THE PREOPERATIONAL LEGAL REVIEW OF CYBER CAPABILITIES: ENSURING THE LEGALITY OF CYBER WEAPONS

*P.J. Blount**

I. INTRODUCTION

In 2011, the United States Department of Defense adopted a policy, as part of its cyber strategy, that cyber attacks could be treated as an act of war and could possibly warrant a non cyber response.[1] An unnamed Defense Department official, who served as the source for the *Wall Street Journal* story reporting the policy change, stated: "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."[2] This stance opened up a variety of legal questions for the United States, but clarified its position regarding whether cyber attacks could rise to the level of an armed attack, and thus justifying self-defense measures for purposes of international law.[3] Shortly after making this policy decision, the United States Air Force adopted a new instruction that stated that cyber weapons and cyber capabilities would receive a pre-operational legal review.[4] This new policy signified that the United States is willing to play by its own rules and treat its cyber capabilities as potential weapons.

States have a duty to perform a legal review of weapons before they are used in international armed conflict, in order to ensure that the weapons comport with the laws of international armed conflict (LOIAC); this is primarily to determine that the weapons' use does not result in unnecessary suffering of combatants or indiscriminate attacks that damage civilians and civilian property.[5] This article provides a brief overview of the general problems related to the use of cyber capabilities in armed conflict, and then turns to analyzing the requirements of a pre-operational review of cyber weapons.

---

* Research Counsel and Instructor of Law, National Center for Remote Sensing, Air, and Space Law, University of Mississippi School of Law.

1. Siobhan Gorman and Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. JOURNAL, May 30, 2011, *available at* http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

2. *Id.*

3. U.N. Charter, art. 51.

4. *See* United States Air Force, *Legal Reviews of Weapons and Cyber Capabilities*, A.F. INSTRUCTION 51-402 (July 27, 2011).

5. *See generally id.*

II. CYBER WARFARE

Since its inception, the Internet has been intertwined with the military.[6] Its initial structure was built at the Defense Advanced Research Projects Agency (DARPA).[7] However, these systems have changed from a military communication network to a worldwide infrastructure, which underlies a great deal of human, economic, and diplomatic interactions.[8] Militaries have not only treated cyberspace as a tool, but have also adopted it as a domain in which they operate.[9] Cyberspace has the potential to be the newest battleground.[10]

In this context, the United States Department of Defense adopted a new policy for cyberspace, which touts that a cyber attack could amount to the use of armed force, and that armed force could be used to retaliate against cyber attacks.[11] This is not surprising and to some extent anticipated, because States tend to interpret international law in order to best pursue their goals and ensure their own security.[12] The stance does, however, highlight some of the foundational legal questions that apply to the cyber use in armed conflict.

Cyber, at its heart, challenges many of the traditional underpinnings of law in armed conflict.[13] For instance, while the use of force is generally recognized as an illegal act,[14] it may be used in self-defense to an "armed attack."[15] Within this rubric, the question of what constitutes "armed" is paramount to the legality of self-defense, which in turn hinges on the question of what constitutes a "weapon." Parsing out the various ambiguities is not the purpose of this particular paper. However, when militaries begin to operate in new domains, the legal definitions from the law of armed conflict often become difficult to apply.[16] This has already been seen in the 20th century with the addition of air

---

6. *See generally* Barry M. Liener et al., *A Brief History of the Internet*, THE INTERNET SOCIETY, 2011, http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet.

7. *See id.*

8. *See id.*

9. *See* Matt Murphy, *War in the fifth domain*, THE ECONOMIST (July 1, 2010), *available at* http://www.economist.com/node/16478792.

10. *See id.; see also* Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 133 (2005).

11. While the specific language did not make it into the unclassified version of the document, there has been little, if any at all, speculation that this view is not in the classified version. *See generally* DEP'T OF DEFENSE, DEP'T OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (JULY 2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf.

12. In this particular case, the United States is one of the most networked nations in the world. While this leads to a higher quality of life for its citizens, it also means the U.S. could be more vulnerable to cyber attacks due to its reliance on cyber technologies.

13. Antolin-Jenkins, *supra* note 10, at 133.

14. U.N. Charter, art. 2(4).

15. U.N. Charter, art. 51.

16. Aviation technology raised numerous questions in the early twentieth century. *See generally* Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Drafted by a Commission of Jurists at the Hague, December 1922 - February 1923, ICRC, *available at* http://www.icrc.org/ihl.nsf/FULL/275?OpenDocument. The author has written several

and space to the cadre of military operations. Cyberspace is no exception, but its lack of a "physical" setting creates new and unique questions for the laws of armed conflict.

The United States' actions, to some extent, serve not to alleviate the ambiguities in the definitions but more to supersede the need for debate. The declaration that cyber attacks can, under U.S. interpretation, rise to the level of an armed attack serves as an explicit warning to nations employing such tactics, whether for aggressive, defensive, or intelligence uses. In a sense, the U.S. has quashed the need for debate over whether cyber actions constitute force, and moved it to address which types constitute force and what constitutes proper use under the law of armed conflict. This also means that the United States military, which is very reliant on cyber capabilities, must attempt to answer these questions in relation to its own capabilities as well. If the U.S. is going to treat certain actions as attacks, then it cannot use similar capabilities without itself being accused of using illegal force. Making the distinction between capabilities that rise to the level of an attack is critical, due to the military and intelligence community's reliance on cyber capabilities. Review of these capabilities will inform such communities about their own restraints in using these technologies.

III. THE DUTY TO EVALUATE WEAPONS

The best articulation of the duty to evaluate weapons can be found in the Protocol Additional to the Geneva Conventions.[17] Article 36 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.[18]

While the United States is not a party to Additional Protocol I, the U.S. embraced the duty to evaluate, before its articulation in Additional Protocol I, through a Department of Defense Directive in 1974.[19] While it is unclear whether this duty extends to the realm of customary international law,[20] the rule is, to some extent, implied by the rules of armed conflict.

---

articles exploring the problems of the laws of war in space. *See, e.g.*, P.J. Blount, *Limits on Space Weapons: Incorporating the Law of War into the Corpus Juris Spatialis*, PROCEEDINGS OF THE 51ST COLLOQUIUM ON THE LAW OF OUTER SPACE (2009), *available at* http://ssrn.com/abstract=1393321.

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

18. *Id.*

19. *See Remarks of Michael John Matheson,* 1978 *PROCEEDINGS OF THE ANNUAL MEETING (AMERICAN SOCIETY OF INTERNATIONAL LAW 26, 27 (1978).*

20. The *Law of War Documentary Supplement*, published by the United States Army in 2008, includes two documents that discuss the customary international law elements of Additional Protocol I. Both of these documents are silent as to Article 36. *See Additional Protocol I as an*

The Hague Convention states that "[t]he right of belligerents to adopt means of injuring the enemy is not unlimited."[21] This implies some responsibility for States to ensure that the weapons they use do not violate the law of armed conflict. In fact, the underpinnings of international humanitarian law reinforce this idea as its purpose is to "[set] limits on armed violence in wartime in order to prevent, or at least reduce, suffering."[22] If States are not permitted to employ weapons that violate these rules, then there must, at the very least, be an implied duty to evaluate the weapons being developed. This review should have a legal component as the law defines the parameters of acceptable weapons.

IV. THE AIR FORCE INSTRUCTION

Air Force Instruction 51-102 was updated in July of 2011 to "[reflect] a change in the Air Force definition of 'weapon' and [require] a legal review of cyber capabilities intended for use in cyberspace operations."[23] Specifically, the Instruction requires that cyber capabilities, like weapons "being developed, bought, built, modified or otherwise being acquired by the Air Force," be "reviewed for legality under [the Law of Armed Conflict], domestic law and international law prior to their possible acquisition for use in a conflict or other military operation."[24]

The review is a three-step process. It first requires that the weapon or cyber capability be evaluated to determine "[w]hether there is a specific rule of law, whether by treaty obligation of the United States or accepted by the United States as customary international law, prohibiting or restricting the use of the weapon or cyber capability in question."[25] If no "express prohibition" is found, then the reviewing officer must examine two specific questions.[26] The first is "[w]hether the weapon or cyber capability is calculated to cause superfluous injury, in violation of Article 23(e) of the Annex to Hague Convention IV."[27] The second question addresses whether the weapon or cyber capability can target

---

Expression of Customary International Law in UNITED STATES ARMY JUDGE ADVOCATE GEN.'S LEGAL CTR. AND SCH., LAW OF WAR DOCUMENTARY SUPPLEMENT 396 - 97 (2008), *and Memorandum for Mr. John H. McNeill, Assistant General Counsel (International), OSD* in UNITED STATES ARMY JUDGE ADVOCATE GEN.'S LEGAL CTR. AND SCH., LAW OF WAR DOCUMENTARY SUPPLEMENT 399 (2008).

21. Annex to Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, Oct. 18, 1907, *available at* http://www.icrc.org/ihl.nsf/FULL/195?OpenDocument.

22. *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, International Committee of the Red Cross Geneva, January 2006*, 88 INT'L REV. OF THE RED CROSS 931, 932 (2006).

23. United States Air Force, *supra* note 4, at 1.

24. *Id.* at 2.

25. *Id.* at 3.

26. *Id.*

27. *Id.*

a "specific military objective" and, if not, is it "of a nature to cause an effect" on military and civilian objectives without distinction.[28]

Interestingly, cyber capabilities are not termed as weapons yet they will receive the same legal review. Weapons, for the instruction's purposes, "are devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or materiel."[29] Cyber capabilities that require review are "any device[s] or software payload[s] intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities."[30] Conversely, devices and software that are "solely intended to provide access to an adversarial computer system for data exploitation" do not need legal review.[31] This distinction is very important, and meant to protect intelligence-gathering operations. If cyber capabilities for intelligence-gathering were reviewed as weapons, then a State that was the subject of such intelligence-gathering might be able to claim that it was the victim of an armed attack. Intelligence operations themselves are not illegal under international law.[32]

The decision to segregate cyber capabilities from weapons is an interesting one in light of the "armed attack" requirement from Article 51 of the U.N. Charter. It is very likely based on a perceived need to be careful about what to refer to as a weapon. A weapon, in general, implies that an action involving that piece of technology is armed. By referring to these items as cyber capabilities, the Air Force Instruction avoids the implication of "armed," but accomplishes the need for compliance with the Law of Armed Conflict. This could very easily be seen as an attempt to have one's cake and eat it too. However, another interpretation might be that determining when a cyber capability rises to the status of a weapon is difficult; therefore, a legal review of capabilities is necessary.[33] Regardless of the interpretation, the legal review is the same for both weapons and cyber capabilities.

V. SPECIFIC CONCERNS FOR CYBER WEAPONS

As stated, cyber weapons create new problems for both *jus ad bellum* and *jus in bello*. This is because new technology does not fit into the traditional theaters of military operation. While cyber operations are meant to have an effect on the domains of land, sea, air, and space, they do not squarely fit traditional

28. *Id.*
29. United States Air Force, *supra* note 4, at 6.
30. *Id.* at 5.
31. *Id.* at 5.
32. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 208, Cambridge Univ. Press (2004).
33. For example, a cyber attack that shuts down substantial infrastructure could be termed an armed attack. *See* Gorman and Barnes, *supra* note 1. Whereas an attack that causes a computer network failure might be argued to be less than armed because of its lack of real space affects.

conceptualizations of weapons. As a result, when applying the law of armed conflict to contemporary technologies, legal reviews of such weapons address novel issues. This section investigates these issues, utilizing the three questions that legal reviewers must ask when reviewing cyber weapons.

A. Whether the Cyber Capability is Outlawed Due to a Rule of Law

The first question is whether the capability violates international or domestic law.[34] This question addresses pure legality: has the specific capability been prohibited by law. A pertinent example of the kind of international law that might prohibit the technology is the Convention on Certain Conventional Weapons.[35] This convention outlaws certain weapons via protocols that are negotiated and ratified by parties to that treaty.[36] To date, there are four protocols that restrict the use of specific weapons, such as land mines and blinding laser weapons among others, in international armed conflict. However, there are no specific limitations on the use of cyber capabilities that have been negotiated at the international level.

Domestic law could also outlaw specific weapons from military use; however, at this time, no such provision relating to cyber capabilities exists. Yet, there are laws that restrict the military in domestic situations. For instance, the Posse Comitatus Act limits the military and its assets from being used in law enforcement.[37] Any cyber capability employed would need to be technically capable of being restricted to use outside the country, rather than on domestic networks and systems.

B. Does the Capability Cause Superfluous Injury

Next, the evaluator must ask whether the capability causes superfluous injury, which is prohibited in Article 23(e) of the Annex to Hague IV Convention of 1907.[38] The Hague Conventions of 1899 and 1907 were some of the first formal negotiations on the Laws of International Armed Conflict and the resulting conventions are still important documents for these laws. Article 23(e) states that it is forbidden to "employ arms, projectiles, or material calculated to cause unnecessary suffering."[39]

This prohibition is geared toward protecting combatants from weapons that cause unnecessary suffering. Unnecessary suffering is defined as "harm greater

---

34. United States Air Force, *supra* note 4, at 3.

35. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Geneva, 1342 U.N.T.S. 137 (Dec. 21, 2001).

36. *See id.*

37. 18 U.S.C. § 1385 (2006).

38. United States Air Force, *supra* note 4, at 3.

39. Annex, *supra* note 21, art. 23(e).

than that unavoidable to achieve legitimate military objectives."[40] It follows that a weapon will not be outlawed simply because it causes horrendous or mass harm, but instead, such a determination requires balancing the interests of the military objective, the harm caused, and the constraints in a given situation. Weapons are deemed illegal when they cause injuries that could have been avoided in a given situation.[41] In any scenario, military lawyers will compare options to find one that avoids the most suffering.[42] However, in the Air Force instruction's test, the lawyer must evaluate whether the weapon is de facto calculated to cause unnecessary suffering. Examples of these types of weapons are most readily found among those that have been explicitly banned. For instance, the international community has banned the use of blinding lasers; the reason for this "is that its impact – permanent loss of vision – is a severe life-long incapacitation, which is irreversible."[43] Such a weapon is illegal because its purpose is to cause incapacitation that will last long past the end of hostilities.

It is unlikely that a cyber capability would fall into this category. For the most part, cyber capabilities are designed to affect bits and bytes in order to cause real world effects. For a cyber capability to toe this particular threshold would push the constraints of the technology that underlies these sorts of capabilities. While science fiction type scenarios could be postulated, it seems that any real life scenario would necessarily involve a legal review of a particular use in the field of a capability. For instance, a cyber capability designed to shut down infrastructures, such as power stations, would not de facto cause unnecessary suffering, but a particular use of it might.

C. Is the Capability Sufficiently Targetable

The final consideration for cyber capabilities is likely the most critical in the review process for these types of technologies. Legal weapons must be capable of discriminating between combatants and civilians, as well as military objectives and civilian property.[44] The purpose of this rule is to minimize civilian casualties and to minimize damage to civilian property. Most weapons can be used either discriminately or indiscriminately. This does not make the weapon itself illegal, but instead makes a particular use of the weapon illegal. If a weapon is used in an indiscriminate manner, that "does not stain the weapons themselves with an indelible mark of illegitimacy."[45] This prong of the review makes an inquiry into whether there is a legitimate use of the weapon that can properly discriminate between military targets and civilian targets.

---

40. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 1996 I.C.J. 226, 257 (July 8, 1996).
41. DINSTEIN, *supra* note 32, at 59.
42. *See id.* at 60.
43. *Id.* at 73.
44. United States Air Force, *supra* note 4, at 3.
45. DINSTEIN, *supra* note 32, at 55.

The principle of discrimination is embodied in Rule 1 of the International Committee of the Red Cross' Commentary on Customary International Humanitarian Law: "The parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians."[46] This rule requires military actors to ensure that their actions do not target civilians. This, of course, does not outlaw the inevitable civilian casualties; instead, it outlaws attacks that either directly target civilians or attacks that are not limited in such a way as to minimize civilian damage. The reasoning behind this principle is obvious: wanton killing of civilians in an armed conflict between States is considered to be particularly evil. The International Court of Justice has referred to this as an "intransgressible" principle of the Laws of International Armed Conflict.[47]

A civilian is any person not a combatant, and civilian objects are objects that are not military objectives.[48] Civilians, according to the ICRC Rule 5, "are persons who are not members of the armed forces. The civilian population comprises all persons who are civilians."[49] Moreover, the ICRC Rule 5 implies that civilian objects are those that are not military objectives,[50] and Rule 8 states that "military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[51] While there are many different formulations of the content of these terms (a debate that sits outside the scope of this paper), this basic rubric can be used to investigate the challenges for new cyber capabilities.

Cyber capabilities are those that "disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities."[52] These capabilities occur through computer networks, and as such are designed to directly affect the computer software of the target computers. This does not mean that these attacks do not have real world effects, as the intent is to use computer networks to degrade a belligerent's ability to engage in hostilities.[53] A

---

46. ICRC, Customary International Humanitarian Law, Rule 1, *available at* http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule1 (last visited Feb. 14, 2012). *See also* Additional Protocol I, *supra* note 17, art. 51.

47. *Legality of the Threat or Use of Nuclear Weapons*, *supra* note 40, at 257.

48. *See* ICRC, Customary International Humanitarian Law, Rule 5, *available at* http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule5 (last visited Feb. 14, 2012).

49. *Id.*

50. *See id.*

51. ICRC, Customary International Humanitarian Law, Rule 8, *available at* http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule8 (last visited Feb. 14, 2012).

52. United States Air Force, *supra* note 4, at 5.

53. John B. Sheldon, *Deciphering Cyberpower: Strategic Purpose in Peace and War*, STRATEGIC STUDIES QUARTERLY, Summer 2011, 95 (2011) ("This strategic purpose revolves around the ability in peace and war to manipulate perceptions of the strategic environment to one's

prime example of such an attack is the Stuxnet virus that shut down Iranian nuclear facilities. This virus attacked very specific computers that ran specific functions in Iran's nuclear plant. [54] The result was more than just an interference with the Iranian computers; indeed, it caused the real space disablement of the nuclear facilities. Concerns have similarly been expressed about using such technology to shut down infrastructure, such as power stations or dams. Many scholars have taken issue with the doomsday-type forecasting, and claim that these technologies would not be as devastating as is often predicted.[55]

Cyber capabilities could have a widespread effect on civilians. If a computer virus were used to shut down infrastructure such as a dam, then the result could be the death of civilians. The threshold question, then, is whether the technology can be used in such a way that properly distinguishes between civilians and combatants. If the technology shuts down critical infrastructure indiscriminately, then the answer would be no. For instance, shutting down a power station near a major city might result in deaths of that city's civilian population. While this might further war objectives generally, the weapon could be seen as indiscriminately attacking civilians. This could be comparable to shutting down a nuclear reactor that is believed to cover for nuclear weapons development. However, while the reactor might be providing power to civilians, the objective of keeping nuclear weapons out of a combat zone might be such that shutting off that power source is justified, even though causing a reactor meltdown would most likely not be justified. Stuxnet provides an excellent example of a targetable cyber capability.[56] It specifically affected only the Iranian nuclear infrastructure, as opposed to infected nuclear facilities worldwide.[57]

Civilian objects are to be preserved as well. Cyber capabilities create unique challenges for the respect given to civilian objects. This is primarily because the most prominent road for the use of cyber capabilities is the Internet, which is essentially a civilian infrastructure despite its military origins.[58] However, as a result of "use" one can argue that the Internet becomes a place for legitimate military action.[59] Of course, it is more often sub-networks and computers at the "ends" of the Internet that are being targeted. The key question, again, is

---

advantage while at the same time degrading the ability of an adversary to comprehend that same environment."); *See also id.* at 96 ("Cyberspace requires man-made objects to exist.").

54. Spencer Ackerman, *With Stuxnet, Did The U.S. And Israel Create a New Cyberwar Era? [Updated]*, DANGER ROOM, Jan.16, 2011, *available at* http://www.wired.com/dangerroom/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/.

55. *See generally*, Antolin-Jenkins, *supra* note 10, at 144, *and* Jerry Brito and Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, Mercatus Center Working Paper No. 11-24 (Apr. 2011).

56. *See* Ackerman, *supra* note 54.

57. *See id.*

58. *See* Antolin-Jenkins, *supra* note 10, at 132-33.

59. I acknowledge that this is a circular argument: the Internet is used by militaries, so its use makes it a legitimate space for military action.

whether such attacks can be limited to the intended targets. For instance, a cyber capability that is intended to disrupt military networks, but also disrupts civilian financial networks, has not been properly limited. Again, as Stuxnet illustrates, cyber capabilities are technologically capable of discriminating and targeting discrete systems. It will be up to the reviewer to ensure that a particular capability can be properly limited.

VI. OTHER ISSUES

The concept of cyber conflict is a complicated matter. This paper only seeks to investigate the review process for cyber capabilities. There is, however, a rich body of literature that investigates related issues that arise from the laws of international armed conflict. The attorneys doing this work for the military need a high level of technical competence in addition to their grasp of legal concepts. Understanding of the architecture and nature of networks will be a requisite for anyone engaged in the evaluation of cyber capabilities. This might require the military to engage in capacity building so that it can ensure that it has properly trained lawyers.

VII. CONCLUSION

The Air Force Instruction[60] serves as an excellent reminder of the U.S. military's ongoing commitment to its international law obligations. The willingness to evaluate these capabilities in light of international humanitarian law shows that the United States takes seriously the commitment to minimizing damage to civilian objects and preventing civilian suffering. It also serves as a reminder of the strategic ground at stake and the U.S.'s posturing in this arena. The cyber-theater is a valuable one, yet operation in it opens up great risks. The race for cyber power will be one that continually challenges national security, and having the proper, legal tools on hand will be the first step in successful military actions.

60. United States Air Force, *supra* note 4.