCADA systems, put sim-

15. *See, e.g.*, Dara Kerr, *Threat of Mass Cyberattacks on U.S. Banks is Real, McAfee Warns*, CNET (Dec. 13, 2012), http://news.cnet.com/8301-1009_3-57559153-83/threat-of-mass-cyberattacks-on-u.s-banks-is-real-mcafee-warns/; Leon Panetta, U.S. Sec. of Def., Remarks on Cybersecurity, Address to the Business Executives for National Security (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

ply, control and manage the operation of utility, transportation and manufacturing systems. Among many other risks, SCADA systems might be manipulated to interfere with the distribution of electricity and fuel, the proper operation of trains and seaports, and the manufacture of heavy machinery. Recognition of the threat to SCADA systems led the U.S. to create the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) under the Department of Homeland Security to bolster defense of the systems.[16] It was just such a SCADA system that was targeted by Stuxnet.

Stuxnet is the name given to a large, sophisticated piece of computer code that was intended to spread both by use of the "AutoRun" feature on thumb drives and by network enumeration. AutoRun was a default feature of the Windows operating system for a long time, though it could be turned off by an administrator.[17] The feature was intended to help computer users by automatically opening any external media that was added to a system. Even casual users will have noticed that when a compact disc is inserted into a computer disk drive the program on the disk often starts to load automatically. The BUCKSHOT YANKEE intrusion set discussed by Deputy Secretary of Defense William Lynn in his *Foreign Affairs* article also took advantage of AutoRun.[18] Similarly, the AutoRun feature gave Stuxnet the ability to span "air gaps" in networks – that is, to jump between networks not physically connected. Careless network administrators who used flash drives to transfer data between unconnected networks introduced malware onto the protected system when Stuxnet used the AutoRun feature to load it onto the air gapped system.

The Stuxnet program as designed was capable of multiple functions. Once installed, it identified its host system, developed network maps of the host network, made copies of itself and distributed them – and had the ability to report back on what it had found. Once the program started, if the system it was on met certain criteria, it took specified actions. Specifically, if the host system was being used to run industrial control systems, and those control systems were being used to control specific centrifuges that matched suspected Iranian uranium processing centrifuges, Stuxnet went to work. The malware caused the delicate centrifuges, spinning at supersonic speed, to speed up or slow down suddenly; the abrupt changes in velocity had the effect of eventually breaking the centrifuges. All the while, another component of the Stuxnet malware was causing the Iranian monitoring software to report the centrifuges were working properly, preventing detection of the problem until it was too late.[19]

At the date of this writing, Stuxnet is the most notorious piece of software

16. *See Frequently Asked Questions*, INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM, http://ics-cert.us-cert.gov/content/frequently-asked-questions.

17. *See* AutoRun, WIKIPEDIA, *available at* http://en.wikipedia.org/wiki/AutoRun. The AutoRun and AutoPlay features were more tightly controlled with the release of Microsoft Windows 7.

18. William J. Lynn III, *Defending a New Domain*, FOREIGN AFF. (Sep.-Oct. 2010).

19. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012) at A1.

routinely characterized as a cyber weapon. Stuxnet had the effect of causing physical damage, and seems from its design to have been intended to cause this damage in the course of its normal operation, thereby meeting most definitions of a weapon, including the one proffered here. But that determination heightens the difficulty for the legal advisor. Ordinary (legal) weapons aren't self-replicating and capable of accidentally and autonomously spreading to the civilian community.[20]

However, Stuxnet is not particularly characteristic of cyber tools. Some of the differences between Stuxnet and other, more prominent "cyber weapons" being used today are discussed below.

B. ZeuS Trojan

ZeuS Trojan is the name given to a family of popular (with cyber criminals) software programs that are part of the larger body of "malware."[21] While computer viruses are generally considered to be malicious software that disrupts the functions of a system, the ZeuS Trojan, like most Trojans, is configured to operate unobtrusively in the background of a system, where it intercepts banking transactions. The Trojan is commonly spread through use of "phishing" or use of unsolicited e-mail that has the code for the ZeuS Trojan disguised as an attachment. It may also be spread by compromise of a web site that serves the software to browsers using specific vulnerabilities in the user's web-browsing software.

Characteristics of the ZeuS Trojan

- Installable program usually spread by phising and website compromises
- Works as a "man-in-the-middle" keystroke logger and form interceptor
- Preconfigured to recognize user access to banking or other websites.
- Reports the user's log-in information (in real time) to a contral controller
- Also allows for remote updaing and execution of downloaded code

If a computer has been compromised by a malicious attachment to an e-mail, and the user logs onto one of the bank websites the program is configured to recognize, the program acts as a proxy and intercepts the logon information typed into the bank's web page. The malware allows the information to go to the bank, so the user is not alerted to a problem, but also sends the information to a command and control server that the distributer of the software may have located anywhere in the world. The controller not only collects the bank data and sends it to the criminal behind the scheme, but also can send updates, issue commands and install additional programs if the criminal chooses.

---

20. Bio-weapons, being illegal, are excepted, though it might be an interesting discussion to review the legal analysis conducted regarding their use to see if it might be applicable.

21. *See* Kevin Stevens & Don Jackson, *ZeuS Banking Trojan Report*, DELL SECUREWORKS (Mar. 11, 2010), http://www.secureworks.com/cyber-threat-intelligence/threats/zeus/; Ben Nahorney & Nicolas Falliere, *Trojan.Zbot*, SYMANTEC, http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99.

While merely tricking someone to install malware and stealing logon information is not an attack in the traditional sense, the software itself is capable of downloading and executing additional code or issuing commands to the infected computer as well. The stolen credentials can also be used to further exploit the target system. Depending on the nature, location or purpose of the compromised system, this may create a potential to deliver significant effects.[22] In the ZeuS Trojan, the purpose of this functionality was to give it the ability to receive updates to prevent detection from new versions of anti-virus programs or to reflect changes in bank websites. The same updating ability, however, would also give the controller the ability to execute other malicious code on the infected system. As a result, if an infected system happens to be the human/machine interface of an industrial control system, the controller may be able to control or damage the underlying SCADA system, and adversely affect the delivery of services, utilities or whatever else the system controls.

C. Poison Ivy RAT

A "remote access tool" or "RAT," is a software application that allows a remote user to interact with a computer system as if the operator had physical access to the system.[23] Poison Ivy is similar to the ZeuS Trojan, but has broader applicability as a general purpose "remote access tool" that is freely available on the Internet. It has primarily been designed as a low footprint tool that can be later configured by downloading modules to the client. Spread in a way similar to ZeuS Trojan and other malware, it is more focused on being customizable and flexible and is used to completely take over a target computer.[24]

Characteristics of Poison Ivy

- Free-ware distributed from an official website
- Operates as "client-server" that allows control of a system by a remote operator
- Capabilities include:
  - Encrypted communication
  - Remote file browsing
  - Process injection
  - Key logging
  - Registry manipulation
  - Screen capture
  - Audio and video capture
  - Password stealing
  - Proxy services
  - Payloads customizable by users

The code required for initial compromise is very small, <10 kilobytes, but once loaded, individual components may be added depending on user requirements.

22. Air Force Predator operators managed to infect the computer system that guides Predators and other unmanned planes, for example. Noah Schactman, *Computer Virus Hits U.S. Drone Fleet*, WIRED DANGER ROOM (Oct. 7, 2011), http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/#more-59492.

23. *See generally* Roger A. Grimes, *Danger, Remote Access Trojans*, SECURITY ADMIN., Sept. 2002, *available at* http://technet.microsoft.com/en-us/library/dd632947.aspx.

24. For a discussion of RATs in general, *see* DMITRI ALPEROVITCH, REVEALED: OPERATION SHADY RAT (2011) (McAfee White Paper), *available at* http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

D. Low Orbit Ion Cannon

Low Orbit Ion Cannon (LOIC) is here just as an example of software that is freely available on the Internet that can make a computer neophyte into an effective "attacker" by allowing the user to participate in distributed denial of service (DDoS) events.[25] DDoS is a very common "attack" that works by flooding a target system with TCP or UDP network packets.[26] The flood of requests overwhelms the target system by filling up available bandwidth, crowding out legitimate requests for resources or overwhelming the target's ability to respond. Users interested in denying service to a target, whether for political reasons, to extort money or just for "the lulz,"[27] can either choose a specific target or pre-configure the software to receive targeting information from an internet relay chat (IRC) server for a coordinated effort. LOIC can deny network resources over a variety of network services, from web to e-mail, and possibly cause a system or service to crash, absent unusual circumstances, it cannot cause any physical damage. Many legal practitioners in the cyber area have opined that a DDoS, other than those unusual cases that cause physical damage, *cannot* amount to a use of force.[28]

Poison Ivy and LOIC at least may be considered a "thing" or, to use Rid & McBurney's phrase, "an instrument of code borne attack."[29] It is possible to examine such things to determine what they are and what they are capable of. With this information, an analysis of whether they fit the traditional notion of a weapon and how their use might be treated under the law of war can be undertaken. These questions are difficult enough. More problematic are those cyberspace operations in which the causative agent is a smart human operator with an intuitive understanding of how the target system works and a knack for social engineering. In these cases, it is very difficult to find the "thing" that is involved that would be the subject of a legal review, especially in a proactive, prior to deployment, sense. To illustrate, it may be helpful to look at some open source cyber operations to illustrate the difficulty.

There are plenty of prankster's tricks that date back to plain old telephone systems (POTS) and facsimile machines that are quite similar to some common cyberspace capabilities. For instance, it used to be considered the height of hilarity to round up a group of friends and have them all "crank call" a certain number. This would have the effect of a denial of service on the affected phone line. The same fundamental idea forms the basis of Internet denial of service

---

25. Information regarding the software is available at the project websites. *LOIC*, SOURCEFORGE, http://sourceforge.net/projects/loic/; *LOIC*, GITHUB, https://github.com/NewEraCracker/LOIC. For background regarding employment, *see Pro-Wikileaks Activists Abandon Amazon Cyber Attacks*, BBC (Dec. 9, 2010), http://www.bbc.co.uk/news/technology-11957367.

26. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both Internet data protocols.

27. An expression referring to doing something for laughs or entertainment value.

28. TALLINN MANUAL, *supra* note 10, at 52.

29. Rid & McBurney, *supra* note 3, at 6.

attacks, where people purposely or accidentally swamp an Internet resource with excessive requests.

Another old standby dates back to the days when the facsimile machine (fax) was a critical piece of office equipment. To deny an office the use of its fax, an individual might tape several pieces of black construction paper into one long sheet the width of a normal sheet of paper. The black sheet would be inserted into the aggressor's fax, after which the target machine's number would be dialed. As the paper passed through the fax, the first page could be taped to the last page, making a single long loop of black paper, constantly feeding through the sending fax. The continuous transmission of a black sheet of paper would both tie up the target line and exhaust the target fax of its toner supply, rendering the fax machine useless until it was resupplied. By itself, this is an irritating prank, but one party to an armed conflict could use it as a form of communications denial supporting other objectives.

In the classic examples set out above, it's difficult to determine what a lawyer would have reviewed as the weapon. It would certainly not be the telephone or the fax, but perhaps the black paper? What could be reviewed for compliance with international law are the operations themselves, the application of a tactic to a target. This same conundrum is present in the following open-source examples of cyberspace attacks. In these cases, too, it is difficult to identify the "thing" that would be characterized as a weapon. And, while the incidents set out here were largely harmless except to the harassed victims, the same techniques could be used to gain control of systems that would control vital national infrastructure, causing effects that could rise to the level of a use of force. For example, a RAT on a SCADA system could be used to over-pressure a gas pipeline, causing it to explode.

E. Sarah Palin Email Hack

The cyber attack on Sarah Palin is a good example of the problematic nature of cyberspace operations. In this case, a young man was deeply concerned that Ms. Palin would be elected Vice President in the 2008 election, and thought to undermine her chances by releasing what he assumed would be the highly controversial contents of her personal e-mail. He knew her account holder was Yahoo, and her user name from her personal e-mail address, gov.palin@yahoo.com. From his personal computer, and using an Internet proxy service called Ctunnel in an effort to hide his activity, he logged onto Yahoo's mail service. Using Yahoo's password recovery feature, he used open source research to correctly guess the answers to the three personal questions required to reset the password. He then posted the contents of her personal e-mail on the internet website 4Chan.[30]

While the actions taken may not seem particularly serious, the underlying

30. Kim Zetter, *Palin E-Mail Hacker Says It Was Easy*, WIRED (Sep. 18, 2008), http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/.

intent was to affect the Presidential election of the most powerful nation in the world. With hindsight, his efforts may seem irrelevant, but if he had been lucky enough to actually find something embarrassing or that resonated with the electorate, or creative enough to use his access to her account to create something embarrassing or that might resonate with the public, he might have sent reverberations throughout the free world.

If this action had been taken by an agent of a foreign power for the purpose of influencing the U.S. Presidential election, it might have been considered a violation of U.S. sovereignty (and thus a violation of international law).[31] That makes it particularly relevant here to ask: where is the weapon? In this case, the hacker didn't use any "malware," but if he had failed in his open source research to compromise Ms. Palin's account, maybe her husband's or daughter's accounts would have been more vulnerable. From one of those accounts, he could have sent Ms. Palin an e-mail that appeared to be from her daughter, with an attachment that contained a tool like Poison Ivy. With that malware, the hacker could have captured Ms. Palin's password as she logged in.

F. HBGary Hack

HBGary is a large cybersecurity firm. In 2011, its Chief Executive Officer (CEO), Greg Hoglund, announced that his company had backtracked through various on-line social media to obtain the names of members of the hacking group Anonymous, and that he planned to provide the names to legal authorities. Unfortunately, he failed to follow a basic rule – before taking on a hacker group, ensure your computer systems are secure.[32]

HBGary ran a company website that used a custom-built content management system (CMS) that was susceptible to an "SQL Inject." A Structured Query Language (SQL) inject is a basic hacking technique that involves sending a piece of code to the target system that it is not expecting and will not be able to handle in a graceful way, resulting in effects the hacker likes and the system designer probably does not. To run the inject, the hackers entered the following Universal Resource Locator (URL) into the HB Gary web server: http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27. This command caused the database server that kept track of registered users to return the user database with all of the website user's names, password hashes, and e-mail accounts.[33] The hackers used a "rainbow table"[34] to identify two users with

31. 1 L.F.L. OPPENHEIM, INTERNATIONAL LAW 430 (9th ed. 1992).

32. Peter Bright, *Anonymous Apeaks:Tthe Inside Story of the HBGary Hack*, ARSTECHNICA (Feb. 15, 2011), http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/; Brad Stone & Michael Riley, *Hacker vs. Hacker*, BLOOMBERG BUS. WK. (Mar. 10, 2011), http://www.businessweek.com/magazine/content/11_12/b4220066790741.htm.

33. A hash is where a password or other piece of data is run through one of a number of algorithms to produce a unique, fixed length number. For example, the common MD5 hashing algorithm takes an arbitrary piece of data, such as an e-mail or a password, and produces a 128-bit value that is effectively unique. It is theoretically impossible to reverse the algorithm. That value can be used to do things like

simple passwords – the CEO and Chief Operations Officer (COO). The CEO also violated a couple of other basic principles of network security – he both reused passwords and ran his personal account with administrator privileges. The CEO was also the administrator of the company's enterprise e-mail account, so his account compromise meant the entire company's e-mail had been compromised. The COO had an account on the server that HB Gary used to store critical backups, but while the account did not have administrator privileges, the server itself was running an unpatched version of Linux with a known vulnerability that allowed the hackers to escalate the COO's privileges into administrative rights and delete all the backups.

HB Gary highlights the lack of a clearly definable cyber weapon in an economically devastating attack against the company. Like the Sarah Palin hack, this relied on tradecraft and social engineering, but clearly would have been considered a "cyber attack" if the U.S. military had thought about using similar techniques under the current definitions.

G. Australia Sewer Hack

Just to demonstrate how physical damage might be caused by a compromised computer, in April 2000, the town of Maroochy Shire, Queensland, woke up to the local creek full of raw sewage, thanks to cyber activity. In this case, it had been an insider. A disgruntled employee of the sewage system installer had his application to work for the county rejected. He retained the logon information to connect to the industrial control systems that ran the town's sewage plant, and used his access to those systems and his knowledge of the plant workings to cause sewage to back up out of the system and flood the town.[35]

If the plant had been a more complicated chemical factory, one that used toxic chemicals in a high pressure vessel for example, a knowledgeable operator with access to the system could have caused substantially more damage just by making use of his remote access to certain computers.

IV. REVIEWING THE WEAPONS OF CYBER WARFARE

Lawyers are deeply involved in DoD planning; significant operations are

---

ensure integrity; if e-mail text gets changed, then the associated hash value will change as well. Rather than store or transmit passwords and risk their compromise, most programs store and transmit the relatively more secure hash values. However, hashes can be vulnerable to both "collisions," where different starting data produces the same hash value, and comparing hashes with the hashes of known data in a "rainbow table."

34. A rainbow table is a pre-computed table that contains known passwords and their hashes. Use of rainbow tables can greatly speed up the process of cracking passwords if the unknown password is in the table because while computing hashes is slow and processor-intensive; comparing two values is relatively quick and easy. *See generally* Brien Posey, *Password Cracking Revisited: Rainbow Tables*, REDMOND MAG. (Sept. 17, 2013), http://redmondmag.com/articles/2013/09/18/password-cracking-revisited.aspx.

35. Tony Smith, *Hacker Jailed for Revenge Sewer Attacks*, THE REG. (Oct. 31, 2001), http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.

subject to multiple legal reviews by dozens of lawyers. At various points in the development of operations, legal advisers review weapons of war and the application of those instruments for the purpose of ensuring there will be no disproportionate negative effect on the civilian population or unnecessary suffering to combatants.[36]

Rather than focusing on the separate review of weaponry, the remainder of this paper discusses the review that assesses the legality of the operation itself. The cyber operation would consist of the proposed target, together with the proposed capability, as well as the techniques planned to achieve the desired effect. The requirement for this operational legal review derives from the DoD directive on the law of war.[37] This final legal review is vital for ensuring the legality of DoD operations, and nothing here suggests this requirement should be altered for cyber operations. In fact, the requirement for this legal review is the critical linchpin supporting the changes to the more generic legal reviews of "cyber weapons" we suggest below.

With a better understanding of the complex and fluid nature of cyber operations, it is easier to understand why resolving issues like the definition of "cyber weapon" are critical to a military's ability to operate in cyberspace. Labeling something as a weapon has far reaching legal, policy and political implications. It also has practical effects, one being that a capability found to be a weapon cannot be used by military forces until it undergoes a legal review as part of the procurement process. With cyber capabilities, the current processes in place to support the procurement system are challenged because of the difference between cyber capabilities and traditional weapons.

At any given time, there are many pieces of code being developed within DoD, and all of them are expected to do something. If the definition of a "cyber weapon" is too expansive, there may not be enough lawyers in DoD to handle the work of reviewing them all. The software may also be obsolete by the time it gets through the review process. Additionally, the snippets of computer code written as software is developed are subject to constant change as bugs are detected, capabilities added, and algorithms tweaked. If each change to the code of a cyber tool requires a new legal review, a legion of operations attorneys will be required to be on call at all times, a requirement that is probably untenable.

On the other hand, it may be difficult to craft an objective, easily applied test to determine when a previously reviewed capability needs a new legal review. Would it be based on the percentage of code that changed, for example? If it is

36. A legal review of all weapons systems is required before acquisition to ensure they comply with international law. THE DEFENSE ACQUISITION SYSTEM, DOD DIRECTIVE 5000.1, at ¶E1.1.15 (2007). A historical overview of judge advocate involvement with U.S. military operations throughout their execution can be found in FREDERIC L. BORCH, JUDGE ADVOCATES IN COMBAT: ARMY LAWYERS IN MILITARY OPERATIONS FROM VIETNAM TO HAITI (2001), as well as in the statements of senior military commanders since the Gulf War era.

37. DEP'T OF DEF., DOD LAW OF WAR PROGRAM, DIRECTIVE 2311.01E (2011). Paragraph 5.7.3 requires lawyers to be available at all stages of planning and execution of military operations.

anything other than a purely objective standard (think "more than five lines of code inserted, deleted, moved or modified"), it may require a lawyer to determine whether a lawyer needs to review the change, which is not helpful. For example, if the standard contains an exception akin to ". . . unless the change is de minimis in its effect . . .", then changes will likely require a legal review to determine whether the change is significant enough to require a new legal review.

Relevant treaty language for the conducting of a legal review can be traced to the Hague Convention (IV), in particular Article 22 of its annexed regulations, which states that the "right of belligerents to adopt means of injuring the enemy is not unlimited."[38] Article 36 of the 1977 Additional Protocol I to the Geneva Conventions of 1949 (AP I) codifies the requirement to conduct legal reviews of all new weapons.[39] While the United States is not a party to AP I, its practice of conducting legal reviews is consistent with and pre-dates the AP I requirement.[40] The U.S. Department of Defense first established a requirement to conduct legal reviews of its weapons, weapon systems, and ammunition in 1974.[41]

So, because both procurement and use of a "weapon" are dependent on its first being subject to legal review, it is crucial that the proper definition for cyber weaponry be chosen. The wrong definition could lead to a failure to comply with international legal standards, if it is too narrow, or an impossibly high standard if it is too broad. Further, an overly broad definition could encompass espionage tools and techniques, subjecting that area to unprecedented and unnecessary scrutiny that would disrupt operations vital to national security.

And since "weapons" are used to conduct military "attacks," an overly broad definition of cyber weaponry may also shape the discussion of how to characterize cyberspace operations in a way that is overly restrictive. For example, if a military force were to acquire the previously discussed Poison Ivy under a weapons analysis, does that create the implication that use of Poison Ivy by itself is an attack? International law prohibits directing military force against civilians and civilian objects. If every cyber capability is defined as a weapon, the use of any of them could lead to the definition of relatively benign actions as attacks. The overwhelmingly civilian nature of most of cyberspace infrastructure means that this might be a serious restriction, prohibiting most potential uses of the capabilities.

---

38. Convention [No. IV] Respecting the Laws and Customs of War on Land, with annex of regulations, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631.

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

40. *Id.* at 35.

41. DEP'T OF DEF. DIRECTIVE 5000.01, *supra* note 37, at ¶E1.1.15 (current location of the requirement); DEP'T OF DEF., LAW OF WAR PROGRAM, DIRECTIVE 5100.77, at 2 (1998) (declaring that procurement authority is established by Directive 5000.01).

While we do not anticipate being able to create bright-line rules that clearly answer all the imponderables either inside cyberspace or outside, the approach discussed in this article will provide a better framework for analysis. The focus of the approach will primarily be answering "what is a cyber weapon?", although the discussion will of necessity touch on other cyber warfare matters, as well and may potentially help elucidate what that term means.

The "cyber weapon" issue is particularly important, as conducting any sort of warfare in the military sense (as opposed to the "War on Poverty" sense) implies the existence of weapons capable of conducting a military attack.[42] If the analogy of land or air warfare is to be extended to a new concept of "cyber warfare," the existence of cyber weapons must be assumed. Arriving at a precise definition of either will help scope the other. Either cyber-war is any warfare conducted with "cyber weapons," or cyber weapons are any weapons used during the conduct of "cyber war."

V. CURRENT APPROACHES TO APPLYING THE LAW TO CYBER WEAPONS

For simplicity's sake, the concern at the heart of this paper may be referred to as the "cyber *weapons*" issue. Because the language used in international agreements is broader, this deserves clarification.

Article 36 of AP I states:

> 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. (emphasis added)[43]

The issue really concerns means and methods, as well as weapons. In our view, however, this additional language does not change the ultimate outcome. For example we could look at a technique such as DDoS and analyze it as a method of warfare. The analysis would involve determining if denying access to a website through a DDoS action could distinguish between civilian and military objects, and whether such an event would cause unnecessary suffering. It is evident that a DDoS *could* be used in a lawful manner. What is difficult is envisioning any cyber technique (i.e., cyber method of warfare) incapable of being used lawfully. Because cyber isn't naturally kinetic, the only conclusion that might be drawn would be that it's *possible* to use any given cyber technique in a manner consistent with international law. Because the conclusion is so

42. Although the popular press often uses the term "attack" in the cyber context in an imprecise way to describe offensive cyber activity, it does have a more precise meaning in international law, and it's that artful use that is addressed here. *See* Protocol Additional to the Geneva Conventions, Aug. 12, 1949, and Relating to the Protection of Victims of Int'l Armed Conflicts (Protocol I), June 8, 1977 (defining attacks as: "acts of violence against the adversary, whether in offence or defence").

43. *Id.* at art. 36.

vague and is basically predetermined, a legal review of generic "cyber methods" seems like square-filling that would do nothing to ensure the protection of the civilian population, which is the goal of the review process.

We might also examine the distribution method separately from the "payload." For example, Stuxnet was delivered by an indiscriminate worm. However, delivery was the only goal of the distribution software so, even though it failed to discriminate between military and civilian targets, it was by no rational definition an attack. The analysis of the delivery mechanism therefore also seems an exercise in futility.

Another approach we might take is analyzing "cyber warfare" writ large as a method of warfare. One meta-opinion analyzing the use of cyber as a method of warfare could be undertaken, and perhaps even one reviewing the legality of using the Internet, if that could be called a method of warfare. There is, perhaps, some merit in paying homage to the requirement to review, but the result of such reviews, isolated from specific operations, will be too general to be of much use. In short, although a discussion of cyber methods of warfare would be fascinating, this article will concern itself with means of warfare, commonly referred to as weapons.

Most simply, a weapon is an instrument used in the course of hostilities. This is unsatisfactory as a definition, both because nearly anything can be used in the course of hostilities, and because it does not provide for a determination of what would be a weapon without reference to a situation of hostilities. That is, an instrument by this standard must be employed in hostilities before the determination can be made.

The most obvious starting place to determine what constitutes a "cyber weapon" is the definition of "weapon" in the physical world. One might think DoD would have an interest in such a definition, but the Department's dictionary neglects to provide it.[44]

In a nod to the subject, reference is first made to the Internet. The website Dictionary.com provides the following definition for the word "weapon": "any instrument or device for use in attack or defense in combat, fighting, or war, as a sword, rifle, or cannon."[45] Rather similarly, according to Wikipedia a "*weapon*, *arm*, or *armament* is a tool or instrument used with the aim of causing damage or harm (either physical or mental) to living beings or artificial structures or systems." Finally, the more traditional Encyclopedia Britannica defines "weapon" as: "an instrument used in combat for the purpose of killing, injuring, or defeating an enemy."

Separately, the U.S. military services have devised their own distinct definitions for a weapon, complicating efforts for a concise uniform definition applicable to the Department as a whole. For the Army, it is instruments and devices "which have an intended effect of injuring, destroying, or disabling

44. JOINT PUB. 1-02, *supra* note 5.

45. *Weapon*, DICTIONARY.COM, http://dictionary.reference.com/browse/weapon.

enemy personnel, materiel, or property."[46] The Navy says weapons are devices "and those components required for their operation, that are intended to have an effect of injuring, damaging, destroying, or disabling personnel or property, to include non-lethal weapons."[47]

The Air Force broke new ground by being the first U.S. military service to issue a regulation specifically addressing the question of how to review cyber capabilities.[48] As the regulation serves as one of the first official U.S. statements on cyber weaponry, it merits a closer look.

The Air Force defines "weapons" as "devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or materiel."[49] As discussed elsewhere in the article, few "cyber weapons" are devices. Rather, they are simply software packages or techniques that provide access to an adversary's computer system. They may exploit unauthorized access to a system or make use of sequences of computer code custom crafted for a particular operation. The Air Force regulation addresses this potential gap, however, by also defining the term "cyber capability." A cyber capability is "any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities."[50] The definition of cyber capability goes on to exclude "a device or software that is solely intended to provide access to an adversarial computer system for data exploitation."[51]

Although none of the definitions discussed above is entirely satisfactory, there is a common theme. Considering all the various definitions of a weapon might lead to a general definition of weapon as "a device intended or designed to cause harm." The intent or design is an important aspect of any technical definition of weapons for military organizations such as DoD. Militaries commonly acquire and use objects that are inherently dangerous and capable of causing great harm, but are not considered weapons, such as bulldozers and blowtorches. These objects are not subject to a weapons review when they are acquired, because they are not obtained with the *intent* they will be used as weapons. Another important consideration is that these items are assumed to be available for use, even in non-combat situations where the use or availability of weapons may be specifically restricted.[52] The point might best be made by examining the humble entrenching tool.

The entrenching tool, or E-tool, is a foldable shovel commonly issued to

---

46. Review of Legality of Weapons , ¶3.a. Army Regulation 27-53, ¶3.a (1979).

47. DEP'T OF THE NAVY IMPLEMENTATION AND OPERATION OF THE DEF. ACQUISITION SYSTEM AND THE JOINT CAPABILITIES INTEGRATION AND DEV. SYSTEM SEC. OF THE NAVY INSTRUCTION 5000. 2E, ¶1.6.1.c (2011).

48. AIR FORCE INSTRUCTION 51-402, *supra* note 3.

49. *Id.* at 6.

50. *Id.* at 5.

51. *Id*. Some of the implications of the Air Force's new regulation are discussed below.

52. For example, during 2004 Tsunami relief efforts in Indonesia and Sri Lanka, the respective ambassadors insisted that military forces not be armed.

infantry troops. The contract specifications for entrenching tools are undoubtedly quite long, but focus on the size, weight, and strength. All the characteristics are relevant to its primary and intended use, which is giving front line troops the ability to create military fortifications. It is not considered a weapon in the acquisition process, and each new variant does not get a weapons review. However, the characteristics that make it useful for digging also make it a good improvised weapon – it is metal, has a pointed end, a serrated edge and is of a size that makes it easy to wield for any purpose. In fact, military hand-to-hand combat instruction contains blocks on how to use the E-tool as a weapon if circumstances call for it. Army Private First Class Anthony T. Kaho'ohanohano was awarded the Medal of Honor for, among other things, killing two Chinese soldiers with an E-tool after he ran out of ammunition on September 1, 1951, while engaged in combat during the Korean War.[53]

With the understanding that a weapon is a device intended or designed to cause harm, the language can now be applied more specifically to cyber capabilities. As we have seen in our examples, there are two aspects of this analysis. The first is whether there is even a device or "thing" in cyberspace operations to analyze; the second is whether the thing causes "harm." The discussion below will illustrate why these are more difficult problems than it might at first seem.

The most obvious problem with isolating the "weapon" in a cyber operation is that most of the time the leverage is software. Not only is software intangible, it is subject to frequent changes; different versions of software can bear little resemblance to each other. For example, think how similar Microsoft Windows 1.0 is to Microsoft Windows 8.1. Other than the name and general function of being an operating system, there are few similarities between the two. The same would be true of software or malware used in a military operation. As the software is edited to meet the evolving objectives of the operation and the targets' defenses, it can change in effect. It would be illogical to conclude that all software that shares a name is the same, regardless of version. However, it would also be impracticable to provide a new legal review each time software is edited. The alternative would be to provide an objective threshold for what magnitude of change requires a new review. For example, an objective standard would be that one percent of the lines of code have been altered. This also fails the logic test, however, as the assessment of whether a change will affect a programs operation must be qualitative rather than quantitative in nature. In sum, modification issues are a much greater issue in the case of software than in the case of physical objects such as kinetic weapons.

Another category of cyber capability that defies characterization under traditional rules might be referred to as "command line tactics." These are procedures followed when entering normal software commands, such as at the

53. Rob McIlvaine, *Korean War Heroes Reflect Conspicuous Gallantry*, ARMY NEWS SERV., Apr. 28, 2011, *available at* http://www.army.mil/article/55695/.

Windows command prompt or from the command console of a router.[54] These actions are not software, but rather are a pattern or series of commands that will yield a desired result. These commands are ordinarily not particularly relevant to an operations discussion, but become relevant when they are facilitated by unauthorized access to a computer system. In other words, performing what are ordinarily perfectly innocent actions on a computer completely changes character when the computer is owned by an adversary and has been accessed using a purloined password. Deleting a file or manipulating data could be a critical part of a military campaign, yet there does not appear to be a weapon involved.[55]

Once the device, or thing, to be reviewed is identified, the next step is determining the intended and proximate effects of using that thing, and comparing those to the effects created by similar objects that are clearly weapons. Even this analysis is not entirely straightforward because, while there are exceptions like Stuxnet that are intended to cause physical effects, the intended and proximate effects of cyber operations are most often entirely contained within cyberspace. Even what would be considered a significant cyber action, such as overwriting the flash memory that stores the basic programming for a router or deleting the contents of a hard drive – both of which could render equipment completely non-functional – causes no visible damage to the equipment, and may be easily repaired or replaced. How far should the rules governing traditional physical effects of weaponry – destruction or damage – be extended by analogy?

The *Tallinn Manual* addresses the question of what constitutes a cyber weapon in Rule 41(2), where it indicates that ". . . cyber weapons are "'cyber means of warfare' that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack."[56] The Manual defines "cyber attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[57] It is important to note that the *Tallinn Manual* expressly excludes the destruction of data from the definition of attack, unless there is a direct connection between the data destruction and death, destruction, etc., as required under Rule 30, or if the data destruction affects the functionality of the cyber system.[58] This is a logical limitation, in that it prevents techniques that merely manipulate data from being

54. *Command Line*, WEBOPEDIA, http://www.webopedia.com/TERM/C/command_line.html. A command line tactic consists of a series of commands issued at the command line by a user, either authorized or not.

55. This could be considered a means or method of warfare. With the broad nature of activity, it would be difficult to define – "electronically manipulating adversary data" or "deleting enemy communications" would be examples. In any event, that is a discussion for another article.

56. TALLINN MANUAL, *supra* note 10.

57. *Id.* at 106.

58. *Id.* at 107-108, 127.

classified as weapons. On the other hand, the Manual's definition of weapon is somewhat overbroad, in that it includes all means that *could* be used for damage, even if there is no intent to actually use them for anything beyond espionage or manipulation of data, for example.

VI. PROPOSED DEFINITION OF CYBER WEAPON

While DoD has no specific definition for weapon, the term is consistent enough in common usage, and in how it is treated under international law, to enable a definition to be cobbled together from extant sources. In that regard, existing law is best captured by defining weapon as "an object designed for, and developed or obtained for, the primary purpose of killing, maiming, injuring, damaging or destroying." This definition, appropriate for kinetic weapons, is also serviceable as a definition for cyber weaponry. To ensure compliance with both international and domestic law, particularly in the absence of clear guidance in cyber-specific operations, it is perhaps most logical to align the definitions relevant to cyber operations with equivalent definitions used in kinetic operations.

This definition is in contrast to the *Tallinn Manual* definition that excludes the "primary purpose" element. In the *Tallinn* construct, even if a capability is never intended to be used destructively, it would require the same level of legal review as a capability only usable as a destructive tool.[59]

Another major advantage of the definition offered here is that is avoids the necessity of trying to ascertain how to review lines of code under a weapons standard. Perhaps the best way to discuss why this is a problem is to use the most developed standard currently in place, which is provided by Air Force Instruction 51-402.

Defining weapons and capabilities as the Air Force does is a problem, as it sets a practically unattainable standard in terms of quantity for cyber legal reviews. Paragraph 1.1.2 of AFI 51-402, notes "all cyber capabilities being developed, bought, built, modified or otherwise acquired by the Air Force . . . are reviewed for legality under LOAC [Law of Armed Conflict], domestic law and international law prior to their acquisition for use in a conflict or other military operation."[60] On its face, this provision requires a new legal review every time a line of code is changed in a computer program determined to be a capability. As this could happen dozens of times during the course of an operation, even many times in a single day, the requirement is impractical, and would unnecessarily hinder a commander's ability to employ timely and effective military power in cyberspace.

The instruction expounds on the required standard in paragraph 1.3.1. "[C]on-

59. On the other hand, the *Tallinn Manual* moves to limit application of the rule by offering employment of a botnet as an example of a cyber means of warfare, leaving aside the code that enabled the user to obtain and marshal the computers forming the botnet. TALLINN MANUAL, *id.* at 119.

60. AIR FORCE INSTRUCTION 51-402, *supra* note 3, at 2.

duct a timely legal review of all weapons and cyber capabilities, where a new weapon or cyber capability at an early stage of the acquisition process, or a contemplated modification of an existing weapon or cyber capability, to ensure legality under LOAC . . . ."[61] As cyber operations often require operators to make changes on the fly, this standard would require an endless series of legal reviews. Further, because security protocols, updates, patches, etc., occur on a frequent basis, every technique will probably require modification before it is actually employed. For the same reason, cyber capabilities are unlikely to be developed and held in reserve, but rather will be created to fulfill a specific operational requirement, and programmers are likely to be contemplating modifications to their products even before they are finished.

By contrast, under the definition presented here, cyber operations that do not constitute an attack under international law would often be conducted without using anything that would be defined as a weapon. This would eliminate the need for a series of legal reviews that would mean little, but would not eliminate the requirement for an operational legal review as described above. The operational legal review would pair the capability with the planned operation, ensuring compliance with international law.

A final advantage of the definition proposed here is that it provides a logical definition of cyber attack, which may then be described as a cyber operation making use of a cyber weapon. More specifically, a cyber attack may be defined as "an operation using cyber means for the purpose of killing, maiming, injuring or destroying." This would make it clear when the laws of war apply to cyber operations, and open the debate on the issues surrounding cyber operations that fall short of a use of force. Such actions constitute the vast majority of cyber operations currently taking place, and doing so with no coherent rules in place to govern behavior.[62]

Although there are advantages to defining cyber weapon as suggested here, there are potential drawbacks, as well. The stricter delineation of cyber weaponry would obviate the need for most legal reviews prior to operational planning. Although the operational legal review would still be required before a cyber technique could be used in an actual operation and would address potential violations of international law, conducting only the later legal review presents the possibility that resources could be wasted in developing code-based capabilities that could not be legally employed. This objection could be ad-

61. *Id.*

62. Press reports indicate the U.S. carried out 231 offensive cyber operations in 2011. Balanced against the $100-500 billion in estimated worldwide losses through cyber misbehavior, this is a tiny number, particularly when the press reported that it was unclear how many of the 231 "offensive" operations were carried out for espionage purposes. Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, WASH. POST, Aug. 30, 2013, at A1; David E, Sanger, *Budget Documents Detail Extent of U.S. Cyberoperations*, N.Y. TIMES, Sept. 1, 2013, at A10; James Lewis & Stewart Baker, CTR. FOR STRATEGIC & INT'L STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE (July 2013), *available at* http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage.

dressed by the conscientious review of cyber *methods* of warfare. For example, states could review the lawfulness of distributing harmful cyber capabilities by computer worm or virus, and could decide that such uncontrolled distribution is unlawfully indiscriminate. Decisions on broad issues of methods of warfare would govern categories of operations, and would have much more practical use than reviews of individual lines of code.

Further analysis of the proposed cyber weapons definition reveals a curious result – cyber would be perhaps the only area of military operations in which a state could proximately cause substantial physical harm without employing a "weapon." This will give even operations-focused lawyers pause because it is exceptional, but it creates no insurmountable legal issues. As noted above, the operational legal review would still address any concerns under international law, whether the concerns arise from the cyber means or method, or the targeting and proportionality of the proposed action. The effect of the operation will still govern whether it would constitute and attack or use of force, even if there is nothing meeting the definition of "weapon" involved. Cyberspace is unique enough to justify this rather unique result.

CONCLUSION

Although the term "cyber weapon" has become part of popular culture, there has been no real consensus on its proper definition. The term has been used to represent conglomerations of computer code that result in anything from slowing down websites to destroying nuclear power facilities. This wide range of possibilities makes it more difficult to oversee cyber operations to ensure compliance with international law and humanitarian standards.

There must be a foundation for legal analysis of those military operations in cyberspace that fall below the level of a use of force other than simply treating them as espionage. The current framework for cyber espionage under international law is becoming increasingly unworkable, while the tendency to conflate all "non-espionage" cyber operations with "cyber attack" unnecessarily confuses the law of war analysis of military operations. The first step of this process should be to develop workable definitions.[63]

Although the need for a definition is clear, some of the definitions that have been proposed by scholars and by DoD are impractical in the context of actual cyber operations. The definition of "cyber weapon" must be both logical and useable for cyber operators and their legal advisers. Of the logical definitions that have been suggested, most fall short of the goal of being useful to operators, because they are either too vague or too broad. Overly vague definitions might require legal reviews of everything procured by the military that could possibly be used as a weapon, which is essentially everything.

63. Some national policy documents relating to military cyber operations, including Presidential Policy Directive 20, may be available to the public. However, it remains a classified document and the authors are not at liberty to discuss the documents or reference versions that may be publicly available.

Over-broad definitions would require reviews of iterative versions of software, which would be operationally impossible.

The definition of cyber weapons should be tied to that of more traditional weapons, addressing only objects whose *primary purpose* is as a weapon, as suggested here. This would permit the use of well-established international standards and is consistent with the approach taken in the *Tallinn Manual*. This practice would meet the needs of military operators, provide them clearer guidance, and continue to provide effective protection for civilians from cyber operations that would be impermissible under international law.