
INTERNATIONAL LAW STUDIES

PUBLISHED SINCE 1895

U.S. NAVAL WAR COLLEGE



Organizing for Cyberspace Operations: Selected Issues

Paul Walker

89 INT'L L. STUD. 341 (2013)

Volume 89

2013

Organizing for Cyberspace Operations: Selected Issues

*Paul Walker**

I. INTRODUCTION

The United States dramatically raised the profile of cyberspace operations as a method of warfare when it announced the establishment of the United States Cyber Command in June, 2009.¹ As a sub-unified command of the United States Strategic Command and led by a four-star general, who also serves as the Director, National Security Agency, Cyber Command absorbed the responsibilities of two separate, lower-profile organizations: Joint Task Force-Global Network Operations (JTF-GNO) and Joint Functional Component Command-Network Warfare (JFCC-NW).²

* Commander, Judge Advocate General's Corps, U.S. Navy; Deputy Director, Office of the Judge Advocate General's Information Operations (Cyber) and Intelligence Law Division. The views expressed here are Commander Walker's personal opinion and do not necessarily represent the views of the Department of Defense, the Department of the Navy, the Naval War College or United States Cyber Command.

1. Memorandum from Secretary of Defense Robert M. Gates to Secretaries of the Military Departments et. al, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations 1 (June, 23, 2009), available at <http://fcw.com/~media/GIG/GCN/Documents/cyber%20command%20gates%20memo.ashx>.

2. *Id.* at 1–2.

There were a number of reasons for creating Cyber Command. First, bringing together JTF-GNO and JFCC-NW eliminated deficiencies and gaps between those operating Department of Defense (DoD) networks and those charged with defending the same networks.³ Second, the newly realized efficiencies would result in an increased ability to support global missions with cyberspace operations.⁴ Finally, deficiencies and gaps in DoD's cybersecurity efforts were identified in response to specific intrusion events into DoD networks.⁵ Operation Buckshot Yankee, the DoD response to "the most significant breach of U.S. military computers ever" in 2008, was a key impetus to the standup of Cyber Command, according to then-Deputy Secretary of Defense William Lynn.⁶ Although Cyber Command will "integrate cyberdefense operations across the military"⁷ through its mission to "direct the operations and defense of specified Department of Defense information networks,"⁸ the command also has the responsibility for conducting offensive operations in cyberspace.⁹

In the ensuing three years, Cyber Command reached full operational capability on October 31, 2010.¹⁰ As that occurred, countries around the world established or announced plans to create their own cyberspace commands. Some, such as China, India and Russia, apparently tied the creation of their units directly to the creation of Cyber Command.¹¹ Like the United States, other countries are establishing such a unit in response to

3. Conference Brief, *Cyber War and International Law*, Panel I: An Introduction to Cyber Operations 1 (remarks of Colonel Ron Reed, U.S. Air Force (Ret.)), <http://www.usnwc.edu/getattachment/97cfcf32-5007-4b2c-b1a8-8fb7b8cd2e4f/ILD-Conference-Brief-2012.aspx> (last visited Sept. 30, 2012).

4. *Id.* at 1–2 (remarks of Captain Timothy J. White, U.S. Navy).

5. *Id.* at 1.

6. William J. Lynn III, *Defending a New Domain*, FOREIGN AFFAIRS, Sept.–Oct. 2010, at 97.

7. *Id.*

8. Fact Sheet, United States Strategic Command, U.S. Cyber Command (Dec. 2011), http://www.stratcom.mil/factsheets/Cyber_Command/.

9. *See id.* The third mission assigned to Cyber Command is "when directed, conducts full-spectrum military cyberspace operations."

10. *Id.*

11. *See* Tania Branigan, *Chinese Army to Target Cyber War Threat*, GUARDIAN (London) (July 22, 2010, 2:31 PM), <http://www.guardian.co.uk/world/2010/jul/22/chinese-army-cyber-war-department>; Harish Gupta, *India Setting Up Cyber Command*, MSN NEWS (May 15, 2011, 6:51 PM), <http://news.in.msn.com/national/article.aspx?cp-documentid=5160226#page=1>; *Vice Prime Minister Rogozin Pledges to Set Up Cyber Command in Russia*, CNEWS, (Mar. 22, 2012, 3:15 PM), <http://eng.cnews.ru/news/top/indexEn.shtml?2012/03/22/482544>.

external threats. In the case of South Korea, the threat is cyber actions emanating from North Korea.¹² For Iran, the decision to create a cyber command came a year after the world learned about the Stuxnet virus, which caused damage to nearly one thousand centrifuges at an Iranian nuclear facility.¹³ Still other States had cyberspace operations units that predated the creation of Cyber Command, but whose existence only became public in the years following Cyber Command's establishment. Germany and the United Kingdom are two such examples.¹⁴

These are just the most prominent examples of States that have taken or are preparing to take such a step. There are undoubtedly others who have created such units in greater secrecy or whose action went unnoticed by the Western media. As more and more States create computer network operations or cyber command units, it is appropriate to examine the international law implications for how such units should be organized to conduct operations given the unique nature of cyberspace as an operating domain.

This article examines three areas of the law of armed conflict with implications for the organization and execution of cyberspace operations. Of necessity, given the little information that is available from most States with respect to cyberspace operations and the prominence of the Cyber Command, these areas will be examined through the prism of DoD practices. Part II examines the issue of reviewing cyberspace weapons for compliance with the law of armed conflict, comparing and contrasting the practices of the services that comprise the U.S. armed forces. Part III addresses the issues that occur in organizing for cyberspace operations raised by the requirement to take precautions against the effects of attacks. Specifically, the section will examine the feasibility of clearly separating military objects and objectives from civilian objects in cyberspace. Part IV extends the discussion of precautions against the effect of cyber attacks to a State's conduct

12. See Jung Sung Ki, *Cyber Warfare Command to be Launched in January*, KOREA TIMES (Dec. 1, 2009), http://www.koreatimes.co.kr/www/news/nation/2009/12/205_56502.html (describing suspicions that North Korea was behind massive distributed denial of service attacks occurring against government and industrial sites earlier in the year).

13 *Iran to Launch First Cyber Command*, PRESS TV (Mar. 25, 2012, 6:02 PM), <http://presstv.com/detail/184774.html>.

14 John Leyden, *Germany Reveals Secret Techie Soldier Unit, New Cyberweapons*, THE REGISTER (June 8, 2012, 11:29 AM), http://www.theregister.co.uk/2012/06/08/germany_cyber_offensive_capability/; Colin Clark Monday, *Stratcom Plows Ahead on Cyber*, DOD BUZZ (June 29, 2009, 11:51 AM), <http://www.dodbuzz.com/2009/06/29/stratcom-plows-ahead-on-cyber/>.

of its own cyber attacks, examining principles implicit in the interaction between a number of customary rules within the law of armed conflict to arrive at an explicit conclusion as to how States should organize and prepare for conducting cyber attacks.

II. WEAPONS REVIEWS

Article 36 of Additional Protocol I obligates States that develop, acquire or adopt “a new weapon, means or method of warfare . . . to determine whether its employment would, in some or all circumstances, be prohibited” by the law of armed conflict.¹⁵ The determination is to be made in the course of the acquisition or development of the weapon, means or method of warfare in order to ensure it can be employed within the law of armed conflict.¹⁶ The rule recognizes the practicality of ensuring that a new weapon, means or method of warfare can be legally used before a State expends the often-considerable expense of procuring it.

Of course, it may not be apparent at that early stage whether the weapon will actually be employed as it was intended to be used during the course of its development. In addition, prohibitions on a weapon’s use may be factually dependent and not all of those situations may be foreseeable during a legal review that occurs during the course of acquisition or development. Thus, in order to meet the requirement of examining the weapons legality “in some or all circumstances,”¹⁷ it may be necessary to conduct more than one legal review of the weapon, not only during acquisition or development, but also prior to employment of the weapon by a State’s operational forces.¹⁸

Neither Article 36 nor the *Commentary* on Additional Protocol I define what is meant by the term “weapon, means or method of warfare.” In fact,

15. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 36, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

16. *Id.*

17. *Id.*

18. Harold Hongju Koh, Legal Adviser, U.S. Department of State, International Law in Cyberspace, Keynote Address at the USCYBERCOM Inter-Agency Legal Conference 4 (Sept. 18, 2012) (transcript on file with author). (“The U.S. Government undertakes at least two stages of legal review of the use of weapons in the context of armed conflict—first, an evaluation of new weapons to determine whether their use would be *per se* prohibited by the law of war; and second, specific operations employing weapons are always reviewed to ensure that each particular operation is also compliant with the law of war.”).

the *Commentary* only uses the term “weapon” and does not address potential differences, if any, between a weapon and the ostensibly broader “means or method of warfare.”¹⁹ If one considers that the purposes of the law of armed conflict are to prevent unnecessary suffering to both combatants and noncombatants, as well as to prevent harm to civilians and civilian objects from attacks, weapons are the devices that are used in attacks to cause such suffering. Unlike “weapon,” there is a definition of “attack” as an “act of violence, whether in offence or defense,” contained in Article 49 of Additional Protocol I.²⁰ Given the uncertain application of the law of armed conflict in the cyber domain, recent scholarship has focused on the question of what the definition of “attack” means by way of resulting effects or consequences.²¹ The emerging consensus is that for a military action, whether it occurs in cyberspace or not, to be considered an “attack,” it must result in a violent consequence such as death, injury, or physical damage to property.²² Weapons, then, are the devices used in attacks that cause the deaths, injuries or damage to property. As will be seen, this view is consistent with the definitions of “weapon” used by the armed forces of the United States.

U.S. practice is to conduct multiple legal reviews of weapons in order to meet the requirements of customary international law as reflected in Article 36. The first review is “an evaluation of new weapons to determine whether their use would be *per se* prohibited by the law of war.”²³ In U.S. practice, this acquisition weapons review is generally conducted by the service—Army; Navy, including the Marine Corps; or Air Force—that is pro-

19. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶¶ 1463–1482 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

20. Additional Protocol I, *supra* note 15, art. 49.

21. See, e.g., Michael N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, in INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89, 94 (Raul A. “Pete” Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies) (“A cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects.”); Paul A. Walker, *Rethinking Computer Network “Attack”: Implications for Law and U.S. Doctrine*, 1 NATIONAL SECURITY LAW BRIEF 33, 47 (2010).

22. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rule 30 (Michael N. Schmitt ed., 2013), (“A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”) [hereinafter TALLINN MANUAL].

23. Koh, *supra* note 18, at 4.

curing the weapon. Once a determination is made to employ a weapon, the operation is reviewed to ensure that, in the specific factual context, the weapon's use complies with the law of armed conflict.²⁴ This second review is completed by the unit employing the weapon. For U.S. military cyberspace operations, that unit is currently Cyber Command.

The acquisition review requirement is formally established in Department of Defense Directive 5000.1, "The Defense Acquisition System," which vaguely states "[t]he acquisition and procurement of DoD weapons and weapon systems shall be consistent with all applicable domestic law and treaties and international agreements . . . customary international law, and the law of armed conflict."²⁵ With respect to cyber weapons, this requirement has been implemented differently by each of the Services. In 2011, the Air Force rewrote its instruction to require not only legal reviews of "weapons," but also legal reviews of "cyber capabilities," which are broadly defined to include almost any effect created in cyberspace, not just the types of effects (death and injury to persons and damage to property) caused by weapons.²⁶ The naval service (Navy and Marine Corps) also revised its acquisition instruction in 2011, but did not similarly single out cyber capabilities. Instead, the Navy guidance defines weapons that must undergo legal review as items "that are intended to have an effect of injuring, damaging, destroying, or disabling personnel or property, to include non-lethal weapons."²⁷ The Army's instruction is older, being last revised in 1979. It also focuses on items that have "an intended effect of injuring, destroying, or disabling enemy personnel, materiel, or property" as weapons.²⁸ Army practice has been to conduct acquisition legal reviews of cyber capabilities if one is requested, but not as a matter of course. Given that the Air

24. *Id.*

25. Deputy Secretary of Defense, DoD Directive 5000.01, The Defense Acquisition System encl. 1, ¶E1.1.15 (2003, current through Nov. 20, 2007), available at <http://www.dtic.mil/wbs/directives/corres/pdf/500001p.pdf>.

26. Secretary, Department of the Air Force, AFI 51-402, Legal Reviews of Weapons and Cyber Capabilities (2011), available at <http://www.fas.org/irp/doddir/usaf/afi51-402.pdf> [hereinafter AFI 51-402].

27. Under Secretary of the Navy, SECNAVINST 5000.2E, Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System ¶ 1.6.1.c (2012), available at <http://www.acquisition.navy.mil/content/download/7754/35836/.../5000+2e.pdf>.

28. Headquarters, Department of the Army, Army Regulation 27-53, Review of Legality of Weapons Under International Law ¶ 3.a, Jan. 1, 1979, available at <http://www.fas.org/irp/doddir/army/ar27-53.pdf>.

Force instruction is the only one to single out cyber capabilities, it is instructive to examine that guidance in more detail.

First, it is important to understand that the Air Force instruction does define “weapons” in a manner similar to the other Services: “devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or materiel.”²⁹ It then goes on to separately define “cyber capability” as “any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities.”³⁰ The only exception to the breadth of this definition is a “device or software that is solely intended to provide access to an adversarial computer system for data exploitation.”³¹ Otherwise, the full review procedures provided in the instruction apply equally to both weapons and cyber capabilities, including any and all modifications to those weapons and cyber capabilities. Thus the Air Force instruction meets the requirements of Article 36 by basically requiring the same type of review for the same types of weapons as the other Services. The guidance to also review cyber capabilities is not required by Article 36, but is a policy choice made by the Air Force. Of course, nothing in the law of armed conflict prohibits States from doing more than the minimum required by those laws. In this case, however, the additional review requirements do very little to advance the purposes of the law of armed conflict and, in fact, result in misapplying its principles. In addition, by not limiting the legal review to those cyber capabilities that are intended to cause destruction of property, deaths or injuries, the over-inclusive definition unnecessarily impedes operations, particularly given the Air Force requirement to conduct a new legal review for any modification of a cyber capability.

As discussed earlier, weapons reviews are conducted to ensure they do not violate prohibitions against unnecessary suffering to combatants and noncombatants, as well as ensuring that the use of the weapon does not result in indiscriminate attacks on civilians or civilian objects, this latter purpose is embodied in the principle of distinction. The problem with the Air Force approach to having all cyber capabilities reviewed is that most of the capabilities acquired will not have the effect or intent of causing any human suffering, much less death or injury. Other than the possible destruction of adversary computer systems, the other types of capabilities that

29. AFI 51-402, *supra* note 26, attachment 1.

30. *Id.*

31. *Id.*

must be reviewed—those that disrupt, deny, degrade, negate or impair computer systems, data, activities or capabilities—in most cases, if not all, will have little to no destructive impact on property. Where there is no intent or ability for the cyber capability to produce the same effects as a weapon used during an attack, then the legal review becomes a needless exercise in paper production.

From an operational perspective, such unnecessary administrative requirements impede the ability to conduct operations in a timely manner, particularly in the area of cyberspace operations where exhortations to move at “net speed” predominate. As a policy matter, it is understandable to place an excess of caution into this developing area and, ideally, operational impacts of extra review requirements are limited when the reviews occur during the acquisition process prior to procurement and deployment to or by operational forces. Unfortunately, the Air Force instruction does not mitigate the operational impact, but, instead, exacerbates them by requiring that cyber capabilities that are modified must undergo a new legal review.³² This new review must be performed within Air Force channels, even if the capability has been operationally deployed. The instruction also does not provide a *de minimus* exception that would permit minor alterations to go unreviewed, even if the alteration does not change the effects to be delivered by the capability in any way. This is a real problem for the conduct of operations. Unlike kinetic weapons, cyber capabilities are routinely modified during the course of employment to account for changes in the operational environment, new versions of operating systems, software updates, changes to anti-virus software, and installation or updating of system firewalls. These types of alterations or modifications, where there is no change to what the capability does, are best left to the operational legal review prior to employment, rather than reinserting them into the acquisition process.

For States organizing for cyberspace operations, an examination of U.S. practice demonstrates the best way to comply with the requirement to conduct legal reviews of new weapons. Cyber capabilities should only undergo a legal review as a “new weapon” when the cyber capability is developed with the expectation or intent that its use will result in death, injuries, or damage or destruction of property. This is consistent with current practice with respect to kinetic weapons and is the approach taken by the U.S. Army and the naval service. The law of armed conflict does not require legal

32. *Id.*, ¶ 1.3.

reviews of all new, and newly-modified, cyber capabilities, as is the current Air Force practice. Instead, cyber capabilities whose use is not expected or intended to result in death, injuries or damage to property should only be subjected to a legal review at the time they are employed as part of the legal review undertaken to ensure that the operation as a whole complies with the law of armed conflict.

III. PRECAUTIONS AGAINST THE EFFECTS OF ATTACKS

When preparing to conduct cyberspace operations, States need to be cognizant of the obligations that the law of armed conflict imposes with respect to protections for the State's own populace. Applying these obligations in cyberspace operations yields different outcomes than those that result from preparing for kinetic operations. Instead of focusing on physical separation of civilians and civilian objects, States that undertake cyberspace operations may need to focus on conducting these operations in such a way that civilian cyber objects are not mistaken by potential adversaries for the State's own cyber military objects and objectives.

The general obligation to take precautions against the effects of attacks occurring within a State's own territory is contained in Article 58 of Additional Protocol I and is written in distinctly "kinetic" terms. It is a three-part obligation that involves "remov[ing] . . . civilians and civilian objects . . . from the vicinity of military objectives";³³ not "locating military objectives within or near densely populated areas";³⁴ and taking "other necessary precautions to protect . . . civilians and civilian objects . . . against the dangers resulting from military operations."³⁵ Of these three, the easiest one to apply directly to cyberspace operations on its own terms is the third one, to take necessary precautions to protect against the dangers resulting from military operations. In the kinetic sense, the commentary on this article makes clear that, when drafted, this portion of the article referred to a State's provision of civil defense measures for its population, such as bomb shelters.³⁶ The commentary also discusses a State's provision of civil defense services and the training and equipping of civil defense forces. In the context of cyberspace operations, cybersecurity measures undertaken by a State to protect civilian cyber infrastructure are equivalent to the types of

33. Additional Protocol I, *supra* note 15, art. 58(a).

34. *Id.* art. 58(b).

35. *Id.* art. 58(c).

36. See COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 19, ¶¶ 2239–57.

civil defense measures contemplated by sub-paragraph (c) of Article 58. Of course, unlike State-sponsored and State-provided civil defense measures, there are a multiplicity of means and mechanisms available for undertaking cybersecurity measures. What Article 58(c) makes clear, though, is that at least to some extent the obligation is a State responsibility and is not something that can be left solely to the private sector to implement. How such measures are to be implemented by States is left to their discretion, but Article 58 makes clear the State's obligation to do something.

The other two provisions of Article 58 concern physical separation between military and civilian objects. This obligation to clearly separate and distinguish between civilian objects not subject to attack by an adversary and military objects that are properly subject to attack serves to aid in the adversary's ability to adhere to the law of armed conflict principle of distinction. The obligations contained within Article 58 are not absolute, however. Instead, they must be undertaken "to the maximum extent feasible," which is described in the *Commentary* as not being required "to do the impossible."³⁷ Over time, a consensus has emerged that the feasibility requirement means that States must do what is practicable and are not required to take steps that are impracticable. The practicality approach is taken by the numerous compilations of customary international law applicable to specific warfighting domains, such as the *Air and Missile Warfare Manual*,³⁸ the *San Remo Manual*³⁹ and with respect to cyberspace operations, the *Tallinn Manual*.⁴⁰

On the flip side of the obligation to segregate military from civilian objects is a requirement not to intentionally intermingle such objects, particularly if the goal is to use an object's civilian or other protected status as a means of protecting the military object from attack. On this aspect of precautions against the effects of attacks, the *Air and Missile Warfare Manual's* discussion of customary international law is explicit: "Belligerent parties subject to air or missile attacks must, to the maximum extent feasible, avoid locating military objectives within or near densely populated areas, hospi-

37. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 19, ¶ 2245.

38. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 42 (2010), available at <http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf>.

39. SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA ¶ 46.3 (Louise Doswald Beck ed., 1995).

40. TALLINN MANUAL, *supra* note 22, at 147.

tals, cultural property, places of worship, prisoner of war camps, and other facilities which are entitled to specific protection. . . .”⁴¹ Examples of State action violating this obligation occurred during the Gulf War to oust Saddam Hussein’s forces from Kuwait. The Iraqi Air Force repeatedly removed combat aircraft from airfields and located them next to mosques within populated areas. Despite this intentional attempt to shield them from bombing, the aircraft remained valid military targets subject to attack, with any damage that might occur to the mosque required to be accounted for within the proportionality analysis by the attacking State. Although this example involves the intentional relocation of a military object next to a civilian protected object, the law of armed conflict also prohibits States from misusing the protected status of civilian objects during the course of attacks.

The question then becomes, what measures are practicable for States to take in separating their military cyber objects from civilian cyber objects. At first blush, it may not seem practicable at all given the ubiquitous nature of cyberspace. After all, the Internet grew out of a project started by the Defense Advanced Research Projects Agency, with an original intent of providing for redundant communication paths. From quite modest beginnings has grown a global phenomenon, with most of the supporting infrastructure in the hands of commercial entities. Cyberspace, the overarching term for not just what is known as the Internet, but the interaction of all connected networks and systems is heavily used by governments; industry, including government contractors; businesses, large and small; and by individual citizens of every country. Often, military communications (usually heavily encrypted) are traveling with and alongside all these other communications, particularly across the backbone infrastructures owned by what are known in the United States as “Tier 1 Internet Service Providers” and their equivalents in other countries.

At least one commentator who has written extensively in this area has declared that in the context of cyberspace operations “segregation of military and civilian objects during an armed attack [is] unfeasible.”⁴² Having concluded that it is not possible for States to meet the obligations of Arti-

41. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 42 (2009) [hereinafter AMW MANUAL].

42. Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEXAS LAW REVIEW 1533, 1535 (2010).

cle 58(a) and (b),⁴³ his analysis focuses on the Article 58(c) obligations imposed on States to take cybersecurity measures to secure their civilian populations and companies from the effects of cyber attacks.⁴⁴ In a similar fashion, the newly-published *Tallinn Manual's* Rule 59 on "Precautions against the Effects of Cyber Attacks" focuses on Article 58(c)'s requirement to take precautions to protect civilians and civilian objects from dangers arising from cyber attacks, and does not specifically address the physical differentiation addressed in Article 58(a) and (b).⁴⁵ The commentary on the *Manual's* Rule 59 makes clear that the Group of Experts that authored the *Manual* viewed the obligations of Article 58(a) and (b) as subsumed within the rule they crafted.⁴⁶ In their view, sections (a) and (b) of Additional Protocol I's Article 58 are redundant with section (c). The commentary does mention actions such as "segregating military from civilian cyber infrastructure,"⁴⁷ but its only substantive discussion of the concept is to make the point that "[i]t may not always be feasible for parties to the conflict to segregate potential military objectives from civilian objects."⁴⁸ The focus of the *Tallinn Manual's* commentary on Rule 59 is very much on what it characterizes as "passive precautions,"⁴⁹ rather than the arguably more active requirements of the other two sections of Article 58. Omitting a separate rule emphasizing and discussing the need for States to ensure physical separation of military from civilian cyber infrastructure unfortunately deemphasizes that aspect of the customary international law requirement to take precautions to protect their civilian populations from the effects of cyber attacks. Rather than downplaying this requirement, where the risk to civilian objects is as prevalent as many assume it is during cyberspace operations, the better course would have been to provide a number of more specific rules addressing these requirements in the specific cyber context. This was the approach taken by the *Air and Missile Warfare Manual*, which derived multiple rules addressing physical separation of military targets from civilians and civilian objects.

It is important, though, to differentiate between military cyber objects and dual-use objects, such as power plants or air traffic control systems,

43. *See id.* at 1542–52.

44. *See id.* at 1552–55.

45. TALLINN MANUAL, *supra* note 22, at 146.

46. *Id.*

47. *Id.*

48. *Id.* at 147.

49. *Id.*

that may be valid military objectives for attack by virtue of the fact that their nature, location, purpose and use makes an effective contribution to military capability. In many respects, dual-use objects, by their very nature and definition, are not subject to segregating their military value from their civilian nature or often from their civilian surroundings. But while Article 58's obligations are directed at both dual-use and sole-use military objectives, the above discussion makes clear that there is too much focus on dual-use objectives and not enough focus on those that are purely military in nature, whether fixed or mobile.

In cyberspace, State practice, particularly that of the United States, makes clear that it is feasible to separate purely military objectives from civilian objectives, at least up to a point. The United States military uses multiple, dedicated networks to conduct administrative, logistical and operational activities.⁵⁰ The three best-known networks are the Non-Classified Internet Protocol Router Network (NIPRnet, which carries information classified up to and including Sensitive but Unclassified), Secret Internet Protocol Router Network (SIPRnet, which carries data classified up to and including the Secret level) and the Joint Worldwide Intelligence Communication System (JWICS carries data classified up to and including Top Secret/Sensitive Compartmented Information). JWICS and SIPRnet are secure data transmission services, including voice over Internet Protocol services used for the transmission of classified information between DoD entities and between DoD and other parts of the U.S. government. Both networks are used for transmitting e-mail and web services, and for file transfer operations. SIPRnet is the main transmission method for operational command and control systems, such as the Global Command and Control System and the Defense Message Service used to communicate at the tactical and strategic levels between DoD commands.

The NIPRnet is an unclassified data service that uses the Internet Protocol for connecting to the public Internet. Like the two classified networks, the NIPRnet provides a transmission method for e-mail applications, web services and file transfers. The NIPRnet provides DoD commands and agencies with protected access to the Internet through a limited number of controlled Internet access points, or external network gateways. Protected, secure access between unclassified networks of DoD agencies, non-DoD agencies and departments, and the intelligence community oc-

50. The facts in the next two paragraphs are drawn from the website of the Defense Information Systems Agency, <http://www.disa.mil> (last visited Sept. 30, 2012).

curs through NIPRnet Federated Gateways. These two types of gateways serve to screen DoD's unclassified networks from the broader Internet and permit implementation of perimeter protection services for DoD networks, including the ability to filter web content and provide "secure DoD-wide Domain Name Service."⁵¹ These activities serve to create "a clear boundary between DoD and others . . . and gives DoD some ability to maneuver at the boundary in response to cyber attacks."⁵²

Although there are many military objectives (dual-use or otherwise) in cyberspace that are inextricably intermingled with civilian cyber objects, as has just been illustrated, there is a very substantial core of military cyberspace activity that occurs on and across dedicated military networks and systems. Here we have an intersection with the *Tallinn Manual's* Rule 50, "Clearly Separated and Distinct Military Objectives," because these networks, most particularly the NIPRnet, present "clearly discrete cyber military objectives" even though they are connected to and integrated with cyber infrastructure used for civilian purposes. Thus, it is incorrect to characterize the Internet or even large portions of it as "dual-use" simply because it happens to carry military information alongside and with civilian information. In part, this is due to the fact that it is nearly impossible to determine the location and military significance of those communications at any given moment and concomitantly act against them. With respect to targeting U.S. infrastructure, characterizing the Internet as "dual-use" would be particularly problematic given the fact that the military networks discussed above are available for discrete targeting to achieve the same objectives.

For the organization of cyberspace operations, the object lesson is to ensure the use of dedicated military networks and systems for cyberspace operations that support the operations of a State's armed forces. Not only are such dedicated systems more easily defended, they also present the type of clearly separate and distinct military objective properly subject to attack. Dedicated military networks serve, therefore, to establish a virtual distinction akin to the physical separation or relocation that are the type of precautions against the effects of attack contemplated in the Article 58(a) and (b).

51. *Sensitive but Unclassified IP Data*, DISA, <http://www.disa.mil/Services/Network-Services/Data/SBU-IP> (last visited Sept. 30, 2012).

52. *Id.*

IV. ORGANIZING TO CONDUCT CYBER ATTACK: MAKING THE IMPLICIT EXPLICIT

As States organize their forces to conduct cyber attacks, there is a need to make explicit that which is currently only implicit in the rules. Namely, that cyber attacks—those actions in cyberspace that are proximately intended to cause death, injuries or destruction of property—must not, to the maximum extent feasible, occur from, or be perceived as occurring from, civilian cyberspace objects such that a State responding to such cyber attacks would be induced to improperly direct its response against civilian cyber objects, whether in the attacking State or another State, rather than legitimate military objects and objectives. In other words, States must take care not to misattribute their cyber attacks to otherwise innocent civilian cyber objects and must segregate as much as they can the modes of conducting cyber attacks from civilian infrastructures. The purpose is to organize in such a way as to essentially take precautions against the effects of cyber attacks on a State's own civilian objects and objectives by ensuring they are not jeopardized by the manner in which that State conducts its own cyber attacks. The remainder of this section will discuss the rules from which this formulation is drawn, discuss the practicality of achieving such a solution given the previously discussed attributes of cyberspace and also discuss the operational practicalities that may result from conducting cyber attacks in this manner.

Article 57 of Additional Protocol I addresses the precautions to be taken by States during the planning and conduct of attacks. Other than the first paragraph, however, Article 57 discusses the measures an attacking State must take—the principles of distinction and proportionality—with respect to the objects of those attacks, with the presumption that such attacks are occurring in the territory of another State. Article 57(1) provides a more generic statement applicable to precautions in attack: “In the conduct of military operations constant care shall be taken to spare the civilian population, civilians and civilian objects.” The commentary on Article 57 notes that this paragraph states a “general principle which imposes an important duty on belligerents with respect to civilian populations”⁵³ without distinguishing where those civilian populations are located. Here, the implication is that the general principle is applicable whether the civilian population is

53. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 19, ¶ 2191.

located in the State to be attacked, the attacking State or in a third State, without regard to whether that State is also a party to the conflict.

The previous section provided an extensive discussion of precautions against the effects of attacks required by Article 58. For purposes of this discussion, it should be noted that the requirements of that article refer to the precautions to be taken by a State with respect to its own population in order to mitigate the effects of attacks from another State. Although the text of the article does not directly address the issue presented in this section, it is implied in the article's application to situations involving certain types of military objectives, specifically weapons systems. One of the rationales for requiring, to the extent feasible, that weapons systems not be based or located within populated areas is that those particular military objects will be given a higher priority in targeting by the enemy precisely because they are the source of a State's own attacks against that enemy.

There are a number of customary international law rules that prohibit using specially protected places for purposes, such as the initiation of attacks, that would expose those places or objects to destruction or damage. For instance, there are well-developed rules against using cultural property and places of worship "in support of the military effort."⁵⁴ A similar customary international law rule is recognized with respect to medical units and personnel (including medical aircraft, ambulances and hospitals), though it is usually phrased in terms of whether those units are used to "commit, outside their humanitarian function, acts harmful to the enemy."⁵⁵ As these examples show, the law of armed conflict has long recognized, or at least felt the need to highlight, the need for specifically stated prohibitions on the use of certain protected places and personnel in the conduct of military operations in a manner that may expose those protected places and personnel to dangers from attack.

The lack of a similar specific prohibition on the use of all dedicated (not dual-use) civilian objects during the course of military operations may seem, at first glance, a surprising oversight. It may well be, though, that to the drafters of law of armed conflict treaties, particularly Additional Protocol I; there was no need to codify what was likely the most basic matter of common sense. After all, Additional Protocol I is replete with formulations of customary international law whose base presumption is the duty of State parties to protect civilians and civilian objects from the dangers of armed

54. Additional Protocol I, *supra* note 15, art. 53(b).

55. AMW MANUAL, *supra* note 41, rule 74.

conflict. The commentary on Article 58 even goes so far as to state an expectation that States “must also cooperate by taking all possible precautions for the benefit of their own population as is in any case in their own interest.”⁵⁶

Unfortunately, international law has not reached the point at which common sense reigns supreme with regard to cyberspace operations. Although the United States recognizes the applicability of the law of armed conflict to cyberspace operations and there is an emerging consensus among academics on this point as demonstrated by the recent publication of the *Tallinn Manual*, not all States share this view and still other States view the law of armed conflict’s application as limited in nature, requiring new treaty law dedicated to these types of operations. These topics are an ongoing subject of discussions between the United States, China, Russia and other nations within the Group of Governmental Experts meeting under the auspices of the United Nations. Further complicating these matters, while there is a great deal of cyber activity ongoing, with much of it attributed to State actors, there has only been one even arguable instance of a cyber attack—the Stuxnet virus that operated against Iranian nuclear centrifuges. Probably, in part, because the Iranians never formally reported the results of Stuxnet as a use of force or an armed attack, the authors of the *Tallinn Manual* have even gone so far as to state that “[n]o international cyber incidents have, as of 2012, been unambiguously characterised by the international community as reaching the threshold of an armed attack.”⁵⁷

The custom and practice of States to this point in the cyberspace revolution has been much more focused on conducting espionage and exploitation activities in cyberspace, rather than its use as a means to conduct attacks. Although there is much public speculation about which States are behind specific activities, fueled by an increasing forensic competition between antivirus vendors such as Kaspersky, Symantec and McAfee, these activities are occurring in a manner such that they are not attributable to the sponsoring State. In his keynote address at the Naval War College’s 2012 “Cyber War and International Law” conference, Professor Goldsmith addressed the characteristics of the cyber problem “that upend the traditional system,” including the “difficulty of attribution.”⁵⁸ Similarly, in his September, 2012, remarks at the Cyber Command legal conference, Harold

56. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 19, ¶ 2240.

57. TALLINN MANUAL, *supra* note 22, cmt. to rule 13, ¶13.

58. Conference Brief, *supra* note 3, at 4 (Keynote Address, Jack Goldsmith, Professor, Harvard Law School, National Security Law and Cyberspace).

Koh, Legal Adviser for the U.S. Department of State, discussed the challenges presented by the dual-use nature of the cyberspace environment and the difficult technical, policy and legal questions presented by attribution in cyberspace.⁵⁹ At the same time, Koh also downplayed their uniqueness to the cyber domain, stating that “[t]hese questions about effects, dual-use and attribution are difficult legal and policy questions that existed long before the development of cyber tools.”⁶⁰

Although the non-attributable manner of conducting espionage and exploitation activities in cyberspace is instructive as to how States may carry out cyber attacks in the future, it is not necessarily illustrative and should not be viewed as dispositive at this point in time. It is one thing to carry out espionage and exploitation activities in a manner that intermingles and hides among the civilian infrastructure of cyberspace and the Internet. That is, after all, exactly how espionage is conducted between nations in the physical world, though generally the spies are physically present on the territory of the other nation. The ten-member Russian spy ring discovered operating in various U.S. East Coast locations in 2010 is but the most recent example.⁶¹

It is quite another thing for States to routinely conduct military operations that cause death, injury or destruction of property during the course of an armed conflict in a manner that is not attributed to the State actor as a matter of course. Setting purely domestic considerations aside, as cyberspace operations move closer and closer to a demonstrated capacity to cause the same type of deaths, injury to persons and destruction of property as kinetic weapons, there will be substantial pressure on military forces to move away from the methodologies of espionage and exploitation in carrying out these cyber attacks. This pressure will occur not only because of the need to comply with customary international law as embodied in the articles of Additional Protocol I discussed earlier, but also because of the need for States to accept responsibility for their actions and the actions of their armed forces during the course of armed conflict. Again, without any available examples of cyber attacks, there is no ability to examine actual State practice in this area. This does mean, however, that there remains room and opportunity for States to conform their future cyberspace operations to the need to keep the military sources of their cyber attacks segre-

59. Koh, *supra* note 18, at 6.

60. *Id.*

61. See, e.g., Scott Shane & Charlie Savage, *In Ordinary Lives, U.S. Sees the Work of Russian Agents*, NEW YORK TIMES, June 28, 2010, at A1.

gated from civilian cyber infrastructure, always, of course, to the maximum extent feasible.

As with the earlier discussion about precautions against the effects of cyber attacks, the question then arises whether it is feasible to conduct cyber attacks from a military cyber infrastructure that is segregated from civilian cyber infrastructure and possibly attributable as such. Given the existence of the dedicated NIPRnet that is virtually segregated from other portions of the civilian Internet infrastructure, the question as to feasibility of using separate military networks to conduct cyber attacks is an unqualified “yes.” Another solution, relying on a component portion of the NIPRnet, was proposed some years ago in an *Armed Forces Journal* article.⁶²

In that article, Colonel Williamson advocated using the af.mil network (the Air Force portion of the NIPRnet) to create a powerful robot network of computers (botnet) that could be used to “direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic.”⁶³ In Williamson’s conception, this ability to “carpet bomb in cyberspace” would function as the cyberspace deterrent that the United States lacks. Building this botnet could occur by using the Air Force’s existing servers and computers housing the service’s intrusion detection systems or the botnet could be created by re-purposing the thousands of computers removed from service every year as part of the Air Force’s annual technology refresh program. Those re-purposed computers could then be networked together using botnet software and made to deliver offensive effects for theater commanders. As the system matures, Williamson envisioned adding .mil machines from other portions of the NIPRnet and possibly computers from other U.S. government agencies.

Although such a system (and others like it) is certainly feasible, it may not be operationally practicable. For instance, the same Internet access points and federated gateways that provide the ability to provide protection at the interface with the civilian Internet would act as potential chokepoints that are easily mapped. Once known, the access points, as well as the system of botnets, may be easily defended against by blocking and filtering by an adversary. Williamson acknowledges the technical and engineering chal-

62. Charles W. Williamson III, *Carpet Bombing in Cyberspace: Why America Needs a Military Botnet*, ARMED FORCES JOURNAL, May, 2008, at 20, available at <http://www.armedforcesjournal.com/2008/05/3375884>.

63. *Id.* The remainder of this paragraph is drawn from this article.

lenges, but understands that those problems can generally be overcome by technical solutions.⁶⁴

The issue of operational impracticability raises an interesting issue with respect to whether or not a technical solution remains feasible. In such a situation, a State would be in the position of declaring that something technically feasible is not practicable (and thus not really feasible under the law of armed conflict) because the State has a preferred way of conducting its operations. Though the law of armed conflict provides no ready answer to this dilemma, one of the key considerations is likely to be how much effort the State undertook to overcome the technical problems causing the operational impracticability. In addition, to the extent that the State chooses not to explore the feasibility of conducting cyber attacks from a segregated military cyber infrastructure, but instead conducts its military operations in a manner that intentionally intermingles those operations with civilian cyber infrastructure, problems would arise under the law of armed conflict.

V. CONCLUSION

As States organize for military operations in cyberspace, particularly the conducting of cyber attacks during the course of armed conflicts, they must remain fully cognizant of the burdens imposed by the law of armed conflict. Properly interpreted and applied, the law of armed conflict supplies the answers to many questions that will arise during the course of preparing to conduct cyberspace operations. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is an important contribution to the effort of addressing these questions. More importantly, the *Manual* provides a set of answers that is consistent in its viewpoint and approach, one that takes a cautious, yet prudent approach largely by analogy, in an area where very little State practice exists or is apparent.

As States conduct the legal reviews of cyber weapons required by the law of armed conflict, the example of U.S. practice is instructive. States should not follow the lead of the U.S. Air Force by requiring legal reviews of all cyber capabilities, but only those cyber capabilities whose intended effect or result is death, injury or destruction of property, the standard followed by the Army and the naval services.

64. *Id.*

When examining the precautions to be taken against the effects of cyber attacks, it is feasible to create—and easier to defend—dedicated military networks in an effort to establish separation, even if it is only virtual in nature, from a State's civilian cyber infrastructure. Likewise, cyberspace operations present unique challenges that, if not prepared for appropriately, will serve to further increase the risks to a country's innocent civilian cyber infrastructure if it executes cyber attacks from infrastructure that is intermingled with, and not segregated from, civilian cyber infrastructure. It is technically feasible to conduct cyber attacks in a manner that does not place civilian cyber infrastructure in increased jeopardy of attack. This area of the law of armed conflict is sure to come under additional scrutiny as States move closer to executing cyber attacks for which they accept responsibility during armed conflicts.