UIC John Marshall Journal of Information Technology & Privacy Law

Volume 27
Issue 3 *Journal of Computer & Information Law - Spring 2010*

Article 1

Spring 2010

Cyberwar Policy, 27 J. Marshall J. Computer & Info. L. 303 (2010)

Matthew Borton

Samuel Liles

Sydney Liles

ARTICLES

CYBERWAR POLICY

MATHEW BORTON*
SAMUEL LILES**
SYDNEY LILES†

Information operations have been a part of the broader spectrum of military operations since almost the beginning of time. The ability to affect the enemy's decision making can go a long way toward winning a battle. Necessarily, these operations embrace technology for mission accomplishment. In the last twenty years, this adherence to technology has developed a new terrain: cyberspace.

The emergence of "cyberspace" as a viable theater of operations has generated questions regarding the applicability of current doctrine to conflict in this new terrain. In Eugene Spafford's testimony to the House Armed Services Committee in 2005, he posited that threats to computer information systems "present a substantial danger to the US military, the civilian government, industry, academia, and the general public."[1] In 2009, before the Senate Committee on Commerce, Science, and Transportation, Dr. Spafford further stated that the country is "currently under unrelenting attack, and has been for years."[2] Spafford's testimony was not a new revelation. The call for increased cyber security from the

* Mathew Borton is a technologist at Purdue University Calumet. His research interests include information security policy and cyber warfare.

** Samuel Liles as an associate professor of computer information technology at Purdue University Calumet researching cyber warfare and cyber terrorism. His research agenda follows the spectrum of information operations and how cyber warfare realistically impacts the kinetic effects of conflict.

† Sydney Liles is a Ph.D. student in Computer Forensics at Purdue University, West Lafayette, Indiana. Her research interests include digital forensics and public policy

1. *Cyber Security, Information Assurance, and Information Superiority: Testimony Before the H. Comm. Of the Armed Services*, 109th Cong. 1 (2005) (statement of Eugene H Spafford, Professor of Computer Sciences).

2. *Cyber security: Assessing Our Vulnerabilities and Developing an Effective Defense: Testimony Before the S. Comm. on Commerce, Science and Transportation,* 111th Cong. 3 (2009) (statement of Eugene H. Spafford, Professor of Computer Sciences).

federal authorities can be traced back to at least the mid 1990s, and likely goes back much further.[3]

It appears that the government is listening, on some level. The National Strategy to Secure Cyberspace acknowledges that cyber security is a real issue and sets several goals for improvement.[4] The National Security Strategy states that one of the prime challenges that the United States and its allies has faced is cyber threats, and that both state and non-state actors could use cyberwar as a means of attack.[5]

Cyberwarfare is a very real threat to the security of the nation. Yet there is confusion and disagreement as to which government body is most appropriate to assume the cyberwar mission. The Strategy to Secure Cyberspace treats the threat primarily as a criminal issue, and assigns responsibility to the Department of Homeland Security.[6] The National Defense Strategy implies that cyberwarfare is a military issue.[7] Both documents may be correct, depending on the case. The cyberspace terrain transcends boundaries, quickly blurring the line between civil or criminal action and an act of war, leaving the government with the issue of assigning an agency to deal with the threat.

Who has the authority to wage cyberwar? What are the appropriate rules of engagement? In the United States, it appears that several agencies have some role in cyber-conflict. This paper will look at the various organizations within the federal government that have some cyber-component, and compare their abilities with applicable law to determine which agency or agencies have the ability to legally engage in cyberwarfare. This paper will also examine whether current methods for determining the rules of engagement for conflicts is relevant or if new procedures need to be drafted.

DEFINITIONS

Experts in the field disagree on the range and scope of cyberwarfare. Some even deny its existence, stating that cyberwarfare is merely an extension of the information operations ("IO") field or other military disci-

3. PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 5 (1997), *available at* http://www.fas.org/sgp/library/pccip.pdf.

4. OFFICE OF THE PRESIDENT, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 2-4 (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_stragety.pdf.

5. DEP'T OF DEFENSE, 2008 NATIONAL DEFENSE STRATEGY 1 (2008), *available at* http://www.defense.gov/news/2008%20National%20Defense%20Strategy.pdf.

6. OFFICE OF THE PRESIDENT, *supra* note 4, at 15-16.

7. DEP'T OF DEFENSE, *supra* note 5, at 22.

pline and that the threat has been overstated.[8] Certainly, this discussion is applicable to the subset of IO known as computer network operations ("CNO"), but it goes further.

CNO is any operation designed to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information infrastructure.[9] While this definition broadly describes a large portion of the spectrum of cyberwarfare capabilities, it does not consider the use of information technology assets to provide kinetic effect. Raymond C. Parks and David P. Duggan point out that cyber attack is meaningless unless it affects something in the real world.[10] Using these two sources can create a working definition. For the purposes of this discussion, cyberwarfare is considered to be any military operation designed to attack, deceive, degrade, disrupt, deny exploit and/or defend through the information infrastructure with a desired kinetic effect. In CNO, command and control are the targets. In cyberwar, they are the terrain.

It should be noted that this document is concerned with cyber*war* and not cyber*crime*. While "defense" against both things is possible, the distinction here is important. The Nineteenth Century Prussian philosopher Carl Von Clausewitz explained that war is "an act of force to compel our enemy to do our will"[11] and that the destruction of the enemy is the means by which this force is applied, through both defensive and offensive engagement.[12] The aim is not personal gain or hooliganism; it is a continuation of policy.[13]

"A crime is any act or omission (of an act) in violation of a public law forbidding or commanding it."[14] By extension, cybercrime is any crime committed in cyberspace. This issue tends to blur the important distinction that war is the exclusive purview of the military, while crime falls in the realm of civil authorities.

---

8. James Andrew Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, CENTER FOR STRATEGIC AND & INTERNATIONAL STUDIES (Dec. 2002), http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

9. U.S. DEP'T OF ARMY, FIELD MANUAL 3-13, INFORMATION OPERATIONS: DOCTRINE, TACTICS, TECHNIQUES, AND PROCEDURES (28 Nov. 2003).

10. Raymond C. Parks & David P. Duggan, Principles of Cyber-warfare, Paper presented at Workshop on Information Assurance and Security, United States Military Academy, West Point, NY (June 5-6, 2001), *available at* http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf.

11. CARL VON CLAUSEWITZ, ON WAR 75 (COL J.J. Graham, trans. 1873).

12. *Id.* at 90.

13. *Id.* at 87.

14. Cornell University Law School, *Criminal Law: an Overview,* LEGAL INFORMATION INSTITUTE, 2009, http://topics.law.cornell.edu/wex/Criminal_law (last visited Nov. 10, 2009).

Cyberspace as a terrain deserves clarification as well. Cyberspace is more than just the Internet. It includes all of the integrated command, control, and communication networks throughout the world.[15] Parks and Duggan point out that cyberspace differs from the physical in that the physical limitations of distance and space are meaningless, and that both the attacker and defender own very little of the actual battle space.[16] This means that attacks in cyberspace may be initiated from or traverse systems within United States' borders owned by private citizens, with or without the individuals' knowledge.

The definition of rules of engagement ("ROE") is fairly straightforward. Though there are several variations on the theme depending on context and cultural bias, the general idea usually means rules for the use of force in conflict. Because this work centers around the creation of ROE, however, a more succinct definition is needed. For this discussion, we will consider rules of engagement as defined by the *Operational Law Handbook*, which is used to train the United States military's lawyers. While an entire chapter of this text is devoted to ROE, it essentially states that they are a means to regulate armed force in the context of applicable policy and domestic and international law.[17]

Further, Baime et al. states that ROE serve three main purposes: to provide guidance to deployed units for the use of force; to provide controls for the transition from peacetime to acts of war; and to provide a framework to facilitate planning, based on national policy, mission requirements, and rule of law.[18] All of these purposes are important, however, this document will primarily focus on the concept of the use of force.

SCOPE

The preceding definitions go quite far to determine the scope of this document but finer points of detail need to be included to narrow the discussion. First, this work assumes a United States perspective and is concerned specifically with the United States federal government. Policies of other nations, as well as the individual states, may differ. This paper will focus on the appropriate agency to manage cyberwar, but will not seek to define command structure, scope of command beyond the idea of cyberwarfare, or operational doctrine. This paper discusses cyberwar and acts of war and is not directly concerned with crime. While non-state actors definitely have the capability to carry out cyberwarfare oper-

15. OFFICE OF THE PRESIDENT, *supra* note 4, at 8.

16. Parks & Duggan, *supra* note 10.

17. THE JUDGE ADVOCATE GENERAL'S SCHOOL, U.S. ARMY, OPERATIONAL LAW HANDBOOK 83 (MAJ John Rawcliffe ed., 2007), *available at* http://fas.org/irp/doddir/army/law2007.pdf.

18. *Id*.

ations,[19] and this work may be applicable to conflicts involving such groups, the primary focus is on state sponsored actors. Additionally, United States forces acting as part of a multinational force and under operational control of a foreign command will adapt ROE mandated by that command.[20] Therefore, this work assumes a force operating under direct authority of a national command. This paper considers government agencies with obvious potential cyberwar capabilities. While several civil authorities may be technically capable of a cyberwar mission, this work holds to the above statement that war is a military matter. Therefore, civilian agencies will not be considered in this document. Several agencies have the ability to be involved in cyber-related activities in specific cases as policy directs, but only those groups that have very broad freedom of action in this area have been considered.

This research deals only with the criteria for setting rules of engagement, not what those rules actually are. While much of the call to action has been to create new rules of engagement,[21] it is important to first determine the criteria for ROE in the new battle space. Defining actual ROE is a possible subject for a later date. Finally, there exists an entire body of knowledge that is classified, and therefore off limits to the author. Indeed, the standing rules of engagement, the basic framework for all other ROE, are classified material. The researcher has access to older, obsolete, and unclassified versions of much of this information. This means that this work may be redundant, obsolete, or irrelevant, unbeknownst to the researcher. The author is a technologist, not a legal expert. Although the legal guidelines concerning this issue appear fairly straightforward, the author may have missed a more intricate point of law.

CURRENT LITERATURE

The body of knowledge concerning cyberwarfare has grown substantially in the past ten years. While most of the work to date is concerned with computer network operations ("CNO"), a good portion of it still applies. Additionally, several documents that are relevant to the discussion have been written concerning the legal aspects of both information operations ("IO") and CNO. There are several government documents that set key policies to rules of engagement ("ROE") and cyberwarfare.

19. Frank Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars 7 (2007), *available at* https://dde.carlisle.army.mil/documents/sis/docs/Hybrid_Wars.pdf.

20. Joint Chiefs of Staff, Joint Pub. CJCSI 3121.01A, Standing Rules of Engagement for U.S. Forces (22 Jan. 2000), *available at* http://www.fas.org/man/dod-101/dod/docs/cjcs_sroe.pdf.

21. Duncan B. Hollis, *E-war rules of engagement*, Los Angeles Times, Oct. 8, 2007, *available at* http://articles.latimes.com/2007/oct/08/opinion/oe-hollis8.

Other documents specifically or indirectly discuss a controlling agency for cyberwar management.

The Threat

Some would dispute that cyberwar is a distinct entity. James A. Lewis is one of the authors leading this faction. In *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,* Lewis claims that cyberwar is merely an extension of conventional war, and the specific risks associated with cyberwarfare have been greatly exaggerated due to the relative youth of the technology.[22] However, Lewis may be too quick to dismiss the threats since he ignores the possibility of effects beyond the information systems themselves.

Michael Tanji disagrees with Lewis. In "Ideas for a More Secure Future," Tanji counts the possibility of cyberwar as among the pressing threats to our nation. He points out that "one man alone could not plunge the world into nuclear winter, yet it was not all that long ago that one man could have broken all the networks of the world."[23] He stresses the point that while cyberwar has been recognized as a threat, little has been done to counter or exploit cyberwar capabilities.[24]

Tanji is by no means the first to see the danger. In *Hybrid Wars,* Frank G. Hoffman discusses how post Cold War conflict involves a mix of state and non-state actors.[25] He points out how the enemy uses information warfare, and the fact that low-tech enemies are able to use the United States' information technology to win the information war.[26] Hoffman reinforces the impending threat of cyberwarfare, clearly refuting those who would claim that the threat has been exaggerated.[27]

The most potent evidence for the need for a cyberwar force comes from a foreign nation state that could easily become a formidable enemy. In *Unrestricted Warfare,* the authors, Chinese military officers, advocate the use of any weapon as long as it is the best weapon for the fight.[28] The authors in *Unrestricted Warfare* discuss using nonconventional weapons for combat and China's desire to use information warfare, among other less conventional tactics, in order to win at any cost.[29] This document is particularly important because China, an emerging power

22. Lewis, *supra* note 8.

23. Michael Tanji, *Ideas and Strategies for a More Secure Future*, *in* THREATS IN THE AGE OF OBAMA 114 (Michael Tanji ed., Nimble Books 2009).

24. *Id*. at114-15

25. Hoffman, *supra* note 19 at 15.

26. *Id.*

27. *Id.*

28. QIAO LIANG & WANG XIANGUI, UNRESTRICTED WARFARE: CHINA'S MASTERPLAN TO DESTROY AMERICA *passim* (2002).

29. *Id.*

in the world, has the potential to be either a powerful ally or a dangerous enemy. Therefore we must be willing to act in these same spaces, and develop a common understanding of proper conduct of conflict in these areas.

Evolution of the Concept

As mentioned above, the need has not gone completely unnoticed. John Arquila and David Ronfeldt provide an early discussion and definition of cyberwar that very much involves the information operations scope of CNO.[30] They also discuss "cyber-war" via "low tech means," the idea that cyber attacks can come from outside the terrain of cyberspace, and provide a good discussion of what the cyber terrain looks like.[31] While they give this overview, they ignore the higher-level policy implications, and, perhaps because of the early stages in which they entered the game, they miss the full potential impact of cyberwar.

Parks and Duggan build upon the work of Arquila and Ronfeldt and make the first and perhaps the most substantial attempt to date to define the phenomenon of cyberwarfare.[32] In *Principles of Cyber-warfare*, they developed eight traits of cyberwarfare that this article discusses in the section below regarding ROE criteria.[33] They do an excellent job of defining the nature of the terrain and hint at policy implications, though this is really outside the scope of their research.[34]

Calls for Policy

Other researchers have been more directly concerned with policy. Davis Brown provides a discussion of international law governing information systems as weapons.[35] He defines the weaponisation of these systems.[36] He also looks at matters relating to infrastructure, and effects on civilians, but stops short of recommending changes or additions to current law or policy.[37]

Duncan B. Hollis takes the idea a step further and calls for international regulations of information warfare.[38] Hollis does not make a dis-

30. John Arquilla & David Ronfeldt CYBERWAR IS COMING!, *in* ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 460 (1997).

31. *Id.*

32. Parks & Duggan, *supra* note 10.

33. *Id.*

34. *Id.*

35. Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47(1) HARV. INT'L L.J. 42 (Winter 2006), *available at* http://www.harvardilj.org/print/73.

36. *Id.*

37. *Id.*

38. Hollis, *supra* note 21.

tinction between information warfare and cyberwar, and he discusses concepts that fit the definition of cyberwar discussed above.[39] He examines cyberwarfare attacks based on the current rules to determine war crimes, and points out where current international regulations fall short.[40] He also points out that if the attack falls outside of the jurisdiction of the laws of war, individual nations' criminal laws apply.[41] Hollis implies that international law will inform United States policy.[42] It is certain to have some influence, but if United States policy makers wait for direction from the international community, our country will certainly suffer at the hands of those with more initiative.

Michael N. Schmitt takes a slightly different direction. He also looks to the international community, but instead, parallels cyber attack and the existing standards for use of force.[43] He discusses the concept of attack and response based on the relevant United Nations Articles.[44] He examines Article 2(4), which governs use of force, and Article 41, which talks about disrupting communications.[45] He then recommends that the international community issue a judgment based on these Articles, in order to more easily identify the legalities of cyber attack.[46] Schmitt misses some of the nuances of cyber terrain and also puts the onus on the international community. He leaves us, however, with perhaps the best jumping off point to talk about rules of engagement.

Current Policy

The Government is starting to pay attention to calls of researchers, and the beginnings of policy are appearing in government publications. The *National Strategy to Secure Cyberspace* sets priorities and goals for the defense of cyberspace.[47] The document is written from a cybercrime perspective.[48] It places the responsibility of security on both corporations and private citizens and the coordination of the defense effort squarely in the Department of Homeland Security's hands.[49] It gives a good overview of bodies responsible for dealing with various levels of threats, but it does not clearly state rules of engagement and steers clear of interpret-

39. *Id*.
40. *Id*.
41. *Id*.
42. *Id*.
43. Micahel N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 886 (1999).
44. *Id*.
45. *Id*.
46. *Id*.
47. OFFICE OF THE PRESIDENT, *supra* note 4, at 15-16.
48. *Id.*
49. *Id*.

ing law.[50] This document lacks any real acknowledgement of a military threat, and while it discusses critical infrastructure, it addresses the issue as a business continuity problem rather than a strategic vulnerability.[51]

The *National Defense Strategy* also acknowledges cyberwar as a threat to national security, and even discusses the fact that other potentially hostile nations as well as non-state actors are nurturing capabilities on this front.[52] While the document recognizes cyberwar as a military issue, it gives only very nonspecific direction as to how to handle the issue.[53]

Joint Publication 3-13 also provides some direction to our nation's military regarding cyberconflict.[54] It defines information operations, computer network operations as a subset of IO and the military's ideal role for CNO. However, it only discusses cyberwarfare in these terms and pays little attention to the possibility of kinetic effect.[55]

Rules of Engagement

Standing rules of engagement ("SROE") are designed in accordance with United States national security policy. The goal of this policy is to preserve the safety and survival of the nation and promote an international environment favorable to United States interests.[56] The United States SROE provide three main points: they implement the right of self defense to all military units, govern use of force consistent with mission accomplishment, and provide guidance for force in operations other than war, escalation of hostilities, or the absence of superseding guidance.[57] Note that the SROE are applicable only to units deployed outside United States boundaries.[58]

First, consider SROE dealing with the premise of self-defense. United States forces have the explicit right to self defense by any means necessary.[59] This right of defense extends from the nation and its citi-

50. *Id.*

51. *Id.*

52. OFFICE OF THE PRESIDENT, *supra* note 4, at 15-16.

53. DEP'T OF DEFENSE, *supra* note 5, at 22.

54. *See generally* JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS (13 Feb. 2006), *available at* http://www.fas.org/irp/doddir/dod/jp3_13.pdf.

55. *Id.*

56. JOINT CHIEFS OF STAFF, JOINT PUB. CJCSI 3121.01A, STANDING RULES OF ENGAGEMENT FOR US FORCES (22 Jan. 2000), *available at* http://www.fas.org/man/dod-101/dod/docs/cjcs_sroe.pdf.

57. *Id.*

58. *Id.*

59. JOINT CHIEFS OF STAFF, JOINT PUB. CJCSI 3121.01A, STANDING RULES OF ENGAGEMENT FOR US FORCES (22 Jan. 2000), *available at* http://www.fas.org/man/dod-101/dod/docs/cjcs_sroe.pdf.

zens to the unit and the individual. It also extends to collective defense in concert with forces of other nations and property of United States citizens in some cases.[60] The next provision, guidance for use of force in operations other than war, tends to be the most commonly thought of provision when discussing SROE. When considered together with the third provision, guidance for use of force in the absence of superseding guidance, the SROE form the basic legal framework for use of force by troops deployed outside U.S. borders.[61]

The idea of a legal framework has been mentioned above but not described. According to the Department of Defense Law of War Program, all United States force's actions must comply with the Law of War in all armed conflict and combat operations.[62] The Law of War is further defined as that part of "[i]nternational law that regulates the conduct of armed hostilities."[63] It includes treaties and international agreements to which the United States is a party, as well as customary international law.[64]

Therefore, Law of War is international in nature. It can be an extremely complex topic – it is rooted in medieval European theology and spans several large multinational treaties, including the Geneva and Hague Conventions.[65] However, this seemingly complex system of tradition, law, and convention can be broken down into four key concepts: proportionality,[66] necessity, discrimination, and humanity.[67]

Proportionality is the idea that the damage and loss of life caused by an attack must not be excessive in relation to the expected gain in military advantage.[68] Proportionality is considered with a view toward the entirety of the military strategy rather than the individual tactical action. While proportionality considers collateral damage, it is not the primary concern.[69]

The second concept is necessity. Necessity is the idea that destruction or seizure of property is allowable only as military need dictates.[70] While a bit more difficult to understand and describe, this concept essen-

60. *Id*.

61. THE JUDGE ADVOCATE GENERAL'S SCHOOL, U.S. ARMY, *supra* note 17, at 84.

62. JOINT CHIEFS OF STAFF, JOINT PUB. CJCSI 5810.01B, IMPLEMENTATION OF THE DOD LAW OF WAR PROGRAM (25 Mar. 2002), *available at* http://www.pegc.us/archive/DoD/docs/CJCSI_5810_01B.pdf.

63. *Id.*

64. *Id.*

65. Thomas W. Pittman & Linda Strite Murnane, *The Law of Armed Conflict in Modern Warfare*, 42 JUDGES' J, 18 (Spring 2003).

66. THE JUDGE ADVOCATE GENERAL'S SCHOOL, U.S. ARMY, *supra* note 17, at 4.

67. *Id*. at 14.

68. *Id.*

69. *Id*.

70. *Id*. at 153.

tially prohibits random destruction or seizure of civilian property, unless it is part of a military objective. Civilian objects are protected from attack unless they are being used for military purposes or there is a clear military need. Note that while the Law of War prohibits intentional targeting of civilians and other protected persons, it is understood that legitimate targeting of a civilian object may at times cause unintended casualties.[71]

Related to this is the principle of distinction. Distinction says that "combatants must be distinguished from non-combatants, and that military objectives be distinguished from protected property or places."[72] Operations must be directed only against combatants and military objectives.[73] Attacks that are "not directed at a specific military objective," unleash effects that cannot be controlled, or cause excessive collateral damage are considered indiscriminate and are prohibited.[74]

The final concept, humanity or "unnecessary suffering," is directed at means used to inflict harm in combat. It is generally accepted that combat involves physical harm and loss of life. The concept of humanity is concerned with using a weapon to cause disproportionate injury or suffering caused as compared to its military effectiveness.[75]

These four ideas form the basis of the Law of War and must also form the basis for ROE developed for American forces. ROE must ensure that combatants bear only the force necessary to achieve the military objective, engage only necessary targets, discriminate between combatants and noncombatants, and that in doing so they do not cause undue suffering.

Cyberwarfare

With the criteria for ROE identified, this discussion will turn to the idea of cyberwarfare. Cyberwarfare has rarely been defined clearly, though it is generally considered to be a subset of information operations.[76] Parks and Duggan provide us with the best example to date. They identified eight principles of cyberwarfare that have been distilled by Cahill, Rozinov, and Mule into the following categories: kinetics, visibility, mutability, masquerade, dual-use weaponry, partition/usurpation, unreliability, and intimacy.[77] It is important to understand these principles because they make cyberwarfare a unique form of operations.

71. THE JUDGE ADVOCATE GENERAL'S SCHOOL, U.S. ARMY, *supra* note 17, at 13.
72. *Id*.
73. *Id*.
74. *Id*.
75. *Id.* at 14.
76. Parks & Duggan, *supra* note 10.
77. Thomas Cahill et al, *Cyber Warfare Peacekeeping*, IEEE Workshop on Information Assurance, United States Military Academy, 101, West Point, NY.

The first principle is kinetics. Attacks from cyberwarfare, and indeed warfare in general must have kinetic effect. Parks and Duggan point out that one can constantly attack something in the cyber world, and it is meaningless without kinetic effect.[78] In their view, kinetic effect includes both physical change to the environment and change in the enemies' decision making.[79]

The next principle is that of visibility. In order to act in the cyber realm, an attacker must manipulate data in some way, which in essence is making one's presence known. However, in order to be seen, as Parks and Duggan point out, someone has to be looking.[80] This means that unless the defender happens to be looking at the right pieces of data, the attacker is essentially able to hide in plain sight.

The idea of mutability is a bit more complex. The physical world follows certain, very nearly constant laws, and one can reasonably expect that the same action repeated in the same situation will yield similar results, but this is not necessarily true in the cyber realm. Since the terrain in which cyberwarfare is conducted is a man-made construct, there are several imperfections that cause inconsistencies and instabilities. The same action repeated twice may yield very different results.[81] This instability may be actively exploited.

The concept of masquerade deals with identities and authorization. This principle maintains that for any action one desires to carry out in cyber-terrain, there is an identity with the appropriate rights to carry out the desired effect. This makes the acquisition and impersonation of the appropriate identity a goal for a large portion of cyber attacks.[82]

Further, the nature of the cyber terrain is such that the weapons employed are dual-use. Parks and Duggan explain the dual-use concept with the analogy that one does not test one's defenses in the physical world by shooting one's own troops.[83] In the physical world, one uses weapons to attack, and armor to defend. The tools have single roles. In cyberwarfare, however, tools can be employed in both offensive and defensive modes.[84] For example, a port scanner could be used defensively to check for vulnerabilities in a system, or offensively to check for open attack vectors.

Partition and usurpation are two closely related concepts. Partition refers to the idea that an entity actually controls only a small portion of cyberspace, although it may act over a much larger portion of it. Gener-

78. Parks & Duggan, *supra* note 10.
79. *Id*.
80. *Id*.
81. *Id*.
82. *Id.*
83. *Id*.
84. Parks & Duggan, *supra* note 10.

ally speaking, an entity will only control the software and hardware with which it interfaces directly, and sometimes even less.[85] Usurpation is the idea of controlling specific space within the cyber domain. If one can gain control of an area that one's enemy uses, even if the enemy does not own that space, the controller gains the military advantage.[86]

Related to the idea of mutability is instability. Like mutability, the principle of instability is derived from the fact that the cyber-terrain is man-made, and therefore imperfect. Where mutability pertains to actively manipulating the environment, instability involves the passive shifting of cyberspace due to man-made imperfections. This leads to uncertainty in the tactics employed in cyber-combat.[87]

The final trait that Parks and Duggan identified is intimacy.[88] Physical distance means nothing in cyberspace.[89] Participants in combat can literally be on opposite sides of the planet and engage the enemy with as much force as troops on the ground.[90]

The Right Force

The next big question is which department is best suited to act on behalf of the United States in the cyber realm. Requirements for a cyberwarfare force can be derived from the regulations and force policy discussed in the literature review, and the definition of cyberwar proposed above. Again, because cyberwarfare would be a military action, the agency will need to fall under the authority of the Department of Defense, or be specially directed to do so by the President. As mentioned above, it may be possible for attacks to originate within the United States. Therefore, is necessary for the assigned agency to be able to act both on foreign soil and domestically.

In "Defining Information Operations Forces," Franz, Durkin, Williams, Raines, and Mills review the specific needs of information operations ("IO") forces inside the military, and the Air Force in particular.[91] Their paper is specifically concerned with computer network operations ("CNO"), rather than cyberwarfare. However, the authors put forth some relevant criticisms. They state that "neither dedicated forces nor a mature training strategy exists for the [Network Warfare] mission area," and that "[l]ack of dedicated forces affects the potency and maturity of

85. *Id*.
86. *Id*.
87. *Id*.
88. Parks & Duggan, *supra* note 10.
89. *Id.*
90. *Id*.
91. Timothy P. Franz et al., *Defining Information Operations Forces*, 21 AIR AND SPACE POWER J. 53 (Summer 2007).

these forces."[92] This argument demonstrates the haphazard way in which the CNO field and cyberwar have been treated in defense circles.

Others agree. Gregory Conti and John Surdu echo the call for a dedicated, specially trained force.[93] In *Army, Navy, Air Force and Cyber – Is It Time For a Cyberwarfare Branch of the Military?*, they advance the idea that another branch of the military is needed to handle cyberwarfare.[94] They reason that the rise of cyberwar capability is analogous to the rise of air power in the early to mid part of the last century.[95] Just as air power warranted its own military command because it dealt with new terrain, so should cyber power.[96] While their idea has merit, the authors' motivation is questionable. Their grounds for suggesting a new force are based on purely social and stereotypical reasons. They suggest that traditional military structures are not compatible with the lifestyle and skills of those involved in cyberwar.[97] Their statements hint at hard feelings about internal politics rather than a genuine interest in furthering the nation's cyberwar capability.[98]

Surdu and Conti contribute to the discussion by proposing the National Security Agency (NSA) as a cyberwar force. They support the idea that the NSA is technically capable of carrying out cyberwar activities within its mission. They dismiss, however, the NSA's role in cyberwar on the basis that actual military personnel only serve limited tours of duty in connection with the NSA, which are not based on any real or substantial grounds.[99]

The United States Code defines much of the structure of the nation's military capabilities. Title 10 defines the structure and powers of the Department of Defense ("DOD").[100] Pursuant to Title 10, Department of Defense Directive 5100.1 details the duties to the DOD.[101] They are to:

> "[s]upport and defend the Constitution of the United States against all enemies, foreign and domestic. Ensure, by timely and effective military action, the security of the United States, its possessions, and areas of vital interest. Uphold and advance the national policies and interests

92. *Id.* at 4.

93. LTC Gregory Conti & COL John "Buck" Surdu, *Army, Navy, Air force, Cyber - Is it Time for a Cyberwarfare Branch of Military?*, 12(1) IA NEWSLETTER 14 (Spring 2009), *available at* http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf.

94. *Id*.

95. *Id*.

96. *Id.*

97. *Id*.

98. For example, "[e]choes of this ethos are also found in disadvantaged assignments, promotions, school selection, and career progression for those who pursue cyberwarfare expertise, positions, and accomplishments." Conti & Surdu, *supra* note 93.

99. Conti & Surdo, *supra* note 93, at 14.

100. 10 U.S.C. § 121-130 (2006).

101. *Id.*

of the United States."[102]

This directive explicitly gives the DOD and its subordinate agencies the power to wage war against the enemies of the United States.[103] There are other regulations that come into play. The most well-known is, perhaps, the Posse Comitatus Act.[104] The Act expressly forbids using the Army and Air Force for domestic law enforcement purposes.[105] The Navy and Marine Corps were also ordered to adhere to this policy under DOD Regulation.[106] Department of Defense Directive 3025.15 further directs this matter.[107] It covers detailed instances that require military support for civilian activities, and includes provisions for emergencies, civil unrest, and acts of terrorism.[108] The directive generally adheres to the Posse Comitatus Act. The importance of this Act is linked to the discussion of the nature of cyberspace above. Because private citizens and assets are involved, with or without their knowledge, any agency must be able to act within the borders of the United States and against those citizens and assets.

Combined with the United States Code, published doctrine clearly defines each of the military branches' specific missions. These documents help shape the way the individual branches interact with the cyberterrain. The United States Army's mission is laid out in Field Manual One. The United States Army's mission is to preserve peace and security, provide for defense, and overcome aggressive acts of enemies.[109] The Army views cyberwar mainly as a subset of information operations, in the form of computer operations, which, as described above, are any operations designed to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information infrastructure.[110]

The Navy has a duty to "promote and defend our national interests by maintaining maritime superiority, contributing to regional stability, conducting operations on and from the sea, seizing or defending ad-

102. DEP'T OF DEFENSE, DIR. 5100.1, FUNCTIONS OF THE DEPARTMENT OF DEFENSE AND ITS MAJOR COMPONENTS 3 (1 Aug. 2002), *available at* http://www.dtic.mil/whs/directives/corres/pdf/510001p.pdf.

103. *Id.*

104. 18 U.S.C. § 1385 (2010).

105. *Id.*

106. DEP'T OF DEFENSE, DIR. 5100.1, FUNCTIONS OF THE DEPARTMENT OF DEFENSE AND ITS MAJOR COMPONENTS (1 Aug. 2002), *available at* http://www.dtic.mil/whs/directives/corres/pdf/510001p.pdf; ERIC V. LARSON & JOHN E. PETERS, OVERVIEW OF THE POSSE COMITATUS ACT: PREPARING THE U.S. ARMY FOR HOMELAND SECURITY: CONCEPTS, ISSUES, AND OPTIONS 244 (2001).

107. DEP'T OF DEFENSE, DIR. 3025.15, MILITARY ASSISTANCE TO CIVIL AUTHORITIES (18 Feb. 1997), *available at* http://www.dtic.mil/whs/directives/corres/pdf/302515p.pdf.

108. *Id.*

109. U.S. DEP'T OF ARMY, FIELD MANUAL 1 (June 2005).

110. U.S. DEP'T OF ARMY, FIELD MANUAL 3-13, INFORMATION OPERATIONS: DOCTRINE, TACTICS, TECHNIQUES, AND PROCEDURES (28 Nov. 2003).

vanced naval bases, and conducting such land operations as may be essential to the prosecution of naval campaigns."[111] The Navy is heavily invested in "network centric warfare." Their main connection to the domain of cyberwar is in their command, control, communications, computers and intelligence initiatives ("C4I"), and the defense of these systems.[112]

Of the various services, the Air Force alone has taken direct initiative toward a cyberwar command. Their mission is similar to Title 10 for the Army with the addition that it should "be organized for . . . prompt and sustained offensive and defensive air operations."[113] The service's main doctrinal publication adds "space" to its capabilities,[114] and their official web site adds that, "[t]he mission of the United States Air Force is to fly, fight and win. . .in air, space, and cyberspace."[115] In September of 2007, the Air Force provisioned cyber-command, whose mission was to operate on the behalf of the Air Force in cyberspace.[116]

The Marine Corps is defined in Title 10 as a command within the Department of the Navy.[117] Chapter 507 of Title 10 designates the Marine Corps with duties of seizure and defense of advanced naval bases, land actions in the prosecution of naval campaigns, detachments for service aboard naval vessels and security of naval property.[118] They also have an obligation as a force in readiness, which falls under a provision in Title 10 written as "other duties as the President may direct."[119] The Marine Corps participates in the Navy's C4I initiatives, as well as maintaining IO components similar to the Army's.[120] The National Guard, though generally serving the same roles as the regular Army and Air Force, has a special significance as the United States' standing militia.[121] U.S. Code Title 32 describes the special nature of the Guard.[122] In particular, Title 32 provides that the individual states may use the

111. DEP'T OF THE NAVY, NAVAL WARFARE 21 (28 Mar. 1994), *available at* http://www.dtic.mil/doctrine/jel/service_pubs/ndp1.pdf.

112. *Id.* at 61.

113. 10 U.S.C. § 8062 (2006).

114. DEP'T OF THE AIR FORCE, AIR FORCE BASIC DOCTRINE 1 (17 Nov. 2003), *available at* http://www.dtic.mil/doctrine/jel/service_pubs/afdd1.pdf.

115. U.S. Air Force, *8th Air Force*, http://www.8af.af.mil/main/welcome.asp (last visited Apr. 10, 2009).

116. Erik Schechter, *Cyber Catch-up*, C4ISR J. (Mar. 6, 2008), http://integrator.hanscom.af.mil/2008/March/03132008/03132008-17.htm (last visited Apr. 10, 2009).

117. 10 U.S.C § 5063 (2006).

118. *Id*.

119. *Id*.

120. DEP'T OF THE NAVY, NAVAL WARFARE 63 (28 Mar. 1994), *available at* http://www.dtic.mil/doctrine/jel/service_pubs/ndp1.pdf; *See also* Marine Corps Order 3120.10 section 3 part b.

121. 32 U.S.C. § 101 (2006).

122. *Id*.

Guard as necessary during peace time.[123] This puts the Guard in an interesting position, as it can be mobilized both as a Federal force and in support of the individual states.

DISCUSSION

Now that the criteria for ROE in traditional combat have been defined, and the principles of cyberwarfare have been identified, the criteria will be applied to each principle in order to demonstrate the applicability or non-applicability of the criteria to each principle. Examples are offered when necessary to provide greater demonstration of the relationships.

Kinetics is the first principle. In general, the criteria will apply as normal to this principle, since kinetics applies to the end result of the physical manifestation of the cyber attack. In order to maintain proportionality, the kinetic effect must not be greater than necessary in order to achieve military effect. With concern to necessity, one may consider whether it is necessary to use computer systems to attack, disrupt, or destroy civilian property to achieve a specific military goal. An example of this would be determining the necessity of overriding a programmable logic circuit to shut down a power grid that may supply both enemy combatants and civilians. Related is the idea of distinction. Again, where the kinetic effect is concerned, actors need to ensure that the target is military in nature and that the kinetic effect achieved is controllable enough to ensure that civilians are not indiscriminately targeted. For example, if an individual were to take control of a nuclear power plant and cause a reactor meltdown, this may violate the criteria of discrimination (and possibly others too) because it is releasing forces that are uncontrollable. Finally, the criteria of humanity is hard to apply in this case, since most examples of kinetic effects that cause undue suffering that come to mind are less technological in nature.[124] However, it is conceivably possible to have a cyber attack that releases kinetic effects that would violate this criterion.

The idea is less straightforward where the principle of visibility is concerned. It would appear that the criteria do not necessarily apply, since this principle is centered on a subterfuge as a means to an end. The concept of visibility then becomes a subordinate or supporting principle of cyberwarfare rather than an active characteristic.

The concept of mutability gets a bit more interesting. In taking advantage of this principle, imperfections in hardware or software are being actively exploited for desired effect. In considering proportionality it must be certain that the secondary and tertiary effects of manipulating the cyberscape do not go beyond what is acceptable for collateral dam-

123. 32 U.S.C. § 109 (2006).

124. THE JUDGE ADVOCATE GENERAL'S SCHOOL, *supra* note 17, at 14.

ages. Malformed code released into the wild may disrupt enemy communication, but what if it spreads to relief agencies providing aid to civilians? Distinction is important here as well, and it may be extremely difficult to achieve as it is important to make sure that in manipulating the data, routing tables for instance, that services to the civilian population are not unduly damaged. Again, the concept of humanity is hard to apply here. Necessity is difficult as well, unless paired with other concepts, as discussed later on.

Masquerade, which amounts to identity theft in civilian circles, primarily needs to stand up to the tests of distinction and necessity. Distinction applies in that the actor needs to ensure that the role being assumed allows access only to appropriate military targets. Acquiring access rights for a hospital's main computing systems and shutting down those computing systems generally would be a violation of this criterion. Necessity is important to ensure that the systems for which rights are acquired are necessary to achieve a military objective. Operators in violation of this idea may find themselves liable to criminal prosecution under statutes involving unauthorized access to computer systems.[125] Proportionality is again largely a concern only when considering second and third level effects, and then only when combining masquerade with one of the other principles. Humanity does not really apply because there is not a conceivable case where assuming a role or identity to carry out a cyber attack would be considered to cause undue suffering on its own.

It is difficult to apply the criteria when considering the dual use nature of tools, like the concept of visibility. However, in this case the difficulty is because the discussion is about the tools and not methods. In the physical world, the analogy would be to weapons systems, and there the tests for the concept of humanity would need to be applied. It is not easy to conceive of an existing tool that exists entirely in cyberspace that would be considered inhumane on its own.

The potential arises for the situation to become a bit sticky, especially in the realm of distinction, when applying the criteria to the principle of partition/usurpation. Military systems can reside on the same physical devices as civilian systems. The systems can also possibly reside in a third nation neutral to the conflict. Therefore, it is extremely important to ensure that the attackers are aware as much as possible of the physical location of the target and that they isolate the attack as much as possible to avoid unnecessary collateral damage. The criteria of necessity also comes into play here because otherwise protected systems may be the subject of an attack due to the desire to control a certain aspect of the cyber-terrain. Proportionality may also become an issue

125. 18 USC 1030 (2010).

because taking control of and denying access to portions of cyberspace may cause undue harm to the civilian population and potentially even other states that are not involved in the conflict.[126] In the case of partition/usurpation, humanity is not likely to have any bearing on this principle.

Instability, while related to mutability, has a different relationship to the criteria, due to its passive nature. The main concern in this case is proportionality. Because of the instability of cyberspace, it is entirely plausible that the kinetic effect of a cyber attack may generate orders that result in a greater magnitude than originally intended. Distinction is also a concern, due to the fact that an attack may inadvertently harm protected property as a result of an unperceived change in cyberspace. Necessity does not play a large part in this case, mainly because instability is a passive force that affects attacks and is uncontrolled by the attacker. Humanitarianism is also not applicable here for the same reason.

The final property, intimacy, focuses mainly on geographic dispersion. The concerns with the criteria align very closely with those mentioned for usurpation, in that they are concerned with the physical locations of cyberspace constructs. The actors need to be aware of physical locations to avoid violating the tenets of proportionality, necessity and distinction.

The relationships between the criteria and the principles can be laid out in a matrix in terms of applicability, as shown in Figure 1. The matrix provides enough information to determine whether or not the criteria for ROE as they stand are appropriate to develop ROE for cyberwarfare.

	Necessity	Distinction	Proportionality	Humanity
Kinetics	Yes	Yes	Yes	Yes
Visibility	No	No	No	No
Mutability	No	Yes	Yes	No
Masquerade	Yes	Yes	No	No
Dual-use	No	No	No	Maybe
Partition/ usurpation	Yes	Yes	Yes	No
Instability	No	Yes	Yes	No
Intimacy	Yes	Yes	Yes	No

FIGURE 1. Matrix demonstrating applicability of criteria to principles of cyberwarfare

The matrix demonstrates that when cyberwarfare is treated as a whole, the criteria used to develop ROE for operations in the physical

126. It is also worth noting that methods used to gain or seize control may be in violation of the International Telecommunications Treaty. *See,* Constitution of the International Telecommunication Union Ch. VI (1994), *available at* http://www.jus.uio.no/english/services/library/treaties/07/7-06/const-international-telecommunication-union.xml.

space are appropriate to operations in cyberspace. It further shows that distinction is the most important criteria for cyberwarfare, and that leaders should pay special attention to this area when developing ROE. This is most likely due to the nature of the terrain itself. A state may only physically own ten percent or less of the battle space; military systems may be collocated with civilian systems. The battle space may traverse the physical boundaries of neutral states. Target systems may be located inside the boundaries of those neutral states, and neutral states may even own those target systems. Thus, it is of the utmost importance that planners take distinction into consideration in order to avoid war crimes charges, rightful retaliation, or unintended escalation of hostilities with third party states.

The idea of proportionality is almost as important. It may appear at first that this criterion would be marginal in applicability. However, when second and third order effects are considered, proportionality becomes a major factor, because the amount of force can multiply by several orders of magnitude and cause large amounts of unintended collateral damage.

Military necessity is also very applicable. While at face value there are no additional considerations when applying military necessity to cyberwarfare, additional scrutiny in this area is warranted when commanders are developing ROE. Essential to this idea is the principle of intimacy. Because of the ambiguous nature of locality in cyberspace, commanders must strongly consider the necessity of the target when they are planning operations focused on disrupting or destroying the enemy's information technology assets. If not, leaders may find themselves vulnerable to the same issues that arise in the consideration of distinction.

It would appear that the criterion of humanity has little value in this discussion. However, it is still a valid criterion and should be applied in developing ROE because the kinetic effects of an action may intentionally or intentionally cause unnecessary suffering, both to military units and civilian populations. This will become increasingly important as cyberwarfare operations become more sophisticated, and as populations rely more and more on information technology for the good order and functioning of society.

Based on the above findings, this researcher recommends that commanders should follow the standard criteria based on Law of War and pay special attention to the considerations noted above when developing ROE for operations in cyberspace. It should be noted that the primary concerns deal with the ambiguity of national boundaries in cyberspace and the possibility of operations' unintended effects. Because of the ambiguity, States' rights in cyberspace need to be more clearly defined, especially in light of the increased States' desire to exploit cyberspace in

conflict.[127] Additionally, though it is not reasonable to expect that the tactical employment of a weapons system in any terrain be capable of completely avoiding collateral damage, researchers in this area must develop tools and techniques that will minimize harm to protected property and noncombatants.

Finally, it should be stressed that this body of work deals with ROE for conflict with States. Non-state actors were not taken into consideration due to the fact that Law of War does not apply in most cases related to non-state actors.[128] In those cases, leaders will need to balance consideration for operations in cyberspace with ROE for counterinsurgency, which is beyond the scope of this work.

Cyberwar Command

Because of the current wording of United States Code, only the National Guard has the legal ability to serve as a cyberwar force and act both domestically and internationally.[129] The provisions in Title 32 regarding the States' ability to use the National Guard permit the National Guard troops to act within the borders of the United States.[130] The various branches of service are limited as to how the Posse Comitatus can use them. However, it should be noted that the Navy and Marine Corps are only bound to the Act by Department of Defense regulation, which could be lifted internally.[131] Accordingly, this researcher recommends that if a cyberwar command is to be created, it should be placed under control of the National Guard. This special provision for the National Guard extends both to the Army National Guard and the Air National Guard. It may be possible to transition the Air Force's cyberwar command to the Air National Guard in order to bring it into compliance with the stipulations above. This would be ideal because it would allow the United States to bring a functional, trained force on-line quickly.

It might also be possible to form another command under the Department of Defense in order fill this role. The issue is that it would ostensibly require a change in United States Code. This would be a long process involving legislative acts. Arguably, the President could issue an executive order to change roles of the agencies, which would make this entire discussion irrelevant. In view of the evidence presented above, this would seem heavy-handed and unnecessary. Finally, a change in DOD policy could free the Navy and the Marines to act domestically. Again, this feels unnecessary in light of the above information. This

127. Office of the President, *supra* note 4.
128. U.S. Dep't of Army, Field Manual 3-24, Counterinsurgency (15 Dec. 2006).
129. 32 U.S.C. §109 (2006).
130. *Id*.
131. 18 U.S.C. §1385 (2009).

leaves the National Guard as the only currently viable force, with Air National Guard in the best position to take on a cyberwarfare mission.

FUTURE WORK

This work only covers a small piece of a larger issue. While cyber security and cyberwar have been acknowledged as critical issues for the continued security of the State, the United States still has a long way to go. The definition of cyberwar is still unclear, as are the rules of engagement for cyberwar and the legal implications at all levels. Due to this uncertainty, strategic and tactical response remains undefined, leaving the nation all but defenseless.

This research verifies the applicability of criteria based on Law of War for the development of ROE for cyberwarfare. It really is the proverbial tip of the iceberg, however. This document is an obvious base for the development of standard rules of engagement for operations in cyberspace. Further, this work may serve as the beginning stages for a framework to guide a more specific military policy for operations in cyberterrain.