Civilians in Cyberwarfare: Conscripts

Susan W. Brenner[*] with *Leo L. Clarke*[**]

ABSTRACT

Civilian-owned and -operated entities will almost certainly be a target in cyberwarfare because cyberattackers are likely to be more focused on undermining the viability of the targeted state than on invading its territory. Cyberattackers will probably target military computer systems, at least to some extent, but in a departure from traditional warfare, they will also target companies that operate aspects of the victim nation's infrastructure. Cyberwarfare, in other words, will penetrate the territorial borders of the attacked state and target high-value civilian businesses. Nation-states will therefore need to integrate the civilian employees of these (and perhaps other) companies into their cyberwarfare response structures if a state is to be able to respond effectively to cyberattacks. While many companies may voluntarily elect to participate in such an effort, others may decline to do so, which creates a need, in effect, to conscript companies for this purpose. This Article explores how the U.S. government can go about compelling civilian cooperation in cyberwarfare without violating constitutional guarantees and limitations on the power of the Legislature and the Executive.

---

* NCR Distinguished Professor of Law and Technology, University of Dayton School of Law.

** Associate, Drew, Cooper & Anding, P.C., Grand Rapids, Michigan.

TABLE OF CONTENTS

I. INTRODUCTION

> *Critical infrastructure owners . . . report that their networks and control systems are under repeated cyberattack . . . from . . . foreign nation-states.*[1]

According to one estimate, 140 nations have developed or are in the process of developing the capacity to wage cyberwarfare.[2] Other

---

1. STEWART BAKER ET AL., MCAFEE, INC., IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 3 (2009), http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf. *See also Attacks on Military Computers Cited*, N.Y. TIMES, Apr. 16, 2010, at A14. ("Computer networks essential to the Pentagon and military are attacked by individual hackers, criminal groups and nations hundreds of thousands of times every day."). "Nearly a third of the IT executives surveyed said their own sector was either 'not at all prepared' or 'not very prepared' to deal with attacks." *Id.* at 16. "[O]nly 37 percent of [those participating in the cyber war survey] were confident their government could continue to deliver services in the face of a major cyberattack." *Id.* at 17.

2. *See* Kevin Coleman, *The Cyber Arms Race Has Begun*, CSO ONLINE (Jan. 28, 2008), http://www.csoonline.com/article/print/216991 ("In a report developed by Spy-Ops in the fall of 2007, they estimated that about 140 countries have active cyber weapons development programs in place and operational."); *see also* Aidan Lawes, *Cyber Crime: A 24/7 Global Battle,* ITP REPORT (Nov. 29, 2007), http://www.itpreport.com/default.asp?Mode=Show&A=1421&R=GL (120 nations have or are developing cyberwarfare capabilities). Cyberwarfare is also known as

countries will follow suit. A 2009 global survey of executives working for critical infrastructure and computer security companies found that "45 percent believed their governments were either 'not very' or 'not at all' capable of preventing and deterring cyberattacks."[3]

Although cyberwarfare will probably not displace traditional, kinetic warfare,[4] it will become an increasingly important weapon in the arsenals of nation-states for several reasons. First, developing the capacity to wage cyberwar costs little compared to the cost of developing and maintaining the capacity to wage twenty-first century kinetic war.[5] The expense of cyberwarfare primarily encompasses training and paying cyberwarriors, and purchasing and maintaining the hardware and software needed to launch and counter cyberattacks, because nations will wage cyberwarfare primarily over publicly accessible networks.[6]

Second, cyberwarfare provides an appealing option for nations because of the relative conservation of human and non-human resources. While cyberattacks are likely to generate human casualties and property destruction, cyberattacks will inflict far less damage than kinetic attacks.[7] This conservation of resources erodes

---

information warfare, electronic warfare, and cyberwar. CLAY WILSON, CONG. RESEARCH SERV., RL 31787, INFORMATION OPERATIONS, ELECTRONIC WARFARE, AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES (2007).

3. BAKER ET AL., *supra* note 1, at 26. Fifty percent of the executives "identified the United States as one of the three countries 'most vulnerable to critical infrastructure cyberattack.'" *Id.* at 30.

4. "Kinetic" warfare "involve[s] the forces and energy of moving bodies, including physical damage to or destruction of targets through use of bombs, missiles, bullets, and similar projectiles." U.S. DEP'T OF AIR FORCE, AIR FORCE GLOSSARY 57 (2007), http://www.e-publishing.af.mil/shared/media/epubs/AFDD1-2.pdf; *see also* Cheng Hang Teo, *The Acme of Skill: Non-Kinetic Warfare* 2–3 (Air Command & Staff Coll., Wright Flyer Paper No. 30, 2008), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485268&Location=U2&doc=GetTRDoc.pdf (providing a more detailed description of kinetic warfare).

5. *See, e.g.*, *Hearing Before the J. Econ. Comm. on Cyber Threats and the U.S. Econ.*, 106th Cong. (2000) (statement of John A. Serabian, Jr., Info. Operations Issue Manager, CIA) [hereinafter Serabian], *available at* https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html ("Terrorists and other non-state actors have come to recognize that cyber weapons offer them new, low-cost, easily hidden tools to support their causes."); MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 177 (2009) ("The case for cyberdeterrence generally rests on the assumption that cyberattacks are cheap and that cyberdefense is expensive."); Stephen J. Cox, Comment, *Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War*, 42 HOUS. L. REV. 881, 891 (2005) (noting low cost as an advantage of information warfare).

6. *See infra* Part II.

7. *See, e.g.*, Arie J. Schaap, *Cyberwarfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 158 (2009) ("[B]enefits include less physical destruction, less cost than other types of traditional warfare, and the ability to still achieve the same results with less risk to military personnel."); *see also* Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1440–

one of the disincentives for launching offensive war. Cyberwarfare has the added advantage of insulating cyberwarriors from physical injury: unlike their counterparts in traditional military organizations, cyberwarriors operate remotely and launch cyberattacks from within the territory of their own nation-state. The remoteness of cyberwarfare effectively eliminates the likelihood of injury or death in a physical encounter with forces from an opposing nation-state.[8] Therefore, a nation-state needs only a relatively small cadre of cyberwarriors to wage cyberwarfare, and it can assume that few, if any, of those warriors will be lost in the conflict.[9]

Third, nation-states are likely to find cyberwarfare attractive because the sponsoring nation-state may be able to disguise the source of the attacks and thereby avoid responsibility.[10] Even if Nation A suspects Nation B launched the cyberattacks that targeted its infrastructure, Nation A probably will not (and under the existing laws of war cannot lawfully) retaliate against Nation B unless and until it confirms that suspicion.[11]

For these and other reasons, nation-states will be forced to deal with the phenomenon of cyberwarfare in the years and decades to come. Cyberwarfare is a new phenomenon that differs in a number of respects from traditional warfare,[12] and these differences raise legal, policy, and practical issues that nation-states will have to resolve, both individually and collectively.[13]

---

41 (2008) ("Unlike a conventional attack, a cyber attack could neutralize . . . targets without causing physical injury to the civilians or physical damage to the site."); Dorothy E. Denning, *Barriers to Entry: Are They Lower for Cyber Warfare?*, IO JOURNAL, Apr. 2009, at 6–10 (explaining that the effects of cyber weapons are less devastating than those of kinetic warfare because cyberwarfare more indirectly results in death and often produces more short-term effects).

8. *See, e.g.*, Denning, *supra* note 7, at 8 (distinguishing cyberwarriors from traditional military personnel, who face a greater risk of physical harm); *see also* SUSAN W. BRENNER, CYBER THREATS: THE EMERGING FAULT LINES OF THE NATION STATE 71–126 (2009) (discussing the nature of cyberattacks).

9. *See supra* note 7.

10. *See, e.g.*, Cox, *supra* note 5, at 891 ("The ability to conduct [information warfare] covertly is its biggest advantage."); *see also* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 410–29 (2007) (describing difficulties associated with attempting to use point-of-attack origin to determine if an attack has come from a particular country). It is also possible for a state to disguise cyberwarfare attacks as cybercrime. *See id.* at 429–40 (analyzing the difficulties in differentiating between cybercrime, cyberterrorism, and cyberwarfare). For another related advantage of cyberwarfare, see Kelsey, *supra* note 7, at 1440–41, discussing how nation-states are less likely to run the risk of war-crime accusations or claims of violating international law of armed conflict (LOAC).

11. *See, e.g.*, BRENNER, *supra* note 8, at 62–64 (noting that under the UN Charter, only defensive war is legal).

12. *See id.* at 65–70 (discussing traditional and cyberwarfare).

13. *See, e.g.*, BAKER ET AL., *supra* note 1, at 28–29 (discussing the difficulties of regulating cyberwarfare). In the spring of 2010, Senator Carl Levin, Chairman of the

This Article focuses on a subset of those issues. As Part II explains, cyberwarfare erodes, and may erase, the distinction that currently exists between combatants (soldiers) and noncombatants (civilians).[14] Under the current law of armed conflict (LOAC), civilians are non-actors: they have no legitimate role in the conduct of traditional military hostilities.[15] However, as seen in Part II.B, civilians are destined to play an active role in cyber-hostilities—not as military personnel, but as civilians. To prepare for that eventuality, the United States will need to formulate laws that authorize civilian participation in this new arena of international combat without violating constitutional restrictions on executive and legislative authority.[16] Part III[17] addresses this issue, and Part IV provides a brief conclusion.

II. CIVILIANS IN WARFARE

> *The right of the noncombatant population to protection . . . involves . . . a corresponding duty of abstaining from . . . hostilities . . . .*[18]

Senate Armed Services Committee noted, "'capabilities to operate in cyberspace have outpaced the development of policy, law and precedent.'" *Attacks on Military Computers Cited, supra* note 1.

14. *See, e.g.*, Dakota S. Rudesill, Note, *Precision War and Responsibility: Transformational Military Technology and the Duty of Care Under the Laws of War*, 32 YALE J. INT'L L. 517, 537 n.110 (2007) (noting the "increasing reliance of the United States and other advanced militaries on civilians and their infrastructure, and the likelihood that 'cyberwar' will involve warfare through and against dual-use information technology infrastructure used predominantly by civilians").

15. *See* BRENNER, *supra* note 8, at 57–60 (discussing the development of the LOAC, specifically rules to protect civilians from war).

16. Other countries may need to take similar steps, but some, like China, do not have the constitutional and structural constraints that complicate the incorporation of civilians into a cyberwarfare effort. *See, e.g.*, BRYAN KREKEL, CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION 33–37 (2009), http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf; *see also* BRENNER, *supra* note 8, at 195–99 (discussing the blurring of the distinction between civilians and military personnel in the context of modern warfare).

17. Since compelling civilian participation in cyber hostilities creates the possibility of injury to persons and damage to civilian-owned property, nations must also develop laws that address the related issue of liability for cyberwarfare-related losses. We address these issues in our second article. *See infra* note 353.

18. Karma Nabulsi, *Evolving Conceptions of Civilians and Belligerents: One Hundred Years After the Hague Peace Conferences*, *in* CIVILIANS IN WAR 9, 16 (Simon Chesterman ed., 2001) (quoting H. Droop, *On the Relations Between an Invading Army and the Inhabitants, and the Conditions Under Which Irregular Troops Are Entitled to the Same Treatment as Regular Soldiers*, *in* TRANSACTIONS OF THE GROTIUS SOCIETY 713 (1871)).

This Part examines the legal issues raised by civilian participation in cyberwarfare. Part II.A reviews the status of civilians under the existing laws of kinetic warfare. Although cyberwarfare relies on methods other than the use of kinetic force, this Article assumes that cyberwarfare qualifies as war under international law.[19] Part II.B reviews the need for civilian participation in cyberwarfare and the roles civilians are likely to play in virtual combat. This Part also provides an empirical context for the analysis in Part III, which analyzes how the United States can compel recalcitrant civilians to become combatants in cyberwarfare.[20]

A. *Warfare*

> *. . . the inherent right of . . . self-defence if an armed attack occurs against a [state].*[21]

According to Michael S. Neiberg, war comprises three dimensions: violence, legitimacy, and legality.[22] War obviously involves violence, but warring nations need legitimacy to motivate citizens to fight for their country and convince them that killing in battle is the "right" thing to do.[23] Therefore, war differs from crime, which can also involve violence, because war "derives legitimacy from a political, societal, or religious source. Men are, in effect, given license to ignore commonly accepted societal conventions against killing and destroying."[24]

This Article's analysis of civilian participation in cyberwarfare concerns "legality," the third dimension of warfare. Legality is an

---

19. Since neither the UN Charter nor multilateral agreements, like the North Atlantic Treaty, explicitly encompass cyberattacks, there are questions as to whether such assaults qualify as warfare. *See* Robert G. Hanseman, *The Realities and Legalities of Information Warfare,* 42 A.F.L. REV. 173, 184 (1997) (noting that the United Nations list does not necessarily exclude information warfare merely because it is not explicitly mentioned). Most commentators conclude that the existing LOAC is malleable enough to encompass cyberwarfare. *See id.*; Richard W. Aldrich, *How Do You Know You Are at War in the Information Age?*, 22 HOUS. J. INT'L L. 223, 236–42, 251–52 (2000) (discussing the scope of the "use of force" under the UN Charter, customary international law, and treaties).

20. This Article assumes it will be necessary for the government to compel some civilians to participate in cyberwarfare just as it has historically been necessary to compel civilians to participate in kinetic warfare. As noted earlier, some nations would not find it particularly difficult to compel their citizens to become cyber-combatants. *See supra* note 16. Others, however, will find it necessary to address issues similar to those analyzed below. *See infra* Part III.

21. U.N. Charter art. 51, para. 1.

22. MICHAEL S. NEIBERG, WARFARE IN WORLD HISTORY 2–3 (2001).

23. One has only to contrast the American public's attitude toward World War II and toward the Vietnam War, particularly in its later stages, to appreciate the importance of legitimacy.

24. NEIBERG, *supra* note 22, at 3.

ancient requirement that has become increasingly sophisticated over the last millennium.[25] As one observer notes, nations fight wars according to "understood sets of rules."[26] These rules have historically been divided into two categories: *jus ad bellum* and *jus in bello*.[27] *Jus ad bellum* governs the legality of starting a war, and *jus in bello* governs the legality of conducting a war.[28] The modern *jus in bello* is particularly concerned with "protecting civilian populations from the injurious effects of armed conflict."[29]

That concern did not always exist. Many trace its origins to *De Jure Belli ac Pacis*, Hugo Grotius's 1625 treatise on the LOAC and peace.[30] Grotius argued that war should be governed by laws because "when arms have . . . been taken up there is no longer any respect for law . . . it is as if . . . a frenzy had openly been set loose for the committing of all crimes."[31] Grotius, and others who would later express similar sentiments, reacted to the way that wars had been waged. Until the mid-eighteenth century, armies fielded by nation-states "were composed largely of mercenaries, whose pay was intermittent and who . . . had to 'live off the country.'"[32] These untrained and undisciplined soldiers brutalized civilians and razed farms and towns in the areas they passed through.[33] For example, during the Thirty Years War in the early seventeenth century, "over

---

25. *See id.* at 9–20, 46–58 (discussing developments in the Classical Age, and the effects of nationalism and industrialism); *see also* Chris af Jochnick & Roger Normand, *The Legitimation of Violence: A Critical History of the Laws of War,* 35 HARV. INT'L L.J. 49, 60 (1994) ("A cursory review of history contradicts the view that ancient wars were lawless."); Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II,* 47 NAVAL L. REV. 176, 182–87 (2000) (providing examples of laws of war in various historical cultures).

26. NEIBERG, *supra* note 22, at 3.

27. *See, e.g.*, Geoffrey S. Corn, *Hamdan, Lebanon, and the Regulation of Hostilities: The Need to Recognize a Hybrid Category of Armed Conflict*, 40 VAND. J. TRANSNAT'L L. 295, 313 (2007) ("[I]t is indisputable that the laws of war emphasize a strict distinction between the law that regulates the conduct of armed conflict (*jus in bello*) and the law that governs the legality of the armed conflict (*jus ad bellum*).").

28. *Id.*; *see also* R.J. Araujo, *Anti-Personnel Mines and Peremptory Norms of International Law: Argument and Catalyst*, 30 VAND. J. TRANSNAT'L L. 1, 7 (1997) (describing Aquinas's foundational understanding of *jus in bello*, the justifications for war).

29. Araujo, *supra* note 28, at 7.

30. *See Hugo Grotius*, *in* THE COLUMBIA ENCYCLOPEDIA 1151, 1151 (Barbara A. Chernow & George A. Vallasi eds., 5th ed. 1998) ("Much of his book [*De Jure Belli ac Pacis*] is an attempt to make the conditions of warfare more humane by inducing respect for private people and their property."); *see generally* HUGO GROTIUS, THE LAW OF WAR AND PEACE (Oskar Piest ed., Francis W. Kelsey trans., Liberal Arts Press, 1957) (1625), *available at* http://www.lonang.com/exlibris/grotius/index.html.

31. GROTIUS, *supra* note 30, at 21.

32. TELFORD TAYLOR, THE ANATOMY OF THE NUREMBURG TRIALS: A PERSONAL MEMOIR 6 (1992).

33. *Id.*

half the German-speaking population was wiped out," and most of Europe was left in "shambles."[34]

Grotius's writings and the devastation left by the Thirty Years War led to a number of reforms, including the professionalization of soldiering: troops were trained; organized in a "chain of command" consisting of "regiments, and other standard units;" and regularly fed, clothed, and paid.[35] Armies added staff to handle supply and transport, and they established procedures to maintain discipline among troops.[36] As a result, customs and rules developed that governed soldiers' relationships with civilians and conduct while occupying foreign territory.[37]

Others echoed Grotius's call for a law of armed conflict. Rousseau, for example, said that because war is a battle between nation-states, soldiers should "respect the person and property of individuals" who are not involved in combat.[38] Others called for reform during the eighteenth century, but the LOAC remained unwritten until the nineteenth century.[39]

In the nineteenth century, humanitarian concerns prompted by newspapers' graphic accounts of battlefield violence played a role in the codification of a LOAC, as did the Union Army's commission of Francis Lieber to draft a code governing the conduct of warfare.[40] Article 15 of the Lieber Code made "military necessity" the basis for determining what actions were appropriate during military combat.[41] Under Article 15, military necessity authorized "direct destruction of life or limb of armed enemies" and others "whose destruction is incidentally unavoidable in the armed contests of the war," as well as capturing enemy soldiers and destroying property.[42] Article 16 qualified this broad grant of authority by explaining that military

---

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*; *see also* Noone, *supra* note 25, at 186–89 (citing historical understandings of soldiers as fighting not as mere men, but as men for the state, implying the necessity of principles of conduct).

38. JEAN-JACQUES ROUSSEAU, DISCOURSE ON POLITICAL ECONOMY AND THE SOCIAL CONTRACT 52 (Christopher Betts trans. 1994) (1762).

39. *See, e.g.*, af Jochnick & Normand, *supra* note 25, at 60–66 (concluding a discussion of the development of LOAC from ancient times through the eighteenth century, with the nineteenth century codification); *see also* Noone, *supra* note 25, at 189–98 (describing developments in the law of war that ultimately brought LOAC codification).

40. *See generally* FRANCIS LIEBER, INSTRUCTION FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD (Gov't Printing Office 1898) (1863) (officially published as the U.S. War Dep't, General Orders No. 100 (Apr. 24, 1863)), *available at* http://avalon.law.yale.edu/19th_century/lieber.asp; *see also* Noone, *supra* note 25, at 189–93 (describing both the effect of war correspondents' accounts and Lieber's contributions).

41. LIEBER, *supra* note 40, art. 15.

42. *Id.*

necessity "does not admit of cruelty—that is, the infliction of suffering for the sake of suffering" or "wanton devastation."[43] Article 37 of the Lieber Code specifically stated that soldiers were not to harm civilians or private property "in hostile countries occupied by them."[44]

In 1874, the Union Army's rules governing the conduct of warfare became the basis of the International Declaration Concerning the Laws and Customs of War, which was drafted at a conference in Brussels.[45] Although the Declaration was never formally adopted (and never became effective), it stimulated a series of efforts that culminated in the Hague Conference of 1899.[46]

The conference produced the Hague Convention of 1899, which failed to develop a fully realized LOAC, but formally articulated the principle that during warfare "populations and belligerents remain under . . . the principles of international law."[47] As a result, civilians and surrendering combatants should be treated as noncombatants.[48] Aside from giving some consideration to noncombatants, the 1899 Hague Convention focused primarily on the methods that could be used to conduct war: it proscribed the use of poison, set restrictions on the use of deception, and outlined procedures that should be used to minimize the death and destruction resulting from "bombardment."[49] The second Hague Conference took place in 1907, and produced another Convention that closely resembled its predecessor.[50]

In the aftermath of World War I, countries adopted pacts that outlawed the use of chemical weapons,[51] an effort that seems to have

---

43. *Id.* art. 16.

44. *Id.* art. 37. Other Articles prescribed similar treatment for museums, libraries, hospitals, churches, charities, and educational institutions. *Id.* arts. 34–36.

45. Noone, *supra* note 25, at 194.

46. *Id.* at 194–96.

47. Hague Convention (II) with Respect to the Laws and Customs of War on Land, pmbl., July 29, 1899, 32 Stat. 1803, 187 Consol. T.S. 429 [hereinafter Hague II]; *see* Noone, *supra* note 25, at 196–97 (noting the significance of the Hague II preamble).

48. Apparently, until the Middle Ages warring states tended to treat all inhabitants of opposing states as enemies, "including women and children." Jill M. Sheldon, *Nuclear Weapons and the Laws of War: Does Customary International Law Prohibit the Use Of Nuclear Weapons in All Circumstances?*, 20 FORDHAM INT'L L.J. 181, 243 n.426 (1996) (citing Lester Nurick, *The Distinction Between Combatant and Noncombatant in the Law of War,* 39 AM. J. OF INT'L L. 680, 681 (1945)). But by 1806, Napoleon's minister Talleyrand would write, "the law of nations does not permit that the rights of war, and of conquest . . . should be applied to peaceable, unarmed citizens." TAYLOR, *supra* note 32, at 7.

49. *See* Hague II, *supra* note 47, arts. 23–28.

50. *Compare id.*, *with* Hague Convention (IV) with Respect to the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, 187 Consol. T.S. 429 [hereinafter Hague IV]. *See also* Noone, *supra* note 25, at 198–99 (discussing Hague IV).

51. *See* Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65.

led to the promulgation of the 1929 Geneva Conventions: the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field and the Geneva Convention relative to the Treatment of Prisoners of War.[52] Both Conventions refined principles that had been articulated in earlier agreements and concerned the treatment of combatants.[53]

In 1949, the 1929 Geneva Conventions were superseded by four new Conventions: (I) the Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field; (II) the Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea; (III) the Convention Relative to the Treatment of Prisoners of War; and (IV) the Convention Relative to the Protection of Civilian Persons in Time of War.[54] Convention IV was "a direct result of the effect of World War II on the civilians of Europe, where the civilians and military personnel were killed in equal numbers."[55] Therefore, Convention IV makes protecting civilians and other noncombatants a binding obligation on countries that become parties to the Convention.[56] One hundred ninety-four countries have ratified Convention IV.[57]

The provisions of Convention IV "apply to all cases of declared war or of any other armed conflict which may arise between two or more . . . Parties, even if the state of war is not recognized by one of

---

52. *See* Noone, *supra* note 25, at 199–203 (describing the development of agreements about chemical weapons leading up to the 1929 Geneva Convention).

53. *See id.* at 202–03.

54. *See* Yale Law Sch., *The Laws of War*, THE AVALON PROJECT: DOCUMENTS IN LAW, HISTORY AND DIPLOMACY, http://avalon.law.yale.edu/subject_menus/lawwar.asp (last visited Sept. 26, 2010) (providing links to the Geneva Conventions, including the four 1949 Conventions referenced); *see also* Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 689 (2004) (stating that the 1949 Geneva Conventions "further rationalized and codified customary and treaty-based norms relating to armed conflict, outlining the rules applicable to civilians, prisoners of war, and wounded and sick members of armed forces").

55. Lori Hosni, *The ABCs of the Geneva Conventions and Their Applicability to Modern Warfare*, 14 NEW ENG. J. INT'L & COMP. L. 135, 141 (2007) (quoting INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW: ANSWERS TO YOUR QUESTIONS 8 (2002), http://www.icrc.org/Web/Eng/siteeng0.nsf/htmlall/p0703/$File/ICRC_002_0703.PDF).

56. *See generally* Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T 3516, 75 U.N.T.S. 287 [hereinafter Convention IV].

57. *See Geneva Conventions of 12 August 1949*, INT'L COMM. OF THE RED CROSS, http://www.icrc.org/ihl.nsf/WebSign?ReadForm&id=375&ps=P (last visited Sept. 26, 2010) (listing signatory nations with dates of signature and ratification); *see also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 17512 [hereinafter Protocol] (providing subsequent provisions elaborating on the former Conventions).

them."[58] Under Article 3, parties to the Convention must treat those who took no active part in the hostilities "humanely,"[59] and protect them from "violence to life and person" and "outrages upon personal dignity."[60] Under Article 53, parties to the Convention are prohibited from destroying any "real or personal property belonging individually or collectively to private persons . . . except where such destruction is rendered absolutely necessary by military operations."[61]

An Additional Protocol supplemented the provisions of Convention IV in 1977.[62] Article 51 of the 1977 Protocol states that civilians "enjoy general protection against dangers arising from military operations" and "shall not be the object of attack."[63] Under Article 51(3), civilians are entitled to this protection "unless and for such time as they take a direct part in hostilities."[64] Article 51 highlights the bifurcation between combatants and noncombatants that structures the modern LOAC. Article 48 of the 1977 Protocol states that "[i]n order to ensure respect for and protection of the civilian population and civilian objects," the parties to a conflict must "at all times distinguish between the civilian population and combatants and . . . direct their operations only against military objectives."[65]

Article 43(2) defines "combatants." Under Article 43(2), the "[m]embers of the armed forces of a Party to a conflict . . . are combatants, that is to say, they have the right to participate directly in hostilities."[66] Article 43(1) defines "armed forces of a Party to a conflict" as

> organized armed forces, groups and units which are under a command responsible to that Party for the conduct or its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, inter alia, shall enforce

---

58. Convention IV, *supra* note 56, art. 2. The Protocol extended the Convention's provisions to conflicts involving non-nation-state actors. *See* Protocol, *supra* note 57, art. 1(4).

59. Convention IV, *supra* note 56, art. 3(1).

60. *Id.* art. 3(2). Article 3(2) also prohibits the taking of hostages, passing of sentences, and carrying out of executions without adequate judicial process. *Id.*

61. *Id.* art. 53. This provision has been interpreted as applying to the property of natural persons (e.g., corporations and other artificial entities) as well as to property owned by real persons. *See, e.g.*, Aaron Ezekiel, *The Application of International Criminal Law to Resource Exploitation: Ituri, Democratic Republic of the Congo*, 47 NAT. RESOURCES J. 225, 238 (2007) (discussing this provision of Convention IV, which "prohibits destruction of state and property owned collectively").

62. *See supra* note 58; *see generally* Protocol, *supra* note 57.

63. Protocol, *supra* note 57, art. 51(1)–(2).

64. *Id.* art. 51(3).

65. *Id.* art. 48.

66. *Id.* art. 43(2).

> compliance with the rules of international law applicable in armed conflict.[67]

Article 4 of Convention III, which deals with the treatment of with prisoners of war,[68] broadens this definition of combatants. Article 4 affords prisoner-of-war status to certain combatants, including members of the armed forces of a party and members of "other militias and members of other volunteer corps" who meet certain requirements.[69] To qualify as combatants, members of militias and "other volunteer corps" must satisfy the following conditions: "(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; [and] (d) that of conducting their operations in accordance with the laws and customs of war."[70] Most commentators agree that the Geneva Conventions create "only two categories: lawful combatants, and civilians."[71] The United States, however, takes the position that there are three categories: "lawful combatants, unlawful combatants, and civilians."[72]

A lawful combatant qualifies as a "combatant" under the Geneva Convention and gains immunity "from prosecution for lawful combat activities."[73] If captured, a lawful combatant receives Geneva Convention prisoner-of-war status "with its special rights, better conditions and more extensive set of benefits."[74] An unlawful combatant is a civilian (someone who does not qualify as a combatant) who nevertheless takes a direct role in the military hostilities.[75] Unlawful combatants forfeit a lawful combatant's immunity from prosecution and prisoner-of-war status and, if

---

67. *Id.* art. 43(1).

68. Geneva Convention (III) Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Convention III].

69. *Id.* art. 4(A)(2). The list also includes ship crews and

> [i]nhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.

Id. art. 4(A)(5)–(6).

70. *Id.* art. 4(A)(2)(a)–(d); *see also* Protocol, *supra* note 57, arts. 43–44 (defining those eligible for prisoner-of-war status along the same lines). These same conditions appear in Hague IV, *supra* note 50, annex, art. 1.

71. Curtis A. Bradley, *The United States, Israel & Unlawful Combatants*, 12 GREEN BAG 397, 398 (2009).

72. *Id.* at 399 (citation omitted).

73. Joseph P. Bialke, *Al-Qaeda & Taliban Unlawful Combatant Detainees, Unlawful Belligerency, and the International Laws of Armed Conflict,* 55 A.F.L. REV. 1, 10–11 (2004).

74. *Id.*

75. W. James Annexstad, *The Detention and Prosecution of Insurgents and Other Non-Traditional Combatants*, ARMY LAW, July 2007, at 72.

captured, "may be tried in a military commission; and if convicted, be punished appropriately."[76] The third category is civilians: individuals who do not qualify as combatants under the Geneva Convention standards and did not take an active role in carrying out military hostilities.[77]

The rules that define the statuses and obligations of civilians and combatants were formulated with individuals in mind because individuals have historically been the sole participants in war: soldiers waged war and civilians suffered the vagaries of war. The Geneva Conventions consequently do not explicitly apply to corporations and other artificial entities.[78] They may, however, reach a corporation's "conduct as violative of customary international law."[79]

Under existing law, warfare is the exclusive province of nation-states,[80] which wage war through the individuals who constitute their armed services.[81] Civilians as civilians have no legitimate role in kinetic warfare.[82] Part III considers whether the same state of affairs should exist for cyberwarfare. Before considering that issue, however, Part II.B examines why some believe that it will be necessary for civilians to take an active role in the conduct of cyberwarfare.

---

76. Bialke, *supra* note 73. For more on this distinction and its consequences, see Benjamin J. Priester, *Who Is a "Terrorist"? Drawing the Line Between Criminal Defendants and Military Enemies*, 2008 UTAH L. REV. 1255, 1280–83 (2008).

77. *See, e.g.*, Thomas J. Bogar, *Unlawful Combatant or Innocent Civilian? A Call to Change the Current Means for Determining Status of Prisoners in the Global War on Terror*, 21 FLA. J. INT'L L. 29, 41–42 (2009) (defining civilians).

78. *2003–2004 Survey of International Law in the Second Circuit*, 31 SYRACUSE J. INT'L & COM. 327, 335–36 (2004) [hereinafter *2003–2004 Survey*]; *see* Presbyterian Church of Sudan v. Talisman Energy, Inc., 244 F. Supp. 2d 289, 316–17 (S.D.N.Y. 2003) (discussing the applicability of treaties to corporations).

79. *2003–2004 Survey*, *supra* note 78, at 336–37. It is not settled as to whether the Geneva Conventions are part of the *jus cogens*—the "intransgressible principles of international customary law." Jean-Marie Henckaerts, *The Grave Breaches Regime as Customary International Law*, 7 J. INT'L CRIM. JUST. 683, 700–01 (2009).

80. *See, e.g.*, BRENNER, CYBER THREATS, *supra* note 8, at 54 (defining war).

81. In the modern world, armed services are composed of individuals who have, more or less, willingly chosen to enlist. GEORGE Q. FLYNN, CONSCRIPTION AND DEMOCRACY: THE DRAFT IN FRANCE, GREAT BRITAIN, AND THE UNITED STATES 1–6 (2002); Adrian R. Lewis, *Conscription, the Republic, and America's Future*, 89 MIL. REV. 15, 15–24 (2009); *see also* David R. Segal & Mady Wechsler Segal, *America's Military Population*, 59 POPULATION BULL. 4, 5–6 (2004) (describing the military recruiting pool). Once civilians join one of their nation's armed services, they cease to be civilians. *See infra* Part III.B.

82. *See, e.g.*, Won Kidane, *The Status of Private Military Contractors Under International Humanitarian Law*, 38 DENV. J. INT'L L. & POL'Y 361, 377–86 (2010) (describing the role of civilians in the Geneva Conventions' framework).

B. *Cyberwarfare*

> *[W]elcome cyber-warriors . . . . Our nation's future depends on you.*[83]

To understand why civilians may have to become cyberwarriors, one needs to appreciate how and why war has historically differed from other human endeavors, as well as why these differences are likely to be less pronounced for cyberwarfare. This Part addresses each of these issues.

1. Kinetic Warfare

The Supreme Court once described war as "the exercise of force by bodies politic . . . against each other, for the purpose of coercion."[84] War, as described earlier, is a struggle between nation-states.[85] While it is carried out by individuals who act on behalf of the states to which they owe allegiance, war—unlike other human endeavors such as commerce, domestic life, and crime—is, for both conceptual and practical reasons, a purely collective undertaking.[86]

Conceptually, war is a struggle between two sovereign entities. While sovereign entities are comprised of individuals, they assume an existence, and an agenda, of their own.[87] Individuals struggle to achieve prosperity, prominence, or other personal goals. Nation-states, on the other hand, struggle to achieve political dominance.[88]

---

83. Charles J. Dunlap, Jr., *Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors*, 87 NEB. L. REV. 712, 724 (2009).

84. The Brig Amy Warwick (The Prize Cases), 67 U.S. (2 Black) 635, 652 (1863).

85. *See supra* notes 80–81 and accompanying text.

86. *See, e.g.*, Willard Hurst, *Treason in the United States*, 58 HARV. L. REV. 806, 836 (1945) ("'[W]ar' is in its nature a collective activity. . . . [I]n no fair sense of the term could the isolated acts of an individual be said to constitute war against a state."); *see also* United States v. Burr, 25 F. Cas. 55, 137 (C.C.D. Va. 1807) (No. 14,693).

> George III. levies war. . . . It is he . . . by whose directions the troops are raised and employed. It is he who levies the war, and not his subjects, who fight the battles. . . . If the subjects of the king of Great Britain were to levy war upon this country, they would . . . be . . . robbers, pirates, and murderers, according to the acts which they would commit; and . . . they would be regarded as individual offenders who had perpetrated those crimes, and proceeded against as such.

Burr, 25 F. Cas. at 137.

87. *See, e.g.*, BRENNER, CYBER THREATS, *supra* note 8, at 68–70 (discussing the role of the nation-state in warfare); *see also The Prize Cases*, 67 U.S. (2 Black) at 652 (noting that war is a struggle between "bodies politic").

88. *See* BRENNER, CYBER THREATS, *supra* note 8, at 221 (discussing relations between nation-states aimed at preserving order).

Historically, war involved a "contention between at least two" nation-states that use their armed forces in an effort to overpower the opposing nation-state(s) and impose "peace on the victor's terms."[89] The enormity of the stakes in war therefore transcends the grasp, and the capacity, of discrete individuals.

Practically, war has been the exclusive province of nation-states because only sovereign entities have been able to summon and exercise the kinetic force needed to wage these vast armed struggles.[90] Non-nation-state actors have on occasion declared war on nation-states,[91] but these declarations are merely symbolic gestures, as no aggregation of individuals can acquire and implement the kinetic resources needed to wage war credibly with one or more nation-state actors.[92] As a result, nation-states have treated these non-state actors as criminals or terrorists.[93]

Traditionally, therefore, individuals could play a legitimate role in the process of waging war only by joining the armed forces of one of the nation-states. This role was not only legitimate; it was essential. Nation-states necessarily act through individuals, and aggregations of individuals serve as a tool that states use to conduct their struggles with each other.[94]

This state of affairs, however, can persist as long as the conditions that sustain it continue to exist. If war ceases to be a struggle between nation-states, and if nation-states no longer

---

89. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 5 (2005). War has been monopolized by the dominant sovereign entity, which has not always been the nation-state. *See generally* MARTIN VAN CREVELD, THE RISE AND DECLINE OF THE STATE (1999) (tracing the evolution of sovereign entities from tribes through city-states and empires to nation-states); BRENNER, *supra* note 8, at 204–08 (discussing the development of nation-states).

90. BRENNER, CYBER THREATS, *supra* note 8, at 208–22; *see also* VAN CREVELD, *supra* note 89, at 242–58 (discussing the large scale and expense of modern warfare). To preserve this monopoly, nation-states take steps to prevent weaponry they control from falling into the hands of civilians or other (possibly hostile) nation-states. *See, e.g.*, 21 U.S.C. § 2751 (2006) (limiting the transfer of arms to foreign governments); *see also Announcement of the Export Control Act 2002*, June 24, 2003, *in* PRACTISING LAW INST., COPING WITH U.S. EXPORT CONTROLS 2008, app. at 485, 581–83 (2008) (describing U.K. export control laws); Robert A. Borich, Jr., *Globalization of the U.S. Defense Industrial Base: Developing Procurement Sources Abroad Through Exporting Advanced Military Technology*, 31 PUB. CONT. L.J. 623, 627–32 (2002) (describing U.S. export control laws). The Supreme Court has indicated that the Second Amendment does not give U.S. citizens the right to possess military-grade weaponry. District of Columbia v. Heller, 554 U.S. 570, 677–79 (2008).

91. *See, e.g.*, Al Qaeda's Fatwa (Feb. 23, 1998), *available at* http://www.pbs.org/newshour/terrorism/international/fatwa_1998.html (declaring jihad, or holy war, on the United States and Israel).

92. *See, e.g.*, VAN CREVELD, *supra* note 89, at 242–58 (discussing the state's central role in the development and prosecution of modern warfare).

93. *See, e.g.*, BRENNER, CYBER THREATS, *supra* note 8, at 37–42 (discussing the development of the concept of terrorism).

94. *See supra* note 86 and accompanying text.

monopolize the weapons used to wage war, traditional warfare may no longer be viable. The following subpart addresses this issue.

2. Cyberwarfare

This Article frames the discussion of cyberwarfare around the roles combatants play in war. More precisely, this Article derives a dichotomy from the roles that combatants traditionally play and uses this dichotomy to explain why and how civilians will become embroiled in cyberwarfare. Military combatants play two roles: offensive and defensive.[95] In their offensive role, soldiers attack the forces of an enemy nation-state; in their defensive role, they seek to repel an attack launched by enemy forces.[96]

These roles—as well as the conception of war from which they derive—are predicated on the assumption that combatants are segregated from noncombatants.[97] In other words, these roles assume segregation between war-space and civilian-space. As we saw earlier, this assumption derives from the LOAC, which requires military commanders to protect civilian populations from the "dangers arising from military operations."[98]

While this principle and the assumed segregation it generates can become problematic, both the principle and the assumed segregation continue to be viable components of conventional warfare.[99] Their viability erodes, however, within the context of cyberwarfare. This erosion manifests itself in two ways, each of which is analogous to one of the roles combatants play in warfare. The subparts below explain how cyberspace erodes the segregation between war-space and civilian-space and how that erosion undermines the distinction between combatants and noncombatants.

---

95. *See, e.g.*, U.S. DEP'T OF ARMY, FIELD MANUAL 3.0: OPERATIONS, paras. 3-37–3-67 (2008) (describing offensive and defensive operations).

96. *See, e.g.*, *id.* para. 3-37 ("Offensive operations are combat operations conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers."); *see also id.* para. 3-53 ("Defensive operations counter enemy offensive operations.").

97. *See supra* Part II.A.

98. Protocol, *supra* note 57, art. 51; *see also supra* notes 63–65 and accompanying text.

99. *See, e.g.*, Jack M. Beard, *Law and War in the Virtual Era*, 103 AM. J. INT'L L. 409, 409–10 (2009) (noting the ongoing concern for avoiding civilian casualties in kinetic warfare); R. George Wright, *Combating Civilian Casualties: Rules and Balancing in the Developing Law of War*, 38 WAKE FOREST L. REV. 129, 140 (2003) (noting the increasing ability to differentiate between military targets and civilians using modern technology).

(a) Defensive Engagement

As noted above, it is possible to maintain some segregation between war-space and civilian-space in kinetic combat. That possibility provides empirical support for laws that require military commanders to separate combatants from civilians.[100] The viability of segregating combatants and noncombatants, however, depends on physical reality.

Kinetic warfare takes place in real-space, which is fixed, tangible, and structured by three physical dimensions.[101] Since physical reality is objective and therefore stable, it is possible for commanders to structure combat activity to have as little effect as possible on civilians. The use of new weapons technologies in the twentieth century complicated the process of segregating war-space and civilian-space, but segregation remained a feasible goal because of the inherent stability of the physical context within which combat occurred.[102]

The use of cyberspace as the medium for attacks further complicates that process because combat takes place in an environment that is unreal, and therefore inherently unstable. Cyberwarfare takes place "in" cyberspace, which is a "domain characterized by the use of electronics . . . to store, modify, and exchange data via networked systems and associated physical infrastructures."[103] Cyberspace is not a physical "place;" it is a "virtual interactive experience" accessible regardless of geographic location.[104] Cyberspace is in effect a fourth dimension—an interactive overlay that is superimposed on and supersedes the constraints of physical reality.[105] As a result, cybercombat will differ

---

100. *See supra* Part II.A.

101. *See, e.g.*, CONCISE OXFORD ENGLISH DICTIONARY 1373 (Judy Pearsall ed., 10th rev. ed. 2002) (defining "space" as "the dimensions of height, depth and width within which all things exist and move").

102. *See, e.g.*, Nathan A. Canestaro, *Legal and Policy Constraints on the Conduct of Aerial Precision Warfare*, 37 VAND. J. TRANSNAT'L L. 431, 447 (2004) (explaining that in World War II the then-new technology used to launch air strikes created a "crisis of discrimination" because "the technology to discriminate military targets from civilian areas" did not yet exist).

103. Michael W. Wynne, Sec'y of the Air Force, Remarks as Delivered to the C4ISR Integration Conference: Cyberspace as a Domain in Which the Air Force Flies and Fights (Nov. 2, 2006), http://www.airforce-magazine.com/SiteCollectionDocuments/TheDocumentFile/Speeches%20and%20Transcripts/wynne_spch110206.pdf.

104. *Cyberspace*, WIKIPEDIA, http://en.wikipedia.org/wiki/Cyberspace (last visited Sept. 26, 2010).

105. *See, e.g.*, Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1, ¶ 11 (2001), http://www.boalt.org/bjcl/v4/v4brenner.htm ("Cyberspace is a domain that exists along with but apart from the physical world."); *see generally* Natasha Solce, Comment, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 296–97 (2008)

in certain respects from the kinetic attacks used in conventional warfare. Combat will be carried out in a different way, even though the goals of combat may remain the same.[106]

At a basic level, cyberwarfare will involve using computer systems to attack other computer systems.[107] Many, however, predict that cyberwarfare operations will be considerably broader than simple attacks on computer systems, and that the attacks will target the victim state's critical infrastructure.[108] Federal law defines

---

(explaining that cyberspace, because of its interconnectedness, is a battlefront that needs to be protected like all others).

106. The goals of cyberwar will remain the same as the goals of kinetic war because both involve struggles for political advantage or dominance between two nation-states. As noted above, only the methods used in a struggle differentiate the two types of warfare. A scene in an episode of the BBC television show *Spooks* illustrates how the methods will differ. John Ozimek, Spooks *Foils Fictional Russian Plot*, THE REGISTER (Nov. 1, 2008), http://www.theregister.co.uk/2008/11/01/spooks_submarine_shutdown/. In the show, agents of the Russian Security Services

> tapped into a transatlantic cable—just off the shore of Cornwall—and prepared to upload a virus onto the UK internet. The virus would have propagated itself to thousands of websites within the UK—and then taken them down key elements of the national network by over-loading them with requests for data.

Id. As explained in the text above, an attack like this could be a viable component of a cyberwarfare assault. The problem with this scenario is not the result the attack was intended to achieve, but rather how the scriptwriters structured the attack itself:

> [T]he submarine . . . was one of the night's dumber plot devices. As our in-house expert said: 'They'd have a hard time putting a sub on top of a cable covertly—normally a sub which has stayed down for a while only has a sketchy idea of where it is, and . . . the cables aren't accurately mapped or easy for a naval sub to detect. And why bother? It's not as though there's some Great Firewall of the UK located offshore somewhere.'
>
> In fact they could probably do just as much damage launching the programme from an internet café in Ealing.

Id. In kinetic warfare, it is essential for the ship, submarine, airplane, or drone that is delivering a weapon to its target to be physically proximate to that target; in cyberwarfare, as Ozimek pointed out, physical proximity is irrelevant. *Id.*

107. *See, e.g.*, Timothy Shimeall et al., *Countering Cyber War*, 49 NATO REV. 16, 17 (2001) ("In a limited cyber war, the information infrastructure is the medium, target and weapon of attack . . . ."); *see also* STEVEN A. HILDRETH, CONG. RESEARCH SERV., RL 30735, CYBERWARFARE 11 (June 19, 2001) (noting the Russian view that cyberwarfare involves disrupting enemy computer systems). Air Force Policy Directive 10–7 defines "network warfare operations" as "integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital portion of the battlespace. Network warfare operations are conducted in the information domain through dynamic combination of hardware, software, data, and human interactions." U.S. DEP'T OF AIR FORCE, POLICY DIRECTIVE 10–7: INFORMATION OPERATIONS 22 (Sept. 6, 2006), http://www.fas.org/irp/doddir/usaf/afpd10-7.pdf.

108. *See, e.g.*, Schaap, *supra* note 7, at 133 (stating that Russia's cyberwarfare capability "would disrupt financial markets and . . . civilian communications capabilities as well as other parts of the enemy's critical infrastructure"); *see also* Susan Landau, *National Security on the Line*, 4 J. TELECOMM. & HIGH TECH. L. 409, 429–31 (2006) (discussing the threat cyberwarfare poses to critical infrastructure);

"critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[109]

Attacking a nation's critical infrastructure allows a hostile state to erode the victim state's internal operational viability and morale,[110] and an attack can deprive the victim state of "infrastructure that supports military actions."[111]

Civilians affect the defense of cyberwarfare because they tend to own the components of a nation's critical infrastructure.[112] Since critical infrastructures are "likely targets" in cyberwar, private

---

Ellen Messmer, *"Cyber War" Author: U.S. Needs Radical Changes to Protect Against Attacks,* FOX BUS., Apr. 7, 2010, http://www.foxbusiness.com/personal-finance/2010/04/07/cyber-war-author-needs-radical-changes-protect-attacks/ (same). One article distinguishes this type of cyberwar campaign from the more limited type noted above. Shimeall et al., *supr*a note 107.

> An unrestricted cyber campaign would . . . be directed primarily against the target country's critical national infrastructure: energy, transportation, finance, water, communications, emergency services and the information infrastructure itself. It would likely cross boundaries between government and private sectors. . . . Ultimately, an unrestricted cyber attack would likely result in significant loss of life, as well as economic and social degradation.

Id.; *see also* Coleman, *supra* note 2 (defining cyberwar as using "attacks on computers . . . to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses").

109. 42 U.S.C. § 5195c(e) (2006). The Homeland Security Act of 2002 incorporated this definition. Pub. L. No. 107–296, § 2, 116 Stat. 2135, 2140 (codified at 6 U.S.C. § 101(4) (2006)). A similar definition is incorporated into 50 U.S.C. app. § 2152(2) (2006), which applies to national defense. A recent report notes that critical infrastructure components include banking and finance, electrical grids, oil and gas refineries and pipelines, water and sanitation utilities, telecommunications, and other systems. *See generally* BAKER ET AL., *supra* note 1.

110. *See, e.g.*, Brian M. Mazanec, *The Art of (Cyber) War*, 16 J. INT'L SEC. AFF. (2009), *available at* http://www.securityaffairs.org/issues/2009/16/mazanec.php (noting "loss of confidence in the U.S. government" that would result from a "chronic loss of services such as power, emergency response, television and telephony across the U.S.," and stating that cyberattacks could "wreak economic havoc" on the United States).

111. Schaap, *supra* note 7, at 172; *see also The New Cyber College of International Lawyers*, 95 AM. SOC'Y INT'L L. PROCEEDINGS 173, 182 (2001) (noting the impact a cyberattack on critical infrastructure would likely have on the civilian population).

112. *See* Shimeall et al., *supr*a note 107, at 17 (listing predominantly civilian entities among the components of information infrastructure); *see also* THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 1 (2003), http://www.dhs.gov/xlibrary/ assets/National_Cyberspace_Strategy.pdf (explaining that the United States' critical infrastructure consists of public and private assets "in several sectors," including commerce, transportation, utilities, and telecommunications). Governments often own certain components of a nation's critical infrastructure, such as emergency services, law enforcement agencies, and water and sanitation facilities. *See id*.; BAKER ET AL., *supra* note 1, at 25 ("Globally, a majority of critical infra-structure is in the hands of private companies.").

companies are likely to be "caught in the crossfire" of cyberwarfare,[113] and they could even become the specific targets of a deliberate cyberattack.[114] It is far from certain that such an attack violates the LOAC.[115]

As Part II.A discussed, the contemporary LOAC evolved to address the conduct of kinetic warfare and is therefore triggered by activity that is identical or analogous to the activity involved in kinetic combat. The requirement of an "armed attack" or the "use of force" derives from the modern *jus ad bellum*,[116] and the primary source of the contemporary *jus ad bellum* (a part of the LOAC) is the UN Charter.[117] Article 2(4) of the Charter outlaws aggressive war and prohibits a nation-state from employing "the threat or use of force against the territorial integrity or political independence of [another] state, or in any other manner inconsistent with the Purposes of the United Nations."[118]

The Charter creates two exceptions to this prohibition: Security Council action under Article 42 and self-defense under Article 51 do not implicate Article 2(4).[119] Article 51 applies to nation-states and provides that "[n]othing in the present Charter shall impair the inherent right of . . . self-defence if an armed attack occurs against a Member of the United Nations."[120] Under the UN Charter, "war" involves a "use of force" or an "armed attack."[121] The Charter, however, does not define either term.[122]

---

113. BAKER ET AL., *supra* note 1, at 31. Eight years ago, a CIA representative told Congress that

> We are detecting . . . offensive cyber warfare programs in other countries. . . . Those nations . . . recognize the value of attacking adversary computer systems, both on the military and domestic front. . . . [T]hey stress the power of cyber warfare when targeted against civilian infrastructures, particularly those that could support military strategy.

Serabian, *supra* note 5.

114. BAKER ET AL., *supra* note 1, at 1.

115. *See, e.g.*, Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV. 1, 5–6 (2009) (showing that experts do not agree on whether a cyberattack constitutes an "act of war," armed attack, or a use of force sufficient to trigger the application of the LOAC).

116. *See supra* notes 27–28 and accompanying text.

117. *See, e.g.*, Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 412 (2007) ("The legal basis for the *jus ad bellum* paradigm is . . . the United Nations Charter.").

118. U.N. Charter art. 2, para. 4.

119. U.N. Charter arts. 42, 51; Condron, *supra* note 117, at 412.

120. U.N. Charter art. 51.

121. This was intended to outlaw aggressive war. Dominika Svarc, *Redefining Imminence: The Use of Force Against Threats and Armed Attacks in the Twenty-First Century*, 13 ILSA J. INT'L & COMP. L. 171, 172 (2006).

122. *See, e.g.*, Davis Brown, *Use of Force Against Terrorism After September 11th: State Responsibility, Self-Defense and Other Responses*, 11 CARDOZO J. INT'L & COMP. L. 1, 21 (2003) (armed attack); Matthew Hoisington, *Cyberwarfare and the Use*

Because the UN Charter was written long before the Internet existed, it was clearly not intended to encompass cyberattacks.[123] Therefore, it is reasonable to assume that the Charter encompasses only kinetic attacks. Since cyberattacks will almost certainly not involve the use of physical force, the Charter and the contemporary LOAC probably do not apply.[124] If the LOAC does not apply to cyberattacks, a country would not commit an illegal act by deliberately launching such attacks at civilian-owned targets; this distinction makes offensive cyberwarfare an attractive option for aggressive nation-states.[125]

---

of Force Giving Rise to the Right of Self-Defense, 32 B.C. INT'L & COMP. L. REV. 439, 440–41 (2009) (use of force).

Article 1 of a related document, the UN Definition of Aggression, defines "aggression" as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State;" Article 3 asserts that "act of aggression" includes invasion, bombardment, and attacks on the victim state's armed forces or marine or air fleets. G.A. Res. 3314 (XXIX), Annex, U.N. GAOR, 29th Sess., Supp. No. 31, U.N. Doc. A/9631, at 143 (Dec. 14, 1974). It also includes attacks by "irregulars or mercenaries" that can be attributed to a nation-state. *See id.* art. 3(g) at 143 ("substantial involvement" of a nation-state).

123. *Cf.* Condron, *supra* note 117, at 413 (noting that although the UN Charter predates the Internet, "many legal scholars would probably agree that a cyber attack *could* amount to a use of force or an armed attack").

124. *See, e.g.*, Schaap, *supra* note 7, at 144–47 (noting that the "international community" seems to assume cyberattacks do not constitute armed attacks or a use of force, at least not unless they cause physical damage). In 2007, Estonia was the target of a two week sequence of cyberattacks that at least resembled cyberwarfare. BRENNER, CYBER THREATS, *supra* note 8, at 1–6. During the attacks, Estonia struggled to maintain the operational viability of essential systems, and sought assistance from the North Atlantic Treaty Organization (NATO). Schaap, *supra* note 7, at 144–45. NATO declined to become involved. As Estonian Defense Minister Jaak Aaviksoo explained, "NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty . . . will not . . . be extended to the attacked country.'" *Id.* (citing Johnny Ryan, *"iWar": A New Threat, Its Convenience—and Our Increasing Vulnerability*, NATO REV. (2007), *available at* http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.). *See generally* Ellen Messmer, *Is the U.S. the Nation Most Vulnerable to Cyberattack?*, NETWORK WORLD (April 7, 2010, 8:07 AM), http://www.networkworld.com/news/2010/040610-cyberattacks-clarke.html (stating that the UN Charter and LOAC "provide a reasonable starting point" for developing a law of cyberwarfare).

125. A state's ability to disguise the nature and source of cyberattacks is one factor that makes cyberattacks an attractive method of aggressive warfare. *See, e.g.*, Brenner, *supra* note 10, at 427–40. Russia is considering legislation that would address this gap in the current LOAC:

> A newly proposed law would give Moscow authority to define and respond to acts of cyber war. The new law 'essentially says that if they can determine that they have been targeted by a government of another state in a cyberattack, of whatever kind, they can treat it as an act of war.'

See also BAKER ET AL., *supra* note 1, at 30 (quoting Kimberly Zenz, Russia Specialist, iDefense Labs). Although aggressive cyberwarfare may not qualify as unlawful warfare under the UN Charter and other aspects of the LOAC, it may still constitute something. It might qualify as state-sponsored terrorism, state-sponsored crime, or

Consequently, civilian involvement in offensive cyberwarfare will be at least partially defensive.[126] Whether an attack targets the electrical grid, the financial system, the air traffic control system, or any of a host of other infrastructure components, the attacker will direct hostile traffic at the computer systems used by the target entities.[127] At that point, the computer staff of the target entities are in a position analogous to that of soldiers who are being attacked by the military forces of enemy nation-states: their position is probably most analogous to that of a harbor fortress being shelled by enemy ships. Like the soldiers in the fortress, computer personnel confronting a cyberattack are responsible for defending their "territory" from hostile activity, and their primary defensive goal will be to keep their systems functioning despite attempts to shut them down.[128]

If confronted with a cyberattack, computer personnel can try to nullify or minimize the effects of the signals targeting their systems or try to end the attack by striking back at the attackers.[129] The most

---

both. Those issues, however, are outside the scope of this Article. For an examination of those issues, see BRENNER, CYBER THREATS, *supra* note 8, at 152–55.

126. *See infra* Part II.B.2.b for more information on offensive civilian involvement in cyberwar.

127. For a description of tools likely to be used in such an attack, see Ashar Aziz, *Barbarians Inside the Cyber Gates*, FIREEYE MALWARE INTELLIGENCE LAB (Jan. 14, 2009), http://blog.fireeye.com/research/2009/01/barbarians-inside-the-cyber-gates; Richard Stiennon, *Technology and the Advent of Cyber War*, INFO. SECURITY RESOURCES (Dec. 15, 2009), http://information-security-resources.com/2009/12/15/technology-and-the-advent-of-cyber-war/. Distributed denial-of-service attacks were used in the large-scale attacks on Estonia in 2007, attacks Estonia initially believed were cyberwarfare. BRENNER, CYBER THREATS, *supra* note 8, at 1–6.

128. One observer used a mixed metaphor to describe this state of affairs:

> "Right now, the sheriff isn't there," said retired Gen. Michael Hayden, who recently ended a long career as a senior U.S. intelligence official as the director of the CIA, saying cyberspace was like the Wild West of legend. "Everybody has to defend themselves, so everyone's carrying a gun." But in the cyber domain that was like expecting each citizen to organize their own national defense. "You wouldn't go to a post office and ask them how they're tending to their own ballistic missile defense . . . but that is the equivalent of the current set-up in cybersecurity," Hayden said.

BAKER ET AL., *supra* note 1, at 26.

129. The Estonian defenders' efforts to minimize the effects of the 2007 distributed denial-of-service attacks are an example of a purely defensive cyberwar strategy. *See* BRENNER, CYBER THREATS, *supra* note 8, at 3–5 (describing the Estonian effort to defend against the attacks). Offensive cyberwar strategy involves "'shut[ting] down somebody trying to attack us.'" Lance Whitney, *Cyber Command Chief Details Threats to U.S.*, CNET NEWS (Aug. 5, 2010) (quoting General Keith Alexander), http://news.cnet.com/8301-13639_3-20012774-42.html. It could also involve attacking a potential enemy either before they attack the United States or as an independent response to an attack on computers in this country. *Id.*; *see also* David E. Sanger et al., *U.S. Steps Up Effort on Digital Defenses*, N.Y. TIMES, April 28, 2009, at A1 (describing potential defenses).

likely response is purely defensive: the assaulted computer personnel will try to nullify or minimize the effects of the attack.[130] In this mode, the position of the computer staff resembles that of civilians in kinetic warfare. Their reactive role resembles casualties (or prospective casualties) whose goal is to limit the amount of damage to the systems for which they are responsible for sustaining. The methods they employ will differ from those civilians have used to withstand kinetic warfare, but the goal is the same. The role they play in attempting to achieve that goal resembles the role civilians play in kinetic warfare, but it differs in certain respects. The most significant difference is that these civilians are advertent targets.[131] As we explain in Part III, this and other aspects of civilians' defensive involvement in cyberwar raise legal issues that have yet to be resolved.[132]

The second response option for computer personnel bombarded by a cyberattack is a defensive–offensive strategy. Although this option involves offensive action in the form of a counterstrike in an effort to end the attack, this Article refers to the counterattack as a defensive–offensive strategy because the use of offensive tactics is reactive. The counterattack is triggered by an attack and is intended to end the attack, unlike the purely offensive strategy we examine in the next subpart.

The civilians' response in this mode is more analogous to the response of a soldier under attack: they will use both defensive and offensive tactics to withstand and repel the attack. Although the use of a defensive–offensive strategy by civilians is not unheard of in the physical world, it is unusual.[133] More precisely, the use of an offensive strategy—whether coupled with or dissociated from a defensive strategy—is an unusual response by civilians caught up in

---

130. Aside from anything else, this would constitute a "legal" response under the LOAC. *See supra* notes 118, 120 and accompanying text (purely offensive attacks are illegal under Article 2 of the UN Charter; pursuant to Article 51 of the UN Charter, only the use of military force in self-defense is legal).

131. *See supra* Part II.A.

132. The fact that civilians are intentionally targeted raises other legal issues as well. If cyberattacks constitute cyberwar, deliberately targeting civilians violates the LOAC; if cyberattacks do not constitute cyberwar, deliberately targeting civilians does not violate the LOAC. It seems they should qualify either as state-sponsored cybercrime or state-sponsored cyberterrorism. These issues, though, are outside the scope of this Article. *See supra* note 125.

133. *See, e.g.*, KARMA NABULSI, TRADITIONS OF WAR: OCCUPATION, RESISTANCE, AND THE LAW 47–51 (1999) (describing guerilla warfare during the Napoleonic Era). The French Resistance's activities during the Nazi occupation of France in the 1940s are an example of a defensive–offensive strategy. *See French Resistance*, WIKIPEDIA, http://en.wikipedia.org/wiki/French_Resistance (describing tactics of the *La Résistance*) (last visited Sept. 26, 2010).

kinetic war[134] for two reasons. The first and perhaps most obvious reason is that civilians usually do not have military-grade weaponry they can use to engage the forces of an enemy nation-state effectively.[135] The second reason is that mounting an offensive response, regardless of whether it is effective or not, can result in punitive reprisals.[136]

If our use of cyberspace does not eliminate the weapons problem, it certainly erodes the constraint on civilian offensive tactics, because most computer hardware and software can be used both by civilians and by military personnel.[137] As for reprisals, there seems to be no logical reason why the use of cyberspace should eliminate them as a possibility, although the nature of the medium might reduce the punitive nature of reprisals. Cyber-mediated reprisals are unlikely to inflict the physical carnage historically associated with reprisals in kinetic warfare.[138] If that is true, the reduction in the physical severity of reprisals might mean that civilians will be more willing to resist cyberattacks than physical attacks.

The critical factor differentiating offensive and defensive participation is that defensive civilian engagement is purely reactive, while offensive civilian engagement is aggressive in varying degrees.

---

134. Aside from anything else, the atypicality of civilian resistance is inferentially derivable from the fact that it was seen as criminal conduct under the early LOAC and is outlawed under the current version of the LOAC. *See, e.g.*, Nablusi, *supra* note 18, at 15–17 (discussing the different rights and protections of civilians and soldiers in war). It may also be due, at least to some extent, to the fact that civilians who join a resistance group forfeit their status as civilians. *See* Convention III, *supra* note 68, art. 4(2); Protocol, *supra* note 57, art. 50(1).

135. *See, e.g.*, *Warsaw Ghetto Uprising*, WIKIPEDIA, http://en.wikipedia.org/wiki/Warsaw_Ghetto_Uprising (last visited Sept. 26, 2010) (indicating that Jewish civilians who rebelled against the Nazi's occupying the Warsaw Ghetto in World War II had few weapons, all of which were inferior to the military-grade weaponry used by the German forces).

136. *See id.* (describing the German response to the uprising). For the historical view of military reprisals against civilians who resisted their advance, see, for example, NABULSI, *supra* note 133, at 27–32.

137. *See, e.g.*, Schaap, *supra* note 7, at 156.

> Dual-use targets are . . . used for both military and civilian purposes, such as power plants that provide electricity to both civilian institutions as well as military command and control centers. Civilian objects that may fall into this dual-use category would include computer networks of certain research facilities, air traffic control networks that regulate both civilian and military aircraft, computerized civilian logistics systems upon which military supplies will be moved, electronic power grid control networks, communications nodes and systems, including satellite and other space-based systems, railroad and other transportation systems, civilian government networks, and oil and gas distribution systems.

Id. (citation omitted); *see also* Kelsey, *supra* note 7, at 1432 (describing the structure of the Internet); Rudesill, *supra* note 14, at 537 n.110 (noting the prevalence of dual-use infrastructure).

138. *See* sources cited *supra* note 136.

As this subpart discussed, offensive civilian engagement can be part of a defensive response to a cyberattack and in these cases is not per se bellicose. The next subpart examines purely offensive civilian engagement in cyberwarfare.

(b) Offensive Engagement

The need for purely offensive civilian engagement in cyberwarfare arises from the fact that civilians and military personnel rely on the same networks:

> In the United States . . . . the Internet provides nearly universal interconnectivity of computer networks without distinction between civilian and military uses. According to one count, "[a]pproximately '[ninety-five percent] of the telecommunications of the [Department of Defense] travel through the Public Switched Network,' and a significant amount of both the operation and maintenance of military-owned network segments is currently handled by civilians on a contracted-out basis."[139]

---

139. Kelsey, *supra* note 7, at 1432 (citation omitted). Richard Clarke, formerly the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, recently noted that because the United States

> is the most Internet-dependent and automated in terms of supply chain, banking, transportation-control systems and other modern facilities, it's also the most vulnerable to cyberattack. . . . And the military's dependence on the Internet also means it would be vulnerable to disruptions of it.
>
> "The U.S. military is no more capable of operating without the Internet than Amazon.com would be," Clarke says. "Logistics, command and control, fleet positioning—everything down to targeting—all rely on software and other Internet-related technologies."

Messmer, *supra* note 108 (quoting Richard Clarke); *see also* Solce, *supra* note 105, at 297 ("[N]inety-five percent of the United States military's information transfers, and ninety percent of large companies' information transfers, depend upon . . . civilian networks . . . ."(citation omitted)).

The U.S. military has its own networks. NIPRNET, which is not secure, and SIPRNET, which is secure. Joshua E. Kastenberg, *Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the NIPRNET*, 64 A.F. L. REV. 175, 183 (2009). The problem is that "information may be transferred to and from the NIPRNET to the [SIPRNET], as well as higher classified systems, placing the higher classification of SIPRNET and other access data at risk." *Id.*; *see also* Condron, *supra* note 117, at 407 ("[M]ilitary networks are . . . vulnerable because they depend extensively on civilian networks for connectivity and transferability of information."). The Department of Defense also heavily relies on commercial-off-the-shelf software, such as Microsoft products. Eric Talbot Jensen, *Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1160 (2003); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, DEFENSE ACQUISITIONS: KNOWLEDGE OF SOFTWARE SUPPLIERS NEEDED TO MANAGE RISKS, GAO Doc. No. 04–678, at 16–18 (2004) (discussing contractors' approaches to software security risks).

This quotation highlights the impossibility of segregating war-space and civilian-space in cyberwarfare.[140] More precisely, it underscores the impossibility of segregating combatants and noncombatants in cyberwarfare.

The LOAC predicates its approach to protecting civilians from the ravages of combat on segregating individuals by geography and by role.[141] Under the LOAC, military commanders must maintain a geographical separation between battle-space and the areas where civilians are located.[142] This is a viable strategy in the physical world, but not in the virtual one. As discussed, cyberspace is not a spatial phenomenon; it is an interactive overlay that eradicates the constraints of geography.[143] The notion of separating war-space and civilian-space becomes meaningless in a medium that has no boundaries and consequently no way to prevent the two "spaces" from coinciding and interacting.[144]

The LOAC's use of role segregation to protect civilians from combat becomes equally problematic. The interconnectedness of civilian and military networks means that "virtually all computer networks" can be legitimate military targets in cyberwar.[145] This

---

140. *See supra* Part II.B.2.

141. *See supra* Part II.A.

142. *See supra* Part II.A.

143. *See supra* notes 104–05 and accompanying text. As Barlow said, cyberspace "is a world that is both everywhere and nowhere." John Perry Barlow, *A Cyberspace Independence Declaration*, IBIBLIO.ORG (Feb. 8, 1996), http://www.ibiblio.org/netchange/hotstuff/barlow.html.

144. If the military used its own, dedicated systems, which civilians could not access, and if those systems were the (1) exclusive implements used to wage war, and (2) primary targets of hostile cyberattacks, a segregation of virtual war-space from virtual civilian-space would be possible. It would not be a spatial separation; it would be a functional segregation of war traffic and civilian traffic, but would probably fulfill the goals of the LOAC. The current intermingling of civilian and military traffic makes this scenario impossible. *See supra* note 139 and accompanying text.

145. Kelsey, *supra* note 7, at 1439 ("[T]he highly interconnected nature of the military and civilian networks . . . renders much of the Internet a dual-use target."); *see, e.g.*, Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1044 (2007).

> The law of war places on states a responsibility to separate . . . civilian populations and objects from . . . military objectives and dangers of military operations. When . . . infrastructures have a "dual-use" serving both civilian and military purposes . . . they qualify as military objectives subject to attack, even if their primary purpose is not military, but civilian. . . . The dual-use rule suggests . . . that U.S. adversaries may treat all U.S. communication systems as military objectives and attack them. . . .

Hollis, *supra*, at 1044 (citation omitted); *see also supra* note 137 and accompanying text. Two authors suggest it would "be difficult for the United States to argue that its telecommunications system, as a shared infrastructure, cannot be considered a military target when it could have developed parallel systems for purely military use." Gregory F. Intoccia & Joe Wesley Moore, *Communications Technology, Warfare, and the Law: Is the Network a Weapon System?*, 28 HOUS. J. INT'L L. 467, 486 n.63 (2006).

interconnectedness will make it difficult—if not impossible—to maintain the combatant–noncombatant distinction in cyberspace.

Part II.B.2.a considered how civilians may have to defend civilian-owned computer systems from cyberattacks launched by hostile states. This type of civilian involvement erodes the distinction between combatants and noncombatants because civilians defending "their" networks are in a position analogous to that of soldiers defending a fort or territory to which their country lays claim.[146] The scenarios are not, however, identical, as this type of civilian participation is distinguishable from that of military combatants because it is purely defensive.[147] Whether this defensiveness removes the participation from the "combatant" category is an open question.[148]

The previous subpart examined defensive civilian participation as if it were an isolated instance. If the attacks were part of a cyberwarfare campaign, they would not be an isolated event, but rather part of a larger, coordinated assault on systems throughout the United States.[149]

If U.S. computer systems become the targets of large-scale cyberwar attacks, the military probably will not want to leave the defense of those and other systems to the idiosyncratic efforts of autonomous civilians. The military will probably want to control and coordinate the responses—offensive as well as defensive—that are used to protect U.S. systems. The logical way to control the responses is to somehow control civilians who have the ability to battle cyberattackers. Bringing civilians into this effort would result in

---

146. *See supra* Part II.B.2.a.

147. *See supra* Part II.B.2.a. In other words, the civilians' goal is simply to repel or otherwise defeat the attack on their system. Unlike soldiers defending a fort, they are unlikely to launch offensive attacks on their attackers and on those affiliated with their attackers.

148. *See, e.g.*, Joshua E. Kastenberg, *Non-intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 62 (2009) ("Given that the U.S. private industry operates the majority of the Internet, there is concern as to whether the category of cyber combatant could be extended to include private civilians operating the Internet."). The type of civilian participation hypothesized in the text above might qualify defending civilians for prisoner-of-war status under Article 4(6) of the Geneva Convention (III). *See* Convention III, *supra* note 68. If they qualified for prisoner-of-war status, they would presumably be considered combatants under the LOAC. *See supra* Part II.B.2.a.

The Department of Defense believes research needs to be conducted to determine when an attack rises to the level of cyberwar and so transforms civilian defense of a system into military action. *See* WILSON, *supra* note 2, at 4–5.

149. *See, e.g.*, Letter from O. Sami Saydjari, Founder, Cyber Defense Research Ctr., et al., to President George W. Bush (Feb. 27, 2002), *available at* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/letter.html (outlining a large-scale, coordinated cyberterrorist attack). As many have noted, a cyberwarfare attack might initially be indistinguishable from a cybercrime or cyberterrorist attack. *See, e.g.*, BRENNER, CYBER THREATS, *supra* note 8, at 71–126 (discussing cyberattacks).

offensive civilian engagement in cyberwarfare and directly raise the issue as to whether those civilians would be considered combatants, because battling cyberattackers will involve the use of offensive as well as defensive measures.[150]

The conscription of civilians for offensive cyberwarfare would raise another issue. Consider U.S. telecommunications networks, which are owned and operated by civilians. These networks are the means by which hostile cyberattacks will be delivered to U.S. targets and by which offensive and defensive responses will be delivered to enemy targets.[151] That means that any cyberwarfare initiative must travel across civilian-owned networks.[152] What would happen if the network owners refuse to let them be used for that purpose?

The need to rely on civilian networks is not problematic as long as the companies that own the networks do not object to the networks being used in cyberwarfare. It is, however, quite possible that the network owners will not want their networks used as implements of war. Accordingly, they may object out of concern that their networks will be damaged in retaliative strikes because their multinational ties make them loath to take sides in a cyberconflict or for other reasons.

Part III discusses the question of how civilians should be incorporated into a cyberwarfare effort, and assumes that civilian participation is essential if the United States is to have a cyberwarfare capability but civilians will not willingly participate in such an effort. The second assumption is almost certainly overbroad because many civilians will be willing to play at least some role in cyberwarfare. Indeed, as the previous Part addressed, many civilians will have little hesitancy about protecting the systems with which they are affiliated.[153] It is also reasonable to assume, however, that some—perhaps many—civilians will not want to become involved in cyberwar for reasons already discussed. If nothing else, some may be concerned about losing their status as civilians: as noted above, a civilian who participates in cyberwarfare may be transformed into a combatant[154] and thereby become a legitimate target for enemy strikes. Part III addresses the two issues that this scenario creates: the first is the need to incorporate recalcitrant civilians into a

---

150. *See, e.g.*, Sanger et al., *supra* note 130. (noting that the United States is developing offensive cyberwarfare tactics); Shane Harris, *The Cyberwar Plan*, NAT'L J., Nov. 14, 2009, *available at* http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (same).

151. *See supra* Part II.B.2.

152. For a cyberwarfare scenario that notes the essential role of telecommunications providers, see, for example, Doug Hanchard, *Global Cyberwar: Installed in Your PC at Home, the Office and Government*, ZD NET (Oct. 21, 2009 5:32 AM), http://government.zdnet.com/?p=5601.

153. *See supra* Part II.

154. *See supra* Part II.B.2.a.

cyberwarfare effort, and the second is whether incorporation transforms a civilian into a combatant under the LOAC.[155]

III. CONSCRIPTS

> *[E]very member of society hath a right to be protected in the enjoyment of life, liberty, and property, and therefore is bound to . . . yield his personal service when necessary.*[156]

Governments have historically used either nationalization or conscription to integrate civilians into warfare.[157] If neither nationalization nor conscription can viably induce civilians to participate in cyberwarfare, then an alternative must be developed. The first two subparts below examine the efficacy of nationalization and conscription and assess the need for an alternative.[158] The third subpart postulates a third, more flexible option that incorporates aspects of conscription and nationalization.

A. *Nationalization*

> *[D]uring the period of war . . . Congress had duly authorized the taking over and operating of the railroads under the direction of the President . . . .*[159]

---

155. There is a residual possibility we do not address—that "U.S. forces . . . [will] retaliate [against a cyberattack] through unwitting computer hosts." WILSON, *supra* note 148, at 5. We do not specifically address this issue because we assume either (1) that the civilian host's ignorance of the fact it is being used as an implement of war absolves it of responsibility as a combatant, or (2) if the host's ignorance does not absolve it of responsibility, its participation will be encompassed by one of the theories we analyze in the next section. *See infra* Part III.

156. PA. CONST. of 1776, art. VIII.

157. A third method has arisen in the cyberwarfare context. Corporations that have historically worked in the defense industry are now providing contractors who perform various tasks in the United States' developing cyberwarfare capability. *See, e.g.*, *Raytheon to Provide Cybersecurity Across DoD Networks*, SPACE WAR (Nov. 17, 2009), http://www.spacewar.com/reports/Raytheon_To_Provide_Cybersecurity_Across_DoD_ Networks_999.html*; see also Cyber Warriors Wanted*, RAYTHEON, http://www.raytheon.com/ capabilities/products/cybersecurity/hiring/index.html (last visited Sept. 26, 2010) ("Raytheon is . . . hiring more cyber warriors to help fight the digital cyber war."). This Article does not address this method because while it raises legal issues of its own, it does not involve the need to compel unwilling civilians to participate in a cyberwarfare effort. *See infra* note 214.

158. Bringing civilians into a cyberwar effort may be but one aspect of what one source describes as a "growing general interpenetration between the civilian and military spheres." Tristan Leullier, *Dual Use Systems Shared by Civilian and Military Sectors*, EUROPOLITICS (Nov. 17, 2009), http://www.europolitics.info/sectorial-policies/dual-usesystems-and-platforms-shared-by-civilian-and-military-sectors-art254406-13.html.

159. Nueces Valley Town-Side Co. v. McAdoo, 257 F. 143, 143 (W.D. Tex. 1919).

Black's Law Dictionary defines nationalization as the "act of bringing an industry under government control."[160] The first instance of a U.S. president nationalizing civilian property for use in a war effort occurred during the Civil War when, "President Lincoln without statutory authority directed the seizure of rail and telegraph lines leading to Washington. Many months later, Congress recognized and confirmed the power of the President to seize railroads and telegraph lines and provided criminal penalties for interference with Government operation."[161] As a result, the issue of whether a President has the constitutional authority to nationalize private businesses did not arise.

The United States entered World War I on April 6, 1917. On December 26, President Wilson took over the nation's railroads, which were not up to the task of transporting military personnel and war supplies.[162] He gave control of the railroads to the Director

---

160. BLACK'S LAW DICTIONARY 1129 (9th ed. 2009).

161. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 685 (1952) (Vinson, C.J., dissenting) (citing Act of Jan. 31, 1862, ch. 15, 12 Stat. 334; 2 WAR OF THE REBELLION, OFFICIAL RECORDS OF THE UNION AND CONFEDERATE ARMIES, 603–04 (1880)).

> When the bill was before the Senate it was said by Senator Wade, of Ohio, that it was supposed that under the war power the Executive might seize this property without the authority of Congress, but it was thought better "that it should be done by authority of the law than by what may be considered by some as an usurpation."

Henry Hull, *Some Legal Aspects of Federal Control of Railways*, 31 HARV. L. REV. 860, 862 (1918). The statute authorized the President to "take over railroads and telegraph lines whenever the public safety required." *Id.* President Lincoln used the seizure to ensure that rail and telegraph companies "cooperate[d] with war needs." JAMES A. RAWLEY, ABRAHAM LINCOLN AND A NATION WORTH FIGHTING FOR 74–75 (2003). The statute also authorized the President to

> place under military control all the officers, agents and employees belonging to the telegraph and railroad lines . . . so that they shall be considered . . . a part of the military establishment of the United States, subject to all the restrictions imposed by the rules and articles of war.

12 Stat at 334. The World War I statute that allowed President Wilson to nationalize the railroads did not include "any similar provision for the regulation of employees." Francis Hoague, Russell M. Brown & Philip Marcus, *Wartime Conscription and Control of Labor*, 54 HARV. L. REV. 50, 52 n.5 (1940) (citing Act of Aug. 29, 1916, ch. 418, 39 Stat. 645)); *see infra* notes 206–12 and accompanying text.

162. RICHARD D. STONE, THE INTERSTATE COMMERCE COMMISSION AND THE RAILROAD INDUSTRY: A HISTORY OF REGULATORY POLICY 17–18 (1991); *see also* Virginian Ry. Co. v. Mullens, 271 U.S. 220, 224 (1926).

> War with Germany was declared April 6, 1917, and with Austria-Hungary December 7, 1917, and . . . Congress pledged all of the resources of the country to bring the conflict to a successful termination. 40 Stat. 1, 429. Under a proclamation declaring his purpose so to do (40 Stat. 1733 (Comp. St. 1918, Comp. St. Ann. Supp. 1919, s 1974a)), the President . . . assumed control, at

General of the newly created U.S. Railroad Administration, "severing the railroads 'completely' from the control and management of their civilian owners."[163]

Wilson cited three sources as authorization for his actions: powers conferred on him by the Constitution and "laws of the United States;" the joint resolution of Congress that declared war on Germany and Austria-Hungary; and legislation Congress adopted on August 29, 1916.[164] The 1916 legislation authorized the President,

> in time of war, . . . to take possession and assume control of any system or systems of transportation, or any part thereof, and to utilize the same, to the exclusion as far as may be necessary, of all other traffic thereon for the transfer or transportation of troops, war material and equipment, or for such other purposes connected with the emergency as may be needful or desirable.[165]

In 1918, Congress adopted the Federal Control Act, which ratified Wilson's actions.[166] Federal control of the railroads ended on March 1, 1920.[167]

The constitutionality of a President's seizure of civilian-owned businesses did not become an issue because Congress again ratified the President's actions.[168] The issue finally arose in 1952, however, when President Truman took over the steel industry to prevent a nationwide strike by steelworkers.[169] Truman characterized the seizure as necessary to continue the production of materials needed for the Korean War.[170]

> noon on December 28, 1917, of various systems of transportation . . . to the end that they might be . . . utilized in transporting troops, war material and equipment, and in performing other service in the national interest.

Virginian Ry. Co., 271 U.S. at 224.

For why the prior system was "inadequate to the task of serving the nation's war efforts," see *United States Railroad Administration*, WIKIPEDIA, http://en.wikipedia.org/wiki/United_States_Railroad_Administration (last visited Sept. 26, 2010).

163. Laura S. Fitzgerald, *Suspecting the States: Supreme Court Review of State-Court State-Law Judgments*, 101 MICH. L. REV. 80, 130 n.207 (2002); *see also* Missouri Pac. R.R. Co. v. Ault, 256 U.S. 554, 557 (1921) (describing presidential seizure of a railroad company).

164. Hull, *supra* note 162, at 860.

165. *Id.* (quoting Act of Aug. 29, 1916, Pub. L. No. 64–242, § 1, 39 Stat. 645 (1916)).

166. Federal Control Act of 1918, ch. 25, § 1, 40 Stat. 451, 451–52; *see also Missouri Pac. R.R. Co.*, 256 U.S. at 557 ("[President's] authority was confirmed by the Federal Control Act . . . and the ensuing proclamation of March 29, 1918, 40 Stat. 1763.").

167. Michael Shane Alfred, *Trying to Level the Playing Field: Management's Entitlement to Economic Damages Resulting from Illegal Labor Strikes*, 65 J. AIR L. & COM. 139, 150 (1999).

168. § 1, 40 Stat. at 451–52.

169. *See* Eric A. White, Note, *Examining Presidential Power Through the Rubric of Equity*, 108 MICH. L. REV. 113, 143 (2009) (describing the steel seizure).

170. *See id.*

The steel companies challenged his actions, ultimately taking the case to the Supreme Court.[171] Truman claimed the order was justified by his inherent authority as President of the United States and commander in chief of the armed forces of the United States.[172] The Court disagreed, explaining that the President's power to issue the order must derive either from an act of Congress or from the Constitution itself. The Court found that no statute authorized "the President to take possession of property as he did here."[173] The Court noted that "the seizure technique to solve labor disputes . . . to prevent work stoppages . . . [was] unauthorized by any congressional enactment," and Congress had previously rejected legislation that "would have authorized such governmental seizures in cases of emergency."[174]

The Court then considered whether the Constitution itself authorized the President to take over the steel companies.[175] Truman did not argue that "express constitutional language" granted him this power; instead, he claimed the power should be implied from the aggregate of his powers under the Constitution:[176]

> Particular reliance is placed on provisions in Article II which say that "the executive Power shall be vested in a President"; that "he shall take Care that the Laws be faithfully executed"; and that he "shall be Commander in Chief of the Army and Navy of the United States".
>
> The order cannot properly be sustained as an exercise of the President's military power as Commander in Chief . . . [W]e cannot

---

> On . . . April 8, Truman issued Executive Order 10340, in which he authorized the Secretary of Commerce to "take possession of all or such of the plants, facilities, and other property" of eighty steel manufacturers listed in the order. This action, the Executive Order stated, was necessary to ensure a "continuing . . . supply of steel," "an indispensable component" of our weaponry used in the Korean War.

Id. (citing Exec. Order No. 10,340, 17 Fed. Reg. 3139, 3141 (Apr. 10, 1952)).

171. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 583–84 (1952).

172. Exec. Order No. 10,340, 17 Fed. Reg. 3139, 3141 (Apr. 10, 1952). For an account of why President Truman believed he had such authority, see Alissa C. Wetzel, Note, *Beyond the Zone of Twilight: How Congress and the Court Can Minimize the Dangers and Maximize the Benefits of Executive Orders*, 42 VAL. U. L. REV. 385, 406 n.86 (2007). His belief in that regard may have also derived from the fact that in 1943 President Roosevelt used an executive order to take control of mines that were threatened with a shutdown due to strikes. *See* United States v. Pewee Coal Co., 341 U.S. 114, 115–16 (1951) (describing the seizure of the mines). The mine owners apparently did not challenge the President's authority for such a takeover of their property; they did, though, eventually bring an action seeking damages for a taking of private property under the Fifth Amendment. *See id.* at 115. The Supreme Court upheld a lower court's ruling that there had been a taking that entitled the mine owners to an award of damages from the government. *Id.* at 118–19.

173. *Youngstown*, 343 U.S. at 585–86.

174. *Id.* at 586.

175. *Id.* at 587.

176. *Id.*

> with faithfulness to our constitutional system hold that the Commander in Chief . . . has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production. This is a job for the Nation's lawmakers . . . .[177]

The Court also rejected the argument that the President's authority derived from "the several constitutional provisions that grant executive power to the President."[178] After noting that the "Constitution is neither silent nor equivocal about who shall make laws which the President is to execute," the Court held that Congress, not the President, makes the laws "which the President is to execute."[179] Therefore, the decision affirmed the district court's injunction against the implementation of the President's seizure order by the Secretary of Commerce.[180]

Given the Court's decision in this case, a contemporary president's ability to nationalize networks that carry Internet traffic seems to depend on the existence of legislation authorizing such action.[181] There is currently one statute that appears to confer such authority. Title 47 U.S.C. § 606 addresses the need to maintain wire and radio communications in wartime.[182] Title 47 U.S.C. § 606(a) applies when the United States is already at war, and it authorizes the President to order radio or wire communications carriers to give priority to national defense communications.[183] Furthermore, 47 U.S.C. § 606(d) specifically applies to "wire communication" facilities.[184] Under § 606(d), if the President proclaims that a state or threat of war involving the United States exists, he can authorize the

---

177. *Id.*

178. *Id.*

179. *Id.* at 587–88.

180. *Id.* at 589. The district court judge had held that Truman's actions were "without authority of law." Youngstown Sheet & Tube Co. v. Sawyer, 103 F. Supp. 569, 576 (D.D.C. 1952), *aff'd*, 343 U.S. 579 (1952).

181. *See Youngstown*, 343 U.S. at 587–88 (stating that the President's authority is dependent on Congressional authorization).

182. 47 U.S.C. § 606 (2006).

183. *See id.* § 606(a).

> During . . . a war in which the United States is engaged, the President is authorized, if he finds it necessary for the national defense and security, to direct that such communications as in his judgment may be essential to the national defense and security shall have preference or priority.

Id. Section 606(b) makes it a crime to "obstruct or retard" interstate or foreign communications by radio or wire. *Id.* Section 606(c) allows the President to suspend or amend the rules and regulations applicable to "stations or devices capable of emitting electromagnetic radiation" within the jurisdiction of the United States and to close or take control of any station "suitable for use as a navigational aid beyond five miles." *Id.*

184. *Id.* § 606(d).

closing of a wire communications facility or the use or control of such a facility by any department of the federal government.[185]

Whether § 606 authorizes the President to seize telecommunications networks in the event or threat of cyberwarfare depends on the resolution of two issues. The first issue is constitutionality: a statute must authorize a presidential seizure of private business for the seizure to be constitutional.[186] Section 606 seems to authorize such seizures, but for that authorization to be valid, § 606 must itself be constitutional. If § 606 is constitutional, the second issue arises: whether the statute actually allows for the seizure of telecommunications networks for use in cyberwarfare.

In 1919, the Supreme Court upheld the constitutionality of the original version of what is now 47 U.S.C. § 606.[187] On July 16, 1918, Congress adopted a joint resolution that provided:

> [D]uring the continuance of the present war [the President] is authorized . . . whenever he shall deem it necessary for the national security or defense, to supervise or to take possession and assume control of any telegraph, telephone, marine cable, or radio system or systems, or any part thereof, and to operate the same in such manner as may be needful or desirable for the duration of the war . . . .[188]

Six days later, President Wilson "exerted the power thus given" in a proclamation which cited the resolution. He declared that it was:

> 'necessary for the national security and defense to supervise and take possession and assume control of all telegraph and telephone systems and to operate the same in such manner as may be needful or desirable.
>
> 'Now, therefore, I, Woodrow Wilson, President of the United States, under and by virtue of the powers vested in me by the foregoing resolution, and by virtue of all other powers thereto me enabling, do hereby take possession and assume control and supervision of each and every telegraph and telephone system, and every part thereof, within the jurisdiction of the United States . . . .
>
> 'It is hereby directed that the supervision, possession, control, and operation of such telegraph and telephone systems hereby by me

---

185. *Id.* The President can close or take control of a wire communications facility for a "period ending not later than six months after the" state or threat of war ends "and not later than such earlier date as the Congress by concurrent resolution may designate." *Id.* The statute requires that "just compensation" be paid to the owners of any facility that is closed or used by the government. *See id.* Section 606(e) says the President "shall ascertain" the compensation to be paid, and establishes procedures which apply if the person entitled to compensation is not satisfied with the amount the President decides to pay.

186. *See supra* text accompanying notes 172–74.

187. Dakota Cent. Tel. Co. v. South Dakota *ex rel.* Payne, 250 U.S. 163, 181 (1919) (quoting J. Res., 65th Cong., c. 154, 40 Stat. 904 (1918)).

188. *Id.* The resolution required that the owners of the systems receive "just compensation" for the takeover with such compensation to be determined by the President. *Id.* The "form of the resolution was borrowed" from the 1916 Act that authorized the President to take over the railroads. *See The Telegraph Industry: Monopoly or Competition*, 51 YALE L.J. 629, 634–35 (1942).

> undertaken shall be exercised by and through the Postmaster General.'[189]

The Postmaster General "assumed possession and control" of the telephone systems and operated them until August 1, 1919, when the seizure ended.[190]

In January of 1919, the state of South Dakota sued the Dakota Central Telephone Company and other companies operating in the state to prevent them from implementing a rate schedule established by the Postmaster General.[191] The companies disclaimed responsibility for the rate schedule because they were operating under government control.[192] The case eventually reached the Supreme Court when South Dakota challenged the constitutionality of the takeover of the phone companies.[193] Upholding the takeover, the Court held that "under its war power Congress possessed the right to confer upon the President the authority which it gave him."[194] The Court also rejected South Dakota's argument that President Wilson exceeded the authority Congress conferred upon him; instead, the Court found that Congress's resolution gave the President the authority "to take complete possession and control" of the U.S. telephone system.[195]

Dakota Central Telephone Co. v. South Dakota ex rel. Payne suggests that § 606 is constitutional.[196] The following subpart will

---

189. *Dakota Cent. Tel. Co.*, 250 U.S. at 182. The President also directed that "'after twelve o'clock midnight on the 31st day of July, 1918, all telegraph and telephone systems included in this order and proclamation shall conclusively be deemed within the possession and control and under the supervision of said Postmaster General without further act or notice.'" *Id.* at 183.

190. *Id.* at 183. For how the Postmaster General operated the phone companies, see *The Telegraph Industry: Monopoly or Competition*, *supra* note 188, at 633–34.

191. *Dakota Cent. Tel. Co.*, 250 U.S. at 179–80.

192. *Id.* at 180–81.

193. *See id.* at 181 (describing the challenge to the law).

194. *Id.* at 183.

195. *Id.* at 184. South Dakota had argued that the resolution only authorized a partial takeover. *Id.* On another note, a state court rejected an argument that the takeover of the phone companies was an unconstitutional taking of property. Read v. Central Union Tel. Co., 213 Ill. App. 246, 256 (Ill. App. Ct. 1919). The Illinois court held that the seizure of the companies was not a taking without due process because (1) the resolution required the payment of just compensation for the property, and (2) the Constitution "expressly authorizes" Congress to make all laws which are necessary and proper for "carrying into execution the power to declare war, or to provide for the common defense." *Id.* at 256–58.

196. The only circumstance that might undermine its constitutionality is that the takeover of the phone companies was authorized by a Congressional resolution, rather than by legislation. The *Youngstown* Court referred to Congress's power to adopt the "laws" the President is to implement. *See supra* notes 171–77 and accompanying text. And President Wilson's seizure of the railroads was authorized by legislation Congress adopted two years earlier. *See supra* notes 164–65. After Wilson exercised that authority, Congress "promptly passed legislation providing in some detail" for the administration of the seizure. *The Telegraph Industry: Monopoly or*

address whether § 606 authorizes the seizure of telecommunications networks for use in cyberwarfare.

There are two issues that arguably undermine the applicability of § 606 in this context. The first is definitional: § 606 predicates the authority it confers on the existence of a state or threat of "war."[197] However, as discussed earlier, the question of whether cyberwar constitutes "war" under the current LOAC has yet to be resolved.[198] If, as seems likely, cyberwar does not constitute "war" under the LOAC, then the provisions of § 606 presumably do not apply to cyberwarfare.[199] The validity of that conclusion is inferentially supported by the fact that the resolution upon which § 606 is based was adopted to deal with kinetic war.[200] Therefore, it is reasonable to assume that, like its predecessors, the current version of § 606 only applies to kinetic war. The definitional issue could easily be resolved because Congress could revise the relevant provisions of § 606 to make it clear that they apply to cyberwar.[201]

The second, more intractable issue is whether a statute authorizing the President to nationalize telecommunications networks encompasses the type of takeover that would be necessary to deal with cyberwar. As noted above, nationalization consists of bringing an industry under government control.[202] It is often, but not always, a response to war.[203] Additionally, the United States has nationalized (and attempted to nationalize) businesses because they provided services or materials that were essential to the successful implementation of a war effort.[204] The common theme in nationalizations is that the government takes control of an industry

---

Competition, *supra* note 188, at 635 (citing Federal Control Act, ch. 25, § 1, 40 Stat. 451 (1918)). And when it adopted the resolution authorizing the seizure of the phone companies, "Congress apparently assumed that similar detailed legislation would be introduced in the event the President determined to exercise the authority granted," but for some reason "no further action was taken." *Id.* (citing 56 CONG. REC. 8729 (1918)).

197. *See supra* note 185 and accompanying text. Title 47 U.S.C. § 606(c), which deals with closing or taking over radio carriers, also applies in "a state of public peril or disaster or other national emergency." Section 606(a) and (d), only apply when there is a state or threat of war.

198. *See supra* notes 120–25 and accompanying text; *see also supra* Part II.A.

199. *See supra* notes 123–25 and accompanying text.

200. *See supra* note 188 and accompanying text.

201. Congress did something similar in 1951, in response to a different technology. *See* Act of Oct. 24, 1951, Pub. L. No. 82–200, 65 Stat. 611 (authorizing the President to "suspend and amend . . . the rules and regulations applicable" to devices emitting radio waves which may be used in navigation).

202. *See supra* note 160 and accompanying text.

203. *See, e.g.*, *Nationalization*, WIKIPEDIA, http://en.wikipedia.org/wiki/Nationalization (last visited Sept. 26, 2010).

204. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 587–88 (1952).

to ensure that it continues to perform its functions (sometimes with increased efficiency).[205]

More precisely, when a government nationalizes an industry, it does so to ensure that the industry continues to perform its *civilian* functions. When the U.S. government took over the railroads, it did so to improve the efficacy with which they carried out their customary functions, not to incorporate them into the military as combatants.[206] The same was true of the takeover of the phone companies: they continued to serve their civilian customers while they supported the war effort.[207]

Nationalization does not transform civilians into combatants. That function is reserved for conscription. As *Black's Law Dictionary* notes, conscription is the "compulsory enlistment of persons into military service."[208] Conscription transforms civilians into combatants;[209] nationalization brings civilians who are performing civilian functions under the control of the government, usually to ensure that the functions are performed in an effective manner and, often, to support a war effort.[210] In nationalization, civilians remain civilians.[211]

The nationalizations that have been implemented and attempted in the United States were all predicated on utilizing the industries for their respective civilian purposes.[212] Neither these precedents nor § 606 authorizes the seizure of civilian-owned facilities for the purpose of transforming them into instruments of war, which is what would be involved in nationalizing the telecommunications networks.[213]

If the President nationalized the networks that carry Internet traffic, he would not do so merely to ensure that they continued to function in their civilian capacity as communication facilities and

---

205. *See Nationalization*, *supra* note 203 (noting examples of nationalization).

206. *See supra* note 162 and accompanying text.

207. *See The Telegraph Industry: Monopoly or Competition*, *supra* note 188, at 634–36.

208. BLACK'S LAW DICTIONARY 567 (9th ed. 2009); *see also Conscription*, *in* THE COLUMBIA ENCYCLOPEDIA, *supra* note 30, at 631, 631. This Article addresses the issue of conscription in the next subpart.

209. *Conscription*, *supra* note 208.

210. *Nationalization*, *supra* note 203.

211. The legislation authorizing President Lincoln's nationalization of the telegraph and railroad companies made the employees of those companies "part of the military establishment" and subject to the laws of war. Hoague et al., *supra* note 161, at 52. It is not clear whether that provision was, in effect, a conscription measure, i.e., whether it formally inducted the employees into the military or simply put them under military control.

212. *See id.* at 52–53 (discussing nationalization of telegraphs, railroads, and mail carrier services).

213. *See id.*; 47 U.S.C. § 606 (2006) (authorizing the President to take control of communications carriers in times of war).

supported a cyberwarfare effort. He would nationalize the networks because civilian-owned networks create and sustain cyberspace, provide the means of access to the virtual battle-space, and carry the traffic used to implement offensive and defensive cyber-attacks.

Nationalizing telecommunications networks and using them to launch cyberwarfare attacks is the functional equivalent of nationalizing civilian air carriers, loading bombs onto a United Airlines 757, and sending it to attack a target in Afghanistan. In both scenarios, a civilian industry's role is transformed from performing purely civilian functions to actively participating in the conduct of hostilities. The status of the network owners and their employees therefore shifts from noncombatant to combatant.[214] Under the LOAC, this means that the networks become legitimate targets for retaliatory attacks by enemy states,[215] a result that was almost certainly not contemplated by the Congresses that approved the 1917 nationalization of the railroads or the takeover of communications facilities authorized by what is now § 606.

Therefore, the purposes for which the President would nationalize telecommunications networks in the event of cyberwarfare at least partially exceed the authority conferred by § 606. The President's authority to nationalize civilian property derives from statutes.[216] Because § 606 does not conclusively confer the authority to seize networks and utilize them as implements of war, that authority, if it exists, must lie elsewhere. No other federal statutes purport to confer such authority.[217] Congress could revise § 606 so that it explicitly confers the necessary authority, but this approach seems inadvisable given the extent to which the tactic being authorized exceeds the conceptual scope of nationalization.[218]

---

214. *See supra* notes 62–71 and accompanying text. Whether the owners of the telecommunications companies and their employees would be lawful or unlawful combatants would depend on how formally they were integrated into the military effort. *See supra* notes 62–71 and accompanying text.

215. *See, e.g.*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 195 (June 27) (stating that the right to retaliate against attack includes "not merely action by regular armed forces" but also encompasses attacks by mercenaries or irregulars that can be attributed to a nation-state); *see also* Hoisington, *supra* note 122, at 440 (explaining that national infrastructure is a potential target).

216. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 588–89 (1952).

217. *See* Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL L. REV. 57, 66–67 (1998) (noting that the authority to disrupt private communications is limited to the conditions listed in § 606).

218. Nationalization might also be overinclusive. When President Wilson nationalized the railroads, he did so to seize control of a domestic transportation industry that was not operating with the general efficiency required by the war effort. STONE, *supra* note 162, at 19. President Truman had a similar motive in his attempt to nationalize the steel companies; like President Wilson, he too wanted to ensure that a

The alternative is to use conscription. The next subpart considers whether conscription would be a viable way to give the U.S. military the ability to utilize telecommunications networks and other corporate resources in offensive or defensive cyberwarfare.[219]

B. *Conscription*

> *[Y]ou do not believe in the militarization of industry? . . . I do not . . . .*[220]

As noted earlier, conscription is the compulsory enlistment of civilians into the military.[221] It is a relatively recent development, because for much of history sovereigns relied on either voluntary enlistment or impressment to staff their armed forces.[222]

---

civilian industry continued to function (and, in the instance of the railroads, functioned with more efficiency) so it could support a war effort. White, *supra* note 169, at 143.

The scope of a cyberwarfare nationalization of telecommunications networks might be narrower than the nationalizations implemented and attempted by Presidents Wilson and Truman. The primary purpose in nationalizing the networks would probably be to ensure they would carry the signals needed to launch and repel cyberwar attacks. That purpose might not be inconsistent with the networks continuing to carry civilian traffic; indeed, the government would probably want to ensure that the use of the networks for cyberwar did not interfere with their use by civilians for civilian purposes, since so much of the U.S. infrastructure relies on communications and signals sent over the Internet. *See, e.g.*, President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (discussing the importance of the Internet in all aspects of American life). Nationalizing the networks could, therefore, be overkill.

219. The discussion in this section focused on telecommunications networks because they are the sole focus of 47 U.S.C. § 606. Telecommunications networks will be an essential—perhaps the essential—corporate resource governments will need to utilize in waging cyberwar. They will not, however, be the *only* corporate resources governments will rely on in cyberwarfare. As seen in Part II.B.2, almost any corporate entity can become a target in cyberwarfare, and this vulnerability requires defensive engagement. As further noted in Part II.B, the government is also likely to need to utilize the resources of other computer-related corporate entities in waging cyberwarfare.

220. SEYMOUR WALDMAN, DEATH AND PROFITS: A STUDY OF THE WAR POLICIES COMMISSION 8, 19, 47 (1932) (exchange between Congressman Collins and Bernard Baruch).

221. BLACK'S LAW DICTIONARY 567 (9th ed. 2009). "Conscription's raison d'être is to fill the ranks of military forces to fight war." FLYNN, *supra* note 81, at 25.

222. Casey B. Mulligan & Andrei Shleifer, *Conscription as Regulation,* 7 AM. L. & ECON. REV. 85, 88 (2005) (describing impressment as "the forced recruitment of individuals with little or no compensation or regulation of service terms or length"); *see also Impressment*, *in* THE COLUMBIA ENCYCLOPEDIA, *supra* note 30, at 1318, 1318.

> Before the establishment of conscription, many countries supplemented their . . . troops by impressment. In England, impressment began as early as the Anglo-Saxon period and was used extensively under Elizabeth I, Charles I, and Oliver Cromwell. "Press gangs" forcibly seized and carried individuals into

Conscription differs from impressment in that conscription is accomplished through induction rather than abduction. Conscription is the legal process by which civilians are formally incorporated into the military, usually for specific terms;[223] impressment is essentially state-sponsored kidnapping.[224]

1. History

Scholars trace the increased use of conscription to the rise of the nation-state and the democratization of warfare.[225] Conscription began to be used in Europe toward the end of the eighteenth century, and it became increasingly popular during the nineteenth century.[226] "By the time of World War I, only the United States and Great Britain did not rely on conscription for mobilization."[227]

Great Britain adopted conscription in 1916,[228] and the United States followed suit in 1917.[229] When President Wilson signed

---

service. . . . After 1800, England restricted impressment mostly to naval service. . . . England generally abandoned such forcible measures after 1835.

Impressment, *supra*, at 1318.

223. BLACK'S LAW DICTIONARY 567 (9th ed. 2009).

224. *See* BLACK'S LAW DICTIONARY 825 (9th ed. 2009) (defining impressment as "[t]he act of forcibly taking (something) for public service."). Conscription is essentially "the legal and regulated form of forced labor for the state." Mulligan & Shleifer, *supra* note 222, at 88; *see also* United States v. Johnson, 314 F. Supp. 88, 89 (D.N.H. 1970) (stating that due process requires conscription to be conducted "in strict compliance with the pertinent regulations").

225. *See, e.g.*, MICHAEL HOWARD, WAR IN EUROPEAN HISTORY 93 (2001) (war became a "conflict not of armies but of populations"); *see also id.* at 94–101 (describing the rise of conscription in Europe). Prior to this, at least in Europe, war was conducted by professional soldiers, mercenaries, or both, who were recruited "by impressment or bounty." *Id.* at 70; *see also id.* at 54–74 (discussing the impact of career professionals on war).

226. *Id.* at 80, 94–101; *see also* W. Hays Parks, *Air War and the Law of War*, 32 A.F. L. REV. 1, 123 n.378 (1990) (discussing the democratization of war). The modern version of conscription was created during the French Revolution. *See id.* (noting that conscription produced a national army); *see also* HOWARD, *supra* note 225, at 80–81 (describing conscription during that period).

227. Parks, *supra* note 226, at 123 n.378.

228. Rachel Vorspan, *Law and War: Individual Rights, Executive Authority, and Judicial Power in England During World War I*, 38 VAND. J. TRANSNAT'L L. 261, 285 (2005).

229. Arver v. United States, 245 U.S. 366, 375–76 (1918) (discussing Act of May 18, 1917, Pub. L. No. 12, 40 Stat. 76 (repealed), which established conscription). The Act subjected "all male citizens between the ages of twenty-one and thirty to duty in the national army for the period of the existing emergency." *Id.* at 375. Prior to the Act, U.S. armies were composed of volunteers; according to one author, the "armies of the Continental Congress consisted almost entirely of volunteers," as did the army that existed between 1812 and the Civil War. Jason Britt, *Unwilling Warriors: An Examination of the Power to Conscript in Peacetime*, 4 NW. J. L. & SOC. POL'Y 400, 402 (2009). Another author elaborates on this, noting that while the Continental Congress and the "states preferred volunteers," relying on them became problematic as the war

legislation implementing the draft, Joseph Arver and five other men refused to register and were charged with violating the new conscription law.[230] They defended themselves

> by denying that there had been conferred by the Constitution upon Congress the power to compel military service by a selective draft and if such power had been given by the Constitution to Congress, the terms of the particular act for various reasons caused it to be beyond the power and repugnant to the Constitution.[231]

The district court rejected their arguments and the defendants were convicted.[232] They appealed to the Supreme Court, which upheld the constitutionality of the conscription law.[233] The Court in *Aryer v. United States* noted, initially, that Congress's

> authority to enact the statute must be found in the clauses of the Constitution giving Congress power 'to declare war; to raise and support armies . . . [and] to make rules for the government and regulation of the land and naval forces.' Article 1, § 8. And . . . the

---

continued and "states were often forced to resort to conscription to meet their quotas" of soldiers. Scott E. Dunn, *The Military Selective Service Act's Exemption of Women: It Is Time to End It,* ARMY LAW, Apr. 2009, at 2. Those who were drafted could provide substitutes, "a practice that allowed for volunteers to be paid by private individuals rather than by" the states. *Id.* "President Madison proposed national conscription during the War of 1812, but his proposal was defeated in Congress." *Id.* at 3. As a result, in

> the period between the Revolutionary War and the Civil War, the needs of a small standing army were met with volunteers. Indeed, the practice of involuntary service had eroded to such an extent by the 1830s that Alexis de Tocqueville observed: "In America conscription is unknown and men are induced to enlist by bounties. The notions and habits of the people of the United States are so opposed to compulsory recruiting that I do not think it can ever be sanctioned by the laws."

Id. (quoting 1 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA (1835)). After the Confederacy seceded from the Union, it adopted a conscription law on April 16, 1862. *Id.* at 4. As a result, 21 percent of the Confederate soldiers were draftees. *Id.* The Union waited almost a year to follow suit. On March 3,1863, President Lincoln signed conscription legislation. *Union Army*, AM. CIVIL WAR, http://www.factasy.com/civil_war/union_regiment.shtml (last visited Sept. 26, 2010). The process of conscription was paid for by the states, who were reluctant "to resort to the coercion of the draft." Dunn, *supra*, at 4; *see also Union Army*, *supra* (discussing state administration of the draft). As a result, men who enlisted before they were drafted were paid a bounty from the federal government and "additional bounties from state and local government." *Union Army*, *supra*. States considered it a matter of pride to fill their quotas [of inductees] without having to resort to the draft." *Id.*

230. *Arver*, 245 U.S. at 366 ("Joseph F. Arver, Alfred F. Grahl, Otto Wangerin, Walter Wangerin, Louis Kramer, and Meyer Graubard were convicted of failing to present themselves for registration under the Act of May 18, 1917 . . . .").

231. *Id.* at 376.

232. *Id.* at 377.

233. *Id.* at 376–77.

> authority 'to make all laws which shall be necessary and proper for carrying into execution the foregoing powers.' Article 1, § 8.[234]

The Court also rejected the argument that although the Constitution gives Congress the power to raise armies, it did not "include the power to exact enforced military duty by the citizen."[235]

> It is argued . . . that . . . the authority to raise armies was intended to be limited to the right to call an army into existence counting alone upon the willingness of the citizen to do his duty . . . in time of war. . . . [T]his proposition is so devoid of foundation that it leaves not even a shadow of ground upon which to base the conclusion. . . . It may not be doubted that the very [c]onception of a just government and its duty to the citizen includes the reciprocal obligation of the citizen to render military service in case of need, and the right to compel it.[236]

Arver is the only case in which the Supreme Court has addressed Congress's power to impose conscription in wartime.[237] *Arver* upheld the power to conscript "in case of need."[238] Therefore, conscription is presumptively constitutional when the nation is at war or is facing a threat of war.[239]

2. Cyberwarfare

Whether conscription could be used to compel recalcitrant citizens to participate in cyberwar depends on the resolution of several issues. The first issue is whether cyberwar constitutes "war"

---

234. *Id.* at 377.

235. *Id.* at 377–78.

236. *Id.* at 378. The Court also rejected arguments that the legislation violated the Constitution by "vesting administrative officers with legislative discretion" and conflicting with Congress's power over the militia. *Id.* at 381–90. Finally, it held that conscription did not constitute "the imposition of involuntary servitude in violation of the . . . Thirteenth Amendment . . . ." *Id.* at 390.

237. *See* Britt, *supra* note 229, at 404–06 (noting that later challenges did not make it to the Supreme Court). Lower courts have considered, and rejected, various challenges to the constitutionality of conscription. *Id.* at 406–09.

238. The *Arver* Court noted that the conscription statute was intended to supply the "military force which was required by the existing emergency, the war then and now flagrant." 245 U.S. at 375. The statute was adopted on May 18, 1917, approximately one month after the United States entered the war. *See id.* at 375 (discussing the Act of May 18, 1917, Pub. L. No. 12, 40 Stat. 76 (repealed)).

239. The Supreme Court has never considered whether Congress has the power to impose conscription "during a time of peace." Britt, *supra* note 229, at 405; *see also* United States v. O'Brien, 391 U.S. 367, 389–90 (1968) (Douglas, J., dissenting) (noting the open question of whether conscription is constitutional absent a declaration of war); Hamilton v. Regents of the Univ. of California, 293 U.S. 245, 265 (1934) (Cardozo, J., concurring) (noting that this case was not a case of conscription during peacetime). Some lower federal courts upheld peacetime conscription, at least whenever Congress "declare[d] that it is necessary or that an emergency exists requiring the raising of an army." Richter v. United States, 181 F.2d 591, 592–93 (9th Cir. 1950). *But see* Britt, *supra* note 229, at 418–20 (noting arguments that peacetime conscription may not be constitutional).

for the purposes of applying Congress's power to institute conscription. As discussed, it is not at all clear that cyberwar constitutes war under the LOAC.[240] If it does not qualify as war, then Congress may not have the power to conscript civilians into a cyberwar effort.[241] The Court's decision in *Arver* was concerned with conscription when the United States was involved in a traditional, kinetic war, so it at least arguably does not apply to cyberwar.[242] The Supreme Court has never addressed the constitutionality of peacetime conscription,[243] and as a result, Congress might not have the constitutional authority to implement conscription when the United States is not engaged in kinetic warfare.[244]

There is authority for the proposition that "war" is not a unitary concept, meaning that varying states of war can exist.[245] One line of cases deals with undeclared war. For example, Congress implemented conscription during the Vietnam conflict without formally declaring war.[246] The Supreme Court did not address this

---

240. *See supra* Part II.B.2.

241. There is some authority for the proposition that Congress has the power to implement "civil conscription," i.e., conscript citizens to fulfill "any civil need of the state." *Civil Conscription in the United States*, 30 HARV. L. REV. 266, 266 (1917). Even if Congress has the power to implement peacetime conscription, that power might not extend to authorizing cyberwar conscription. The question would be whether the hypothesized peacetime conscription authority could encompass a cyberwar effort. In other words, the issue to be resolved would be whether cyberwar, which this Article assumes does not constitute "war" under the LOAC, qualifies as a peacetime activity. If Congress's authority to conscript encompasses only two states ("war" and "not-war"), then an argument can be made that Congress could conscript civilians to participate in a cyberwar effort on the premise that it is either "war" (in which case the war conscription power applies) or "not-war" (in which case the hypothesized peacetime conscription authority applies). If Congress does not have the power to implement peacetime conscription, the analysis is limited to the single issue addressed in the text above.

242. *See Arver*, 245 U.S. at 375 (noting that conscription was enacted for the purpose of fighting World War I).

243. Britt, *supra* note 229, at 405.

244. *Id.* at 419–20 (discussing the possible constitutional hurdles to a peacetime draft).

245. *Id.* at 414–17.

246. *See id.* at 401 n.7 (noting that joint resolution rather than declaration of war authorized combat involvement in Vietnam). There is also authority for the proposition that war can be "imperfect," i.e., less than total. In *Bas v. Tingy*, Justice Washington explained that hostilities can exist between

> two nations . . . being limited as to places, persons, and things; and this is more properly termed *imperfect war;* because . . . those who are authorised to commit hostilities, act under special authority, and can go no farther than to the extent of their commission. Still, ... [i]t is a war between the two nations, though all the members are not authorised to commit hostilities . . . .

4 U.S. (4 Dall.) 37, 40–41 (1800). This notion of imperfect war might apply to cyberwar because cyberwarfare almost certainly will not involve "all the members" of the warring nations or even all their armed forces. *See id.* at 40. It is more likely to involve hostilities conducted by a select few (military personnel and civilians) on each side, all

issue, but lower federal courts held that a state of war existed under Article I, Section Eight, Clause Eleven of the Constitution because Congress had adopted a resolution approving the use of force,[247] had ratified the President's initiatives by appropriating money "to carry out military operations in Southeast Asia," and by implementing conscription with the knowledge that conscripts would be "sent to Vietnam."[248]

These cases cannot resolve the status of cyberwarfare under the LOAC because they focused on the United States' failure to declare war, but the LOAC does not require declarations of war.[249] The Vietnam draft cases focused on the failure to declare war because they were primarily concerned with whether that struggle constituted war under the U.S. Constitution (rather than the LOAC).[250] The Vietnam draft cases could be used to argue that Congress can authorize conscription as part of a cyberwar effort if, as in the Vietnam conflict, Congress authorized or ratified the use of military forces in such an effort.[251] If this argument is valid, cyberwarfare conscription would presumably be lawful under U.S. law, though questions might remain as to the lawfulness of conscription under the LOAC.[252]

A second issue concerns the practical difficulties of conscripting civilians to participate in cyberwar. Conscription has traditionally involved the induction of civilians into the military; inductees report

---

of whom "act under [some type] of special authority." *See id.*; *see also, e.g.*, BRENNER, CYBER THREATS, *supra* note 8, at 1–6 (describing Estonia's response to 2007 cyberattacks); Nonie C. Cabana, *Cyber Attack Response: The Military in a Support Role,* AIR & SPACE POWER J. (Apr. 4, 2000), *available at* http://www.airpower.maxwell.af.mil/ airchronicles/cc/cabana.html.

247. *See* Britt, *supra* note 229, at 401 n.7, 407 (discussing courts' rejection of Thirtheenth Amendment challenges to the Vietnam Era draft despite the lack of a declaration of war).

248. Orlando v. Laird, 443 F.2d 1039, 1042 (2d Cir. 1971); *see also* Britt, *supra* note 229, at 415–16 (discussing whether conflicts like Vietnam are essentially war).

249. *Cf.* BRENNER, CYBER THREATS, *supra* note 8, at 63 (noting the insignificance of declarations of war since the end of World War II).

250. *See* Mitchell v. Laird, 488 F.2d 611, 615 (D.C. Cir. 1973) (discussing the ability of Congress to approve war other than by a formal declaration). The Vietnam Era and later cases parsing "war" have also relied on other factors. *E.g.*, United States v. Prosperi, 573 F. Supp. 2d 436, 449–55 (D. Mass. 2008) (considering factors including extent of authorization, war definitions under international law, scope of conflict, and diversion of resources). In some of the Vietnam cases, the plaintiffs relied on the law of war to assert a Nuremberg defense, i.e., that the war violated international law and they could be held individually liable if they submitted to the draft and fought in the war. *E.g.*, United States v. Valentine, 288 F. Supp. 957, 987 (D.P.R. 1968). Courts cited the political question doctrine as their basis for refusing to entertain the defense. *Id.* at 984–87.

251. Congress might also have to authorize funding for the cyberwarfare effort. *See supra* notes 246–48 and accompanying text.

252. If the conscription was not valid under the LOAC, then the conscripted civilians might not be entitled to the status of lawful combatant. *See supra* Part II.A.

for duty, are sworn in as members of the U.S. military, and from that point on are under military command.[253] They wear uniforms when on duty, usually live in military housing, and devote their time to military pursuits.[254] Induction, in other words, is absolute for the period for which the person is conscripted because during that period the inductee gives up his or her civilian life and becomes a soldier.[255] This system, however, would almost certainly not facilitate the conscription of civilians to participate as combatants in cyberwar.

The traditional model of induction would be counterproductive in a cyberwar conscription effort. Historically, conscription did not discriminate according to ability because its goal was to induct masses of men into the military, where they became the primary "engine of war."[256] Cyberwar conscription must be selective because its goal would be to compel civilians who have particular technical expertise and work for telecommunications and other Internet-related companies to participate in defensive or offensive cyberwar initiatives. The goal of cyberwar conscription is to *exploit* the status of civilians, not do away with their status altogether. Consequently, cyberwar conscription would resemble a kind of semi-conscription in which conscripts continue to perform their civilian duties but are also required to perform additional tasks when and as needed; the system would maintain the status quo of the conscripts' professional lives.[257]

---

253. *See, e.g.*, 53 AM. JUR. 2D *Military and Civil Defense* §§ 86–91, 160–61 (2010) (describing induction); *see also Becoming a Soldier*, GO ARMY, http://www.goarmy.com/soldier-life/becoming-a-soldier.html (last visited Sept. 26, 2010) (same).

254. *See Being A Soldier*, GO ARMY, http://www.goarmy.com/soldier-life/being-a-soldier.html (last visited Sept. 26, 2010) (describing various roles of army personnel).

255. This was also characteristic of the impressment of property under certain circumstances. During the Civil War, the Union adopted an impressment act that required the officer in charge of impressing property for Union Army use to assess "whether the absolute ownership, or the temporary use thereof, only" was needed. Yulee v. Canova, 11 Fla. 9, 1864 WL 1115, at *23 (Fla. 1864).

256. Audrey Kurth Cronin, *Cyber-Mobilization: The New Levee en Masse*, 36 PARAMETERS 77, 77–79 (2006). This was a function of the democratization of warfare. As war became a struggle between nations, it required larger armies. *See* HOWARD, *supra* note 225, at 93 (war became "a conflict not of armies, but of populations"); *see also* RICHARD A. PRESTON ET AL., MEN IN ARMS: A HISTORY OF WARFARE AND ITS INTERRELATIONSHIPS WITH WESTERN SOCIETY 188–89 (1956) (Napoleon's victories were "due to the mass armies" that the Revolution produced).

257. Functionally, their position would to some extent be analogous to that of members of the U.S. Air Force who pilot unmanned predator drones. Many Air Force drone pilots live and work in the United States; they spend their days flying drones in combat in Iraq or Afghanistan and then go home to "church activities, . . . soccer practices, et cetera." P.W. SINGER, WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE TWENTY-FIRST CENTURY 345–46 (2009). The more apt analogy may lie in comparing the cyberwar conscripts hypothesized above and the civilian contractors who also fly drones in Iraq, Afghanistan, and other places. *See id.* at 371–72. Like the cyberwar conscripts hypothesized above, the contractors who operate drones in combat are civilians who participate in military combat. *Id.* And as Singer notes, there are concerns that these contractors can be considered illegal combatants under the LOAC.

These additional tasks would probably be cyberwar-specific, but the conscripts' routine tasks might also be cyberwar related, at least in part.[258]

This type of semi-conscription generates a host of legal issues. The first is constitutionality, and constitutionality would likely depend on the legal status of the semi-conscripts. If they are formally inducted into a branch of the military, their status would resemble that of traditional conscripts, and the conscription could be justified as a variation of a type of conscription that the Supreme Court has already ruled constitutional.[259] If the semi-conscripts are not formally inducted into the military and are merely put under military control for certain purposes, their status would not be at all analogous to that of traditional inductees and could raise difficult questions about the propriety of infringing on the liberty of civilians.[260]

This raises the issue of whether Congress can conscript civilians for purposes other than directly serving in the armed forces.[261]

See id. at 372; *see also supra* Part II.A; *see generally* Daniel P. Ridlon, *Contractors or Illegal Combatants? The Status of Armed Contractors in Iraq*, 62 A.F. L. REV. 199 (2008).

258. According to various sources, the People's Liberation Army (PLA) of China is implementing joint military–civilian units that are capable of—and may already be—launching cyberwar attacks on other nations. *E.g.*, BRYAN KREKEL, THE US-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, REPORT ON THE CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION 33 (2009), *available at* http://www.cfr.org/publication/21054/capability_of_the_peoples_republic_of_china_to_conduct_cyber_warfare_and_computer_network_exploitation.html ("PLA [is] creating [cyberwar] militia units comprised of personnel from the commercial IT sector and academia" that represent "an operational nexus" between the PLA "and Chinese civilian information security . . . professionals."); *see also id.* at 7, 37 (discussing the Chinese hacker community). The U.S. military is relying heavily on civilian contractors in its preparations for cyberwar. *See, e.g.*, Christopher Drew & John Markoff, *Contractors Vie for Plum Work, Hacking for U.S.*, N.Y. TIMES, May 31, 2009, at A1.

259. *E.g.*, United States *ex rel.* Zucker v. Osborne, 54 F. Supp. 984, 986–88 (W.D.N.Y. 1944).

260. If Congress has the authority to implement peacetime conscription, this scenario might be justified as a valid exercise of that authority. *See supra* notes 237–39 and accompanying text. Courts have held that military conscription does not constitute an unconstitutional violation of an individual's liberty or other interests. *See, e.g.*, *Osborne*, 54 F. Supp. at 986–87. A few courts have held that peacetime military conscription does not impose an unconstitutional deprivation of liberty. *E.g.*, Etcheverry v. United States, 320 F.2d 873, 874 (9th Cir. 1963).

261. There are cases that have upheld Congress's "power to conscript individuals for work of national importance . . . in time of war." *Osborne*, 54 F. Supp. at 986. These conscientious objector cases are not, however, relevant to the point currently under consideration because they address compelling individuals "to serve in useful civilian work in lieu of active military service." United States v. Bartell, 144 F. Supp. 793, 797 (S.D.N.Y. 1956). In contrast, the concern of this Article is with compelling civilians (or quasi-civilians) to support active military initiatives or to engage in those initiatives themselves.

During the Revolutionary War, Congress authorized the Continental Army to conscript services from civilians.[262] This seems to have been the only time in U.S. history that civilians as civilians were subject to a type of military conscription.[263] In the early 1920s, bills were introduced into Congress that would have authorized "a draft of labor."[264] Later, other bills were introduced that would have authorized a "draft of 'services'" or a "draft of persons in the management or control of industry," but the proposed legislation was never adopted.[265] Since this seems to have been the only attempt to authorize the conscription of civilian services, there is apparently no authority that directly addresses Congress's power to conscript civilians for purposes other than serving in the armed forces.[266]

---

262. E. JAMES FERGUSON, THE POWER OF THE PURSE: A HISTORY OF AMERICAN PUBLIC FINANCE, 1776–1790, at 58–69 (1962) ("Congress authorized Washington to impress goods and services"; later, Congress encouraged the states to authorize conscription of goods and services.). This system was more a process of impressment than conscription because its execution was purely ad hoc, i.e., services were conscripted when and to the extent that particular officers needed them. *Id*. at 58–59. It differed from both impressment and conscription in one notable respect—when officers conscripted services, they paid for them or, if they did not have the cash to pay for them, gave those providing the services "certificates." *See id*. at 59 (noting that certificates could also be used if the owners refused to sell their goods to the military at the legislated price). The certificates were "essentially IOUs," and left Congress with massive debts after the war ended. J. Gregory Sidak, *The President's Power of the Purse,* 1989 DUKE L.J. 1162, 1167 n.18 (1989); *see* FERGUSON, *supra*, *at* 59–66 (describing the financial impact of the certificate program).

The "arbitrary and oppressive" use of impressment during the Revolutionary War contributed to the adoption of the Compensation Clause of the Fifth Amendment, which developed into modern "takings" law. Jed Rubenfeld, *Usings*, 102 YALE L.J. 1077, 1122–33 (1992); *see also* Matthew P. Harrington, *Regulatory Takings and the Original Understanding of the Takings Clause*, 45 WM. & MARY L. REV. 2053, 2067 (2003) (explaining that the Compensation Clause was more about impressment than about land use regulation). It seems to follow that conscripting the services of a corporation (along with its property) would constitute a taking under the Fifth Amendment. *See* Yulee v. Canova, 11 Fla. 9, 1864 WL 1115, at *24 (Fla. 1864).

263. In *Butler v. Perry*, the Supreme Court held that states could conscript civilians to work on roads and bridges in the county where they lived. 240 U.S. 328, 333 (1916). The Court held that conscripting Butler to work on roads in his Florida county neither deprived him of liberty without due process of law nor constituted involuntary servitude in violation of the Thirteenth Amendment. *Id.* at 332–33. While the *Butler* case upheld the conscription of labor, it is irrelevant to the issue under consideration because it did not involve conscription for the purpose of participating in or supporting military initiatives. In other words, it did not address the issue of whether Congress can conscript civilians, as civilians, to participate in war efforts.

264. Hoague et al., *supra* note 161, at 61–62.

265. *Id*. at 62–63. The bills all contemplated conscription during a time of war. *Id.* They were part of an attempt to implement a "[u]niversal [d]raft" of all "resources, industrial organizations and services over which Government control is necessary" for the "successful termination" of a state of war. WALDMAN, *supra* note 220, at 5 (internal quotation marks omitted). The primary purpose seems to have been to "take the profit out of war." *Id.* (internal quotation marks omitted).

266. *See Butler*, 240 U.S. at 333 (stating that the purpose of the Fourteenth Amendment was not to deprive the government of its essential powers). It might be

The obvious alternative is to induct employees of the companies whose support is deemed essential to a cyberwar effort into a branch of the U.S. armed forces.[267] This would not only resolve the conscription issue, but would also resolve issues that might arise as to whether civilians (or semi-civilians) can be compelled to take orders from military officers.[268] If the employees are inducted into

---

possible to derive the existence of such authority from Congress's power to "raise . . . Armies," but the viability of such a strategy would depend on whether the concept of "Armies" could be extrapolated to encompass civilians (or quasi-civilians) who were being compelled to support the efforts of members of the armed forces and, at least on occasion, to act as surrogate members of the armed forces. U.S. CONST. art. I, § 8, cl. 12. For the purposes of this analysis, this Article assumes such an extrapolation is not viable, and will, therefore, use other means to justify conscripting civilians into a cyberwarfare effort.

When the issue of conscripting labor was debated in the 1920s, some argued that Congress has the power to conscript civilians to serve in a support role during wartime:

> There would seem to be little doubt . . . that since Congress may compel one man to participate in armed conflict in war-time it may compel another to supply the instruments necessary to help carry out its declaration of war. . . .
>
> . . . . [Congress has] the power to conscript labor. . . . [w]hether it chooses to . . . execute it is another matter.

WALDMAN, *supra* note 220, at 62. The Selective Service Act of 1940, Pub. L. No. 76–783, 54 Stat. 885, gave the government the authority to "commandeer plants" under certain circumstances. *Executive Commandeering of Strike-Bound Plants*, 51 YALE L.J. 282, 285 (1941). According to one source, this provision was included "because of popular demand to provide for the 'conscription of capital' to balance the power to [conscript] men for military service." R. ELBERTON SMITH, THE ARMY AND ECONOMIC MOBILIZATION 514 n.25 (Kent Roberts Greenfield ed. 1959). "Section 9 of the Selective Service Act of 1940 . . . permitted seizure of manufacturing facilities . . . [if] the owners refused to give preference to Government orders or to accept them at reasonable prices as determined by executive officers." *Executive Commandeering of Strike-Bound Plants*, *supra*, at 285. Though this and other sources refer to the authority granted by § 9 of the Selective Service Act as the power to "commandeer" companies, the provision seems to have authorized the President to nationalize companies.

Congress must have realized that "commandeering" companies constituted a taking under the Fifth Amendment because § 9 of the Selective Service Act of 1940 "provides that rentals for commandeered plants shall be 'just and fair.'" *Judicial Control of Profits on Government Wartime Contracts*, 51 YALE L.J. 855, 862 n.33 (1941) (citing § 9, 54 Stat. at 892).

267. This would also address another issue. The kind of semi-conscription of the employees postulated earlier might not be effective because their employers might resist losing control of their workers. If that occurred, the owners of the companies might try to frustrate the semi-conscripts' ability to participate in cyberwarfare by assigning them to tasks that would not be relevant to cybercombat (or even discharging them).

268. This might not become an issue. Title 10 U.S.C. § 802(a)(10) (2006) subjects civilians "serving with or accompanying an armed force in the field" to the Uniform Code of Military Justice if their service occurs during a "declared war or a contingency operation." According to one source, this provision "subjects these civilians to every punitive article in the UCMJ, including . . . disrespect toward superiors, disobedience of orders, absence without official leave, and desertion." Geoffrey S. Corn, *Bringing Discipline to the Civilianization of the Battlefield: A Proposal for a More Legitimate Approach to Resurrecting Military-Criminal Jurisdiction over Civilian Augmentees*, 62

the military, they become members of the armed forces and are clearly obligated to obey the commands of superior officers.[269]

Although this option has an appealing simplicity, it raises other issues. One issue is whether those who have become members of the U.S. military can continue to work for a civilian-owned company. If civilians are inducted into the military whose talents and assistance are needed in a cyberwar effort, are they still employees of the companies that control the telecommunications networks and other strategically relevant Internet businesses, or are their civilian and military responsibilities mutually exclusive? As discussed earlier, induction has always been total, as an inductee's status shifts from being a civilian to being a member of the armed forces.[270] A version of this change in status could be incorporated by inducting these employees into a branch of the armed forces and having them continue to perform their old job but be paid by the military.[271] That solution, however, creates other problems because an employer might resist having its workforce, or a substantial part of its workforce, operating under the aegis of the military. This solution might also create conflicting chains of command if the civilian management of a company and the military officers assigned to the company vie for control over the workforce.[272]

U. MIAMI L. REV. 491, 497 (2008) (citation omitted). A "contingency operation" is a "military operation" that (1) has been "designated by the Secretary of Defense as an operation in which members of the armed forces" may become involved in hostilities with "an opposing military force," and (2) "results in the call or order to, or retention on," members of the armed services. 10 U.S.C. § 101(a)(13) (2006).

269. 10 U.S.C. § 802(a)(1); *see id.* § 892 (declaring any person subject to the title who does not obey orders as subject to punishment by court-martial).

270. *See supra* Part III.B.2.

271. The military apparently lets members of the armed forces work part time in civilian positions if they have permission from their superior officer. *See, e.g.*, Miller v. United States, 643 F.2d 481, 482 (8th Cir. 1981) (describing a soldier's part-time construction job). It might, therefore, be possible to approach the scenario outlined in the text as a situation in which members of the armed forces are working in civilian positions with the approval of their superiors.

These issues could perhaps be resolved by implementing a variation of the dual-status employment that already exists in the federal system: "Air Reserve Technician[s] (ART). . . . are full-time civilian employees who are also members of the Air Force Reserve . . . ." Jeffries v. Dep't of the Air Force, 999 F.2d 529, 530 (Fed. Cir. 1993). Although ARTs are civilian employees, they are employed by the federal government and the dual-status position is the result of an "agreement between the military agency and the Office of Personnel Management . . . ." *Id.* at 529–30. Membership in the military is essentially a qualification for the civilian position. *Id.* at 530. The civilian and military roles are, therefore, unlikely to come into conflict.

272. An article discussing the process of operating companies "commandeered" during World War II noted that "the top men" in the company, who might not be cooperative, could be "displaced." *American Economic Mobilization: A Study in the Mechanism of War*, 55 HARV. L. REV. 427, 525 (1942) [hereinafter *American Economic Mobilization*].

That raises a related issue: precisely who or what would need to be conscripted in a cyberwar effort? As the scenario outlined above illustrates, cyberwar conscription would involve conscripting a company as well as the individuals who work for that company. The corporation that owns the telecommunication or other Internet-related business whose employees become cyberwar conscripts would still own the business, but conscription would limit its ability to control the company's day-to-day operations. Furthermore, the corporation could not prevent the company's employees and assets from being used in cybercombat.

The above analysis assumes that conscription would only target employees. In practice, however, conscription would necessarily encompass the equipment and other assets the employees would need to launch and repel cyberattacks. In sum, the actual scope of conscription would be much broader because entire companies would have to be conscripted. The telecommunications networks and other Internet-related businesses whose staff and assets will be essential in a cyberwarfare effort are generally owned by corporations.[273] The law treats corporations as persons.[274] Consequently, corporations have been encouraged to "assume the modern obligations of good citizenship,"[275] such as paying taxes and abiding by all applicable laws. The doctrine of conscription can be extrapolated to encompass

---

273. *See* Richard Clarke, *Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks,* 12 DEPAUL BUS. L.J. 33, 36–39 (1999/2000) (noting the importance of cooperation between the government and private entities in protecting infrastructure from cyberattacks).

274. *See* Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876, 899 (2010) (noting that First Amendment protection extends to corporations); Tara J. Radin, *700 Families to Feed: The Challenge of Corporate Citizenship*, 36 VAND. J. TRANSNAT'L L. 619, 653 (2003).

> [C]ourts have extended protection to corporations for behavior encompassed by the 1st, 4th, 5th, and 14th Amendments. The due process rights of corporations have been protected, as have been their rights to freedom from illegal searches and seizures. In addition, courts have determined that corporations have citizenship, even though they are not biological individuals.

Radin, *supra*, at 653 (citation omitted); *see also* Woodrow Barfield, *Intellectual Property Rights in Virtual Environments: Considering the Rights of Owners, Programmers and Virtual Avatars*, 39 AKRON L. REV. 649, 656 n.64 (2006).

> A legal person . . . enjoys many of the rights and obligations of individual citizens, such as the ability to own property, sign binding contracts, and pay taxes; but they do not retain all the rights of a natural person, e.g., they do not have the right to vote or hold public office.

Barfield, *supra*, at 656 n.64; *see generally* Carl J. Mayer, *Personalizing the Impersonal: Corporations and the Bill of Rights*, 41 HASTINGS L.J. 577 (1989) (discussing how the Bill of Rights applies to corporations).

275. A.P. Smith Mfr. Co. v. Barlow, 98 A.2d 581, 586 (N.J. 1953).

corporate entities because the law recognizes corporations as citizens that share many of the duties and obligations of citizenship.[276]

The possibility of such an extrapolation raises the question of what corporate conscription would encompass and how it would differ from nationalization. In other words, if corporate conscription can be implemented, then one must consider how and why it might be implemented. Although a corporation is a "person," it would not be sufficient to simply conscript the corporate entity itself. Conscripting the corporate entity would give the military control of the company's assets and capabilities. In that regard, it would be analogous to conscripting individuals, each of whom has expertise that is essential to a cyberwar effort. Conscripting the corporation's assets and capabilities would not suffice because the government would still need to compel the participation of the employees who have the expertise to carry out cyberwar activities. Therefore, the government would need to conscript the corporation and the corporation's employees.[277] The corporation would continue to carry out its civilian functions but would on occasion be obliged to participate in cyberwar operations.

This Article now addresses why the United States might want to implement corporate conscription. First, corporate conscription should resolve conflicting chain of command issues by conscripting the corporation's management as well as its staff.[278] If the government conscripts managers and executives, they too would be required to obey orders given by the military personnel who take charge of the company, and this obedience should discourage (if not eliminate) the possibility of conflicting directives from corporate management. Second, conscripting the corporation puts it under military control and transforms it, in part, into an implement of war, and this transformation should make it possible for the military to use the corporate conscripts effectively in cyberwar activities.

The conscription of corporations has disadvantages, as well. First, to facilitate the efficient command of employees when necessary, military personnel would presumably either assume control of the corporation or have the ability to assume such control

---

276. *See supra* note 274 and accompanying text.

277. Some might argue that it would only be necessary to conscript the employees who have the skills needed to launch and repel cyberattacks, but the employees who can engage in cyberwar would not be able to do so unless the other employees (whose efforts are essential to corporation's function) were in place performing their own support tasks. Conscripting all (or most) of the company's employees is essential if the company is to continue providing services to the general public, which would be particularly important with regard to telecommunications companies. *See American Economic Mobilization*, supra note 272, at 525–30 (discussing the operation and employee status of companies commandeered by the government).

278. *See supra* note 268 and accompanying text.

on very short notice.[279] In either event, military control could interfere with the corporation's ability to carry out its civilian functions effectively, thereby creating a takings issue.[280] Conscription could also transform the corporation into a "combatant" under the LOAC, making it a legitimate target for retaliatory attacks by an enemy.[281] This could create a new takings issue or exacerbate the effects of the original issue.[282]

Corporate conscription certainly has other advantages and disadvantages, and other implementation issues would have to be resolved. The goal of this Article is not to attempt to identify and analyze every issue raised by conscripting corporations to participate in cyberwarfare, but rather to analyze the permissibility and utility of utilizing corporate conscription as an alternative to nationalization. That discrete goal is, of course, part of determining if nationalization or conscription is a satisfactory way of compelling civilian participation in cyberwarfare. The next subpart assesses their respective suitability for this task and the potential need for another alternative.

C. *A Third Option*

As discussed in the previous two subparts, neither nationalization nor conscription is likely to be particularly effective in compelling the cooperation of civilians—especially companies and their employees—in cyberwar offense and defense. They suffer from reciprocal deficiencies: nationalization gives the government the

---

279. In "commandeering" companies under the Selective Service Act of 1940, Pub. L. No. 76–783, 54 Stat. 885, the government had available "three tested methods of operation of the expropriated industry: operation through a regular government department, a private corporation which enters into a managerial contract with the Government, or a government-owned corporation." *American Economic Mobilization, supra* note 272, at 513, 525–26 (citation omitted). President Wilson relied on the first and third of these methods; he put the nationalized telephone and telegraph systems under the control of the Postmaster General, and the railroads under the control of the Director General of the new United States Railroad Administration. *See supra* text accompanying notes 163, 189. These methods are appropriate when companies are nationalized (or commandeered) because the companies continue to perform their civilian functions; they are not transformed, in whole or in part, into military combatants. Since the purpose of taking over telecommunications networks and other companies is to utilize their capabilities directly in cybercombat, the seizure should be implemented by the military.

280. *See* United States v. Pewee Coal Co., 341 U.S. 114, 117–19 (1951) (holding that the government became liable to pay just compensation to owners of a seized mine).

281. *See* SINGER, *supra* note 257, at 373 (noting that civilian contractors may be considered illegal combatants under the LOAC).

282. *See Nationalization*, *supra* note 203. For a discussion of how the takings issue was handled with regard to the plants commandeered during World War II, see *American Economic Mobilization*, *supra* note 272, at 530–35.

ability to take over and operate companies as part of a war effort, but the government is limited to operating the companies in their civilian capacity.[283] Nationalization does not authorize the government to transform businesses into implements of war or, perhaps more accurately, into combatants.[284]

Conscription gives the government the ability to transform civilians into members of the armed forces.[285] It is not clear if the government's power to conscript civilians encompasses corporations; even if it does, implementing conscription becomes problematic for the reasons discussed in the previous subpart. First, how can the government conscript the corporation for cyberwarfare while preserving the corporation's civilian functions? Second, what is the scope of corporate conscription? If the government conscripts a corporation, are the corporation's employees conscripted as well?

All of these issues can be resolved. One solution is to fuse nationalization and conscription. Under this approach, the government takes control of corporate entities with functions essential to protect the country from cyberattacks. Government personnel take charge of the corporation but leave the administration of routine, "civilian" tasks to the company's civilian management. In other words, government personnel assume operational control of a corporation only when necessary and only to the extent necessary to utilize the corporation's employees and facilities in responding to (or initiating) cyberattacks. Although this approach lacks empirical precedent, it is probably a viable option, at least as a matter of law. Congress has the authority to implement conscription and nationalization, and a model that fuses the doctrines should survive constitutional challenges.[286]

Therefore, the objection to this model lies not in law but in practice. As a practical matter, while this model may seem to represent a type of nationalization, it essentially involves the conscription of a corporate entity because the paramount goal is not to take over the entity to ensure that it performs its civilian functions consistently and, perhaps, more efficiently than it would otherwise. Instead, the paramount goal is to ensure that the government will be

---

283. *Nationalization*, BRITANNICA ENCYCLOPEDIA ONLINE, http://www.britannica.com/EBchecked/topic/405796/nationalization (last visited Sept. 26, 2010) (describing nationalization projects in several countries, including takeovers of the banking industry in communist Russia and the oil industry in Mexico—these industries continued to operate in their official capacities, but were owned by the government post-nationalization).

284. *See id.* (describing various nationalization efforts in which the government took over operations of a formerly private industry).

285. *Conscription*, BRITANNICA ENCYCLOPEDIA ONLINE, http://www.britannica.com/EBchecked/topic/133307/conscription (last visited Sept. 26, 2010) (defining conscription as "compulsory enrollment for services in a country's armed forces").

286. *See* discussion *supra* Parts III.A, III.B.1.

able to utilize the entity as a weapon, i.e., as part of a cyberwarfare response effort. The model incorporates the objective of nationalization, but it is subsidiary to the primary goal of integrating the corporate entity into a cyberwarfare effort.

In the prior model, conscription eclipses nationalization, and the asymmetrical importance of conscription suggests a model that resembles the National Guard—a customized, Cyberwar National Guard (CNG).[287] Structurally and operationally, the CNG more closely resembles the common law militia than the contemporary National Guard. Unlike the contemporary National Guard, which operates according to formal procedures that are analogous to those employed by the U.S. military, the proposed CNG (or Cyber Militia) operates on a more ad hoc basis. For example, it would not be feasible to call members of the CNG into service for specific periods of time and give them notice as to when they were to report for duty. Instead, like the common law militias, members would have to be

---

287. The new organization could instead be called the Cyber Militia, because its structure and function closely resembles the common law militia. As the Illinois Supreme Court explained:

> Lexicographers and others define militia, and so the common understanding is, to be "a body of armed citizens trained to military duty, who may be called out in certain cases, but may not be kept on service like standing armies, in time of peace." That is the case as to the active militia of this State. The men comprising it come from the body of the militia, and when not engaged at stated periods in drilling and other exercises, they return to their usual avocations, as is usual with militia, and are subject to call when the public exigencies demand it.

Dunne v. People, 94 Ill. 120, 138 (Ill. 1879). In *Perpich v. Dep't of Defense*, the Supreme Court noted that modern National Guard members "continue to satisfy this description of a militia" because they have both a "civilian hat" and "an army hat—only one of which is worn at any particular time." 496 U.S. 334, 348 (1990).

The proposed Cyber National Guard would be distinct from the U.S. Air Force's Cyber Command and a similar unit proposed by the U.S. Army. *See* Michael Cheek, *Air Force Cyber Command to Go Operational*, THE NEW NEW INTERNET (Jan. 27, 2010, 1:31 PM), http://www.thenewnewinternet.com/2010/01/27/air-force-cyber-command-to-go-operational/ (describing Air Force cyber unit); Amber Corrin, *Army Mulls Realignment to Fortify Cybercommand*, FED. COMPUTER WK. (Jan. 15, 2010), http://fcw.com/Articles/2010/01/15/Army-mulls-realignment-to-fortify-cyber-command.aspx (describing Army cyber unit); *see also* Bob Brewin, *Here Comes the Navy Cyber Forces*, NEXTGOV (Jan. 11, 2010, 4:46 PM), http://whatsbrewin.nextgov.com/2010/01/here_comes_the_navy_cyber_forces.php (describing plans for a Naval cyber unit). The Department of Defense is also seeking to create its own cybercommand. Sean Gallagher, *New Threats Compel DOD to Rethink Cyber Strategy*, FED. COMPUTER WK. (Jan. 25, 2010), http://fcw.com/articles/2010/01/25/ cover-story-long-cyber-march.aspx. The Air Force, Army, and Navy cybercommands would be composed of members of the U.S. military; the Department of Defense cybercommand would apparently be staffed by members of the military and by civilian employees and contractors. *See id.* (explaining that the Defense Department is requiring both military and civilian personnel to obtain certification before being able to access Defense Department systems).

ready to serve as soon as they were called into action and for only as long as they were needed.[288] It is this flexibility that makes a CNG an advantageous way to incorporate civilians into cyberwarfare: civilians become combatants when and for as long as needed, and then resume their status of noncombatants.[289]

A version of a procedure that the National Guard utilizes could be employed to incorporate CNG members into the U.S. military. When someone joins the National Guard, he or she becomes "part of the Enlisted Reserve Corps of the Army."[290] If the government required civilians working for businesses that are likely to have strategic importance in cyberwarfare to join the CNG, the military could efficiently take control of the employees if and when the need arose. [291]

If the President calls the proposed CNG units to active duty, they become members of the U.S. military.[292] Unlike National Guard

---

288. The United States' experience with the militia could serve as precedent for creating the Cyber National Guard (or Cyber Militia). In 1792, Congress adopted a statute that required "every able-bodied male citizen between the ages of 18 and 45" to be enrolled in the militia and to equip himself with the weapons he would need to discharge his responsibilities as a member of the militia. *See Perpich*, 496 U.S. at 341 (citing 1 Stat. 271 (1792) (repealed 1901)). In adopting the statute, Congress acted pursuant to the authority conferred on it by Article I, Section Nine, Clause Fifteen of the Constitution (giving Congress the power "[t]o provide for calling forth the Militia to . . . repel Invasions"). For the history of the common law militia and its evolution into the modern National Guard, see BRENNER, *supra* note 8, at 165–74.

289. This also distinguishes it from the Cyber Force proposed by Natasha Solce. *See* Solce, *supra* note 105, at 313–18. The Cyber Force, as outlined in Solce's article, would be a new military branch—the cyber-equivalent of the Army, Air Force, Marines, and Navy. *Id.* Solce believes that creating a new military branch and assigning it primary responsibility for cyberwar is the appropriate approach because the military has expertise in dealing with warfare. *Id.* As already explained, the authors do not see this as a desirable, or even an optimal, approach to cyberwarfare; unless every aspect of our society is militarized, cyberwarfare will inevitably target civilian-owned entities. Therefore, the authors of this Article believe that the appropriate approach is to return to the historical strategy that was devised to deal with what might be called pervasive war, i.e., with combat that occurs when there is no segregation between war-space and civilian-space. *See* supra Part II.B.2.

290. *Perpich*, 496 U.S. at 345.

291. As noted earlier, there is some precedent for imposing such a requirement. Air Reserve Technicians are civilian employees who are required to join the Air Force Reserve as part of their employment. *Opportunities for Air Force Reserve Technicians*, AIR FORCE RESERVE COMMAND, http://www.afrc.af.mil/library/jobs/ (last visited Sept. 26, 2010) ("ARTs are full-time civilian employees who are required to serve as members of the Air Force Reserve . . . ."). Certain types of businesses could, perhaps, be declared essential to our cyberwar effort, and Cyberwar National Guard membership could be made a prerequisite for being hired. Imposing this requirement on categories of businesses should reduce the possibility that people would seek employment from another company in order to avoid having to join the CNG.

292. The CNG would have to differ from the National Guard in one important respect. The National Guard has two components: (1) the state National Guards, and (2) the National Guard of the United States. Under current law, when someone enlists in a state National Guard, he or she simultaneously enlists in the National Guard of

members, who can be called up for long terms, CNG members might only be needed for days, or even hours.[293] The government could call them up for only as long as their participation is needed.[294] This scheme creates an efficient and flexible method to bring corporate employees under military control, but could also possibly mitigate the extent to which the conscripted employees (and, perhaps, their corporate employer) are regarded as combatants under the LOAC. The members of the CNG would not be persistent members of the U.S. military, but rather occasional members for the periods when cyberwarfare rages and the government calls them to active duty. During those times, they would be combatants under the LOAC.[295] At all other times they would be civilians and noncombatants. Under the LOAC, the company and its employees might not be legitimate

---

the United States. BRENNER, CYBER THREATS, *supra* note 8, at 172. Members of a state National Guard unit can be deployed as members of the federal armed forces, which means they lose their status as members of their state National Guard and become members of the National Guard of the United States. *Id.* at 171–72. Since CNG members would have to be activated very quickly, the CNG would not include this two-tiered approach to National Guard membership; its members would become members of the U.S. military once they were called to active duty. If nothing else, this could be accomplished by requiring that the members of cyberwarfare-relevant corporations join the Army National Guard or the Air Force National Guard, which collectively comprise the National Guard of the United States. *E.g.*, *National Guard of the United States,* WIKIPEDIA, http://en.wikipedia.org/wiki/National_Guard_of_the_United_States (last visited Sept. 26, 2010); *see also* BRENNER, CYBER THREATS, *supra* note 8, at 171–72.

293. *See generally* Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1 (describing the abruptness of the cyberattacks on the Estonian government in May 2007).

294. As noted earlier, this means their role would be analogous to, but even more attenuated than, that of the military personnel who live in the United States and use drones to carry out air strikes in Afghanistan and elsewhere. *See supra* note 257; *see also* Parks, *supra* note 226, at 121 ("Nation-states look to their entire population . . . to provide for the common defense.").

295. An issue that could arise as to the combatant status of CNG members who were on active duty is the requirement that combatants identify themselves as such by wearing "the uniform assigned to the regular, uniformed armed units of a party to the conflict." Protocol, *supra* note 57, art. 44(7); *see also supra* note 70 and accompanying text (explaining that militias and volunteer corps are identified by "a fixed distinctive sign"). Taken literally, this would mean that CNG members would have to don a uniform associated with one of the branches of the U.S. military as soon as they were activated to participate in cybercombat, and then remove the uniform once they were deactivated. Such a requirement is impracticable and pointless, since neither of the parties to a cyberbattle actually see their human opponents. The fact that members of an opposing force are, or are not, wearing uniforms is therefore irrelevant with regard to establishing that they are bona fide lawful combatants under the LOAC. Unless bits and bytes can be equipped with "uniforms," this aspect of the LOAC logically cannot, and probably should not, apply to cyberwarfare. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 196 (2009) (noting that "[t]here are no flags . . . in a cyber attack"); Mark R. Shulman, *Discrimination in the Laws of Information Warfare*, 37 COLUM. J. TRANSNAT'L L. 939, 955 (1999) ("Whether they are wearing military uniforms or not is inconsequential when the parties cannot see each other."). The issue of uniforms and insignia also relates to the issue of perfidy, discussed in the note immediately below.

targets for retaliatory strikes when the employees are not on active duty with the CNG.[296]

This strategy should also solve any issue of a conflicting chain of command. If all of a company's employees are required to join the CNG, they would all be subject to military command once—and for as long as—they are called to active duty.

IV. CONCLUSION

. . . to . . . fight and win . . . in . . . cyberspace.[297]

Although the issues analyzed in this Article may seem speculative and implausible, the threat of cyberwarfare is real.[298] The issues addressed are the product of two forces. The first force is the world's ever-increasing dependence on cyberspace. As already discussed, as civilian pursuits move into cyberspace, military strategy adapts by seeking ways to exploit cyberspace for martial purposes.[299] The second force is an evolving symbiosis (which originated in the physical world) between the military and civilian mercenaries and contractors.

---

296. Some might argue that this approach could trigger claims that the United States is engaging in perfidy in violation of the LOAC. Article 37 of the Protocol to the Geneva Conventions states that it is "illegal to kill, injure or capture an adversary by resort to perfidy." Protocol, *supra* note 57, art. 37(1). Article 37(1) defines perfidy as involving various types of deception, one of which is "the feigning of civilian, noncombatant status." *Id.* An antagonistic nation might claim that CNG members are simply feigning noncombatant status at certain times but are, in reality, constant members of the U.S. military. To rebut that contention, the United States would have to show that CNG members really were occupying the status of noncombatants at all times other than those when they had been activated as members of the U.S. military. This should overcome a claim of perfidy since perfidy necessarily involves treachery, i.e., deception that is intended to exploit the honorable conduct of one's opponent. *See* GEOFFREY BEST, WAR AND LAW SINCE 1945, at 288–93 (1997) (describing the necessary elements, of perfidy, which includes deception).

The United States could also point out that the Article 37(1) ban on perfidy would not apply to the activities CNG members carry out when they have been activated. CNG members would not seek to, nor would they, "kill, injure or capture" any of their adversaries, assuming, of course, that an "adversary" is defined as a human being. Protocol, *supra* note 57, art. 37(1). It is only logical to assume that adversary is limited to another human being since, as noted earlier, the prohibition on perfidy is intended to penalize treacherous conduct that exploits honorable behavior by an enemy combatant. *See* BEST, *supra*, at 288–93 (discussing perfidy in International Humanitarian Law).

297. *United States Air Force Mission*, U. S. AIR FORCE, http://www.airforce.com/learn-about/our-mission/ (last visited Sept. 26, 2010).

298. *See, e.g.*, Dunlap, *supra* note 83, at 723 ("Cyberspace has evolved . . . to the point that science fiction has become more science than fiction.").

299. *See* discussion *supra* Parts II.B.

A "mercenary" is essentially someone "who accepts money or some benefit for military service."[300] Mercenaries are not members of the regular armed forces of any recognized nation, and they fight for money rather than loyalty to a country or a cause.[301] The role of the mercenary in history is far from insignificant: as one author notes, mercenaries "have played a role in warfare, to varying degrees, throughout most of history."[302] The first reported use of mercenaries occurred in the twelfth century BCE, and the use of mercenaries continued for over three millennia.[303] By the early twentieth century, however, mercenaries essentially disappeared.[304] The decline in the use of mercenaries was due to the rise of the nation-state, which began with the Peace of Westphalia in 1648.[305] Nation-states tended to view "mercenaries as unreliable with questionable loyalty."[306]

A resurgence in the use of mercenaries began after World War II.[307] It started in Africa, where decolonization left many "governments vulnerable to insurgents who were quick to employ skilled mercenaries."[308] The use of mercenaries continued through the twentieth century and accelerated in the first decade of the twenty-first century.[309] As a result, "[d]espite historical American antipathy toward mercenaries, the United States has come to rely increasingly on [them], deploying at least 20,000 in Iraq."[310] That

---

300. Michael Scheimer, *Separating Private Military Companies from Illegal Mercenaries in International Law: Proposing an International Convention for Legitimate Military and Security Support that Reflects Customary International Law*, 24 AM. U. INT'L L. REV. 609, 615 (2009). For a more detailed definition, see Protocol, *supra* note 57, art. 47.

301. *See* Protocol, *supra* note 57, art. 47 ("[A] mercenary is . . . motivated to take part in the hostilities essentially by the desire for private gain and . . . is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict . . . .")

302. Ridlon, *supra* note 257, at 211.

303. *See* MATTHEW TRUNDLE, GREEK MERCENARIES: FROM THE LATE ARCHAIC PERIOD TO ALEXANDER 4–7 (2004) (detailing the use of mercenaries in Ancient Greece); *see also* JANICE E. THOMSON, MERCENARIES, PIRATES AND SOVEREIGNS 7–41 (1996) (detailing the history of mercenaries in Europe).

304. Ridlon, *supra* note 257, at 211.

305. *See, e.g.*, BRENNER, CYBER THREATS, *supra* note 8, at 205–08, 213–15 (explaining how and why the Peace of Westphalia triggered the rise of the nation-state, and why nation-states quickly moved away from mercenaries to national armies composed of their own citizens).

306. Ridlon, *supra* note 257, at 211. As to why nation-states viewed them with distrust while prior sovereigns had not, see BRENNER, *supra,* note 8, at 213–15.

307. Ridlon, *supra* note 257, at 211–12.

308. *Id.*

309. *See, e.g.*, Roger Doyle, *Contract Torture: Will* Boyle *Allow Private Military Contractors to Profit from the Abuse of Prisoners*, 19 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 467, 472 (2007) (noting increasing use of mercenaries since 1969).

310. Saad Gul, *The Secretary Will Deny All Knowledge of Your Actions: The Use of Private Military Contractors and the Implications for State and Political Accountability*, 10 LEWIS & CLARK L. REV. 287, 289 (2006).

figure, as one author notes, "places the United States at the forefront of military outsourcing."[311] Mercenaries, however, are not the only type of military outsourcing.

Like mercenaries, contractors work for pay rather than out of loyalty to a cause or country.[312] Some commentators claim that mercenaries and contractors differ in certain important respects,[313] but others reject the significance of these differences and contend that the two are indistinguishable for all practical purposes.[314] Contractors can be divided into categories of contractors who participate in combat[315] and contractors who merely provide support services to the military.[316] Some argue that contractors who participate in combat are subject to the LOAC because they are functionally indistinguishable from mercenaries.[317] The use of both types of contractors raises difficult questions under the LOAC,[318] but this Article does not address those questions.

---

311. *Id.* at 290.

312. Contractors are often citizens of the countries whose militaries they serve, and therefore may have an allegiance to that country in their personal lives. *See, e.g.*, Ronald D. White, *For Titan, Deaths Hit Close to Home*, L.A. TIMES Apr. 19, 2004, at C1 (reporting on a contractor and U.S. citizen killed in Iraq who was awarded the Purple Heart for service in the Iraqi war). Their professional work for the military, on the other hand, tends to be purely the product of a business arrangement:

> [T]he use of contractors raises the enduring question about mercenaries. Nicolo Machiavelli argued against mercenaries in his classic work of politics, *The Prince*, because they work for pay. Illustrating Machiavelli's warning that soldiers working for pay would not take the kind of life-risking action that can turn the tide of battle, some contractors during the Gulf War fled from a possible chemical weapons attack . . . .

Martha Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism and Democracy*, 46 B.C. L. REV. 989, 1021 (2005).

313. E.L. Gaston, *Mercenarism 2.0? The Rise of the Modern Private Security Industry and Its Implications for International Humanitarian Law Enforcement*, 49 HARV. INT'L L.J. 221, 228–240 (2008).

314. *Id.*; Zoe Salzman, *Private Military Contractors and the Taint of a Mercenary Reputation*, 40 N.Y.U. J. INT'L & POL. 853, 887–89 (2008) (rejecting the argument that contractors differ from mercenaries because they (1) operate from within a corporate structure, (2) "work only for legitimate states," or (3)both).

315. *See, e.g.*, Gaston, *supra* note 313, at 225 ("[P]rivate military firms offer combat capabilities, tactical analysis, and other direct military support."). Some argue that there really is no difference between the two types of contractors. *See, e.g.*, Minow, *supra* note 312, at 1015. ("Great Britain concluded that '[t]he distinction between combat and non-combat operations is often artificial.'").

316. *See, e.g.*, Gaston, *supra* note 313, at 225 ("[F]irms like Halliburton or Kellogg, Brown & Root rarely, if ever, engage in direct combat. Instead, they provide the logistics, supplies, and technical and operational support for most modern military deployments . . . .").

317. *See* Salzman, *supra* note 314, at 880–90 (comparing mercenaries and private contractors).

318. *E.g.*, Geoffrey S. Corn, *Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions*, 2 J. NAT'L SECURITY L. & POL'Y 257, 257–62 (2008).

For the purposes of this Article, the significance of the United States' increasing reliance on mercenaries and contractors lies in the reasons for that reliance. According to one author, there are three reasons why the United States is "at the forefront of military outsourcing."[319] The first is the military downsizing that began in the 1990s: the United States' "active duty force is [now] 30 percent lighter than at the end of the Gulf War," but "the number of missions increased."[320] The second reason is the emphasis on outsourcing, which began in the 1950s and accelerated as the century drew to an end. The Department of Defense policy now "requires the military departments to utilize commercial support whenever appropriate."[321] The third reason is what one author calls "cradle to grave contracting," which is largely a function of the increasing complexity of military technology.[322] She explains that:

> Historically, the private sector would research and develop technology and then relinquish it to the military.
>
> In contrast, most current weapons system contracts extend far beyond technology development. Contractors increasingly are responsible for . . . operation . . . . Contractors may be required to be present during the weapon system's operation, either on a military installation or a battlefield. Many experts believe the military could not function without these contractors.[323]

Contractors have played an integral part of the second Iraq war and the war in Afghanistan by providing support services from behind the lines and even accompanying troops into the field.[324]

The bifurcation between civilians and combatants that once existed and upon which the LOAC is predicated has been eroding for years and may soon disappear in the physical world. The accelerating use of contractors is increasingly a function of the military's use of technology, especially their use of information technology.[325] The military's use of technology forces reliance on

---

319. Gul, *supra* note 310, at 290.

320. Rebecca Rafferty Vernon, *Battlefield Contractors: Facing the Tough Issues*, 33 PUB. CONT. L.J. 369, 375 (2004).

321. *Id.* at 376 (citing DEP'T OF DEFENSE, DIRECTIVE 4100.15: COMMERCIAL ACTIVITIES PROGRAM ¶ 4.4 (Mar. 3, 1989)).

322. *Id.* at 377–78.

323. *Id.* (citation omitted).

324. DAVID ISENBERG, A FISTFUL OF CONTRACTORS: THE CASE FOR A PRAGMATIC ASSESSMENT OF PRIVATE MILITARY COMPANIES IN IRAQ 21 (2004), http://www.ssrnetwork.net/uploaded_files/3463.pdf ("When the Army's technology-heavy 4th Infantry Division deployed to Iraq in 2003, about 60 contractors accompanied the division to operate its digital command and control systems.").

325. *See* P.W. SINGER, CORPORATE WARRIORS: THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 62–63 (2003) (discussing potential problems facing the U.S. military with the increased information technology abilities on non-state actors); Mark Calaguas, *Military Privatization: Efficiency or Anarchy?*, 6 CHI.-KENT J. INT'L & COMP. L. 58, 63–64 (2006).

contractors because civilian-owned entities develop and control the technology[326] and "the technology of modern warfare often exceeds the ability of militaries to train their personnel" to operate it.[327]

Cyberwar is the next—perhaps the ultimate—step in this trend. In kinetic war, the military relies on civilians to develop, implement, and operate technologies for combat purposes.[328] The financial rewards of providing and supporting military technology ensure that interested civilians and civilian-owned entities will step forward to meet the military's needs. Therefore, the military does not need to compel civilian participation with nationalization or conscription.

Cyberwar is very different. As discussed, cyberspace supersedes the constraints of physical reality and, in so doing, makes it impossible to segregate war-space and civilian-space.[329] In effect, cyberwar will be total war, because there will be no principled distinction between combatants and noncombatants and between military and civilian targets.[330]

Therefore, cyberwar will take the integration of civilians into warfare to a higher level. Because civilian-owned technology will *be* the battlefield, cyberwarriors must have access to the technology used by a particular civilian entity and must be able to operate it. The military cannot perform the cyberwarrior's function for several reasons. First, the military does not have enough personnel—let alone enough technologically adept personnel—to take on this task.[331]

---

326. *See* Calaguas, *supra* note 325, at 63 ("[C]ivilian ingenuity, coupled with the rapid pace of development, has endowed non-state entities with greater access to technology than the government . . . ."). The military has hired contractors to develop the weaponry needed for cyberwar. *See, e.g.*, Sanger et al., *supra* note 129.

327. Michael N. Schmitt, *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 CHI. J. INT'L L. 511, 518 (2005). In this same article, Schmitt elaborates on this proposition:

> First, while some technology is so complex that only highly trained individuals can operate it, most military personnel lack the aptitude or length of service to develop the requisite skills. Second, some hi-tech military equipment exists in small numbers in the inventory. Thus, the training thereon is extraordinarily expensive because it benefits from no economies of scale. Both dynamics have led to "package deals" in which the military purchases not only the weapon system, but also contracts for training and maintenance support, and, in some cases, even operation of the system.

Id.

328. *See, e.g.*, 50 U.S.C. app. § 2152(5)(A) (2006) (defining "defense contractor" as "any person who enters into a contract with the United States . . . to furnish . . . a critical technology for the national defense . . . ."); *see also* RAYTHEON, http://raytheon.com (last visited Sept. 26, 2010) (describing the vast array of this civilian company's military technology).

329. *See* discussion *supra* Parts I, II.B.2.

330. *See* discussion *supra* Parts I, II.B.2.

331. *See* THE WHITE HOUSE, CYBERSPACE POLICY REVIEW 17–19 (2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (urging that in order to provide adequate cybersecurity, the government and private sector

Second, even if the military had appropriately trained personnel who could operate the proprietary technology used by a particular target, the personnel would not be able to deploy quickly enough for the response to be effective.[332] In the physical world, militaries can have days, even weeks, to regroup and deploy troops.[333] Cyberattacks

---

must share responsibility and resources). The proposition enunciated in the text above is inferentially derivable from two independent sources.

The first is the respective number of people enlisted in the U.S. military versus the number of people employed in providing computer security and computer support services. According to one source, on December 31, 2009, 1,421,668 people were on active duty in the U.S. military. DEP'T OF DEFENSE, ACTIVE DUTY MILITARY PERSONNEL STRENGTHS BY REGIONAL AREA AND BY COUNTRY (309A) 4 (2009), http://siadapp.dmdc.osd.mil/personnel/MILITARY/history/hst0912.pdf. There were "an additional 848,000 people in the seven reserve components" of the U.S. military. S. 3001, 110th Cong. § 411 (2008). That yields a total of 1,422,516 military personnel who *could* be summoned to take over civilian personnels' roles during a cyberwarfare event. *See id.* We will also assume, for the purposes of this analysis, that these figures are understated to some extent since Secretary of Defense Robert Gates has, on several occasions, proposed increasing the size of one or more branches of the U.S. military. Bryan Bender, *Gates Calls for Buildup in Troops: Asks Bush for 92,000 more by 2012*, BOSTON GLOBE, Jan. 12, 2007, at A1.

According to the Bureau of Labor Statistics, there are currently at least 2,915,000 individuals directly employed in positions requiring computer expertise. BUREAU OF LABOR STATISTICS, DEP'T OF LABOR, HOUSEHOLD DATA ANNUAL AVERAGES, tbl.11 (2009), http://www.bls.gov/cps/cpsaat11.pdf (759,000 computer scientists and systems analysts; 498,000 computer programmers; 952,000 software engineers; 384,000 support specialists; 207,000 network and systems administrators; and 115,000 computer operators). The civilian figure does not, of course, include employees whose primary occupational duties do not involve computer expertise but who work with computer technology in a manner that would be integral to a company's response to cyberfare attacks. In other words, the civilian figures are understated to an uncertain extent.

While either or both may be understated, the figures for the military and civilian personnel are likely to correctly indicate the comparative size of each constituency. Based on sheer numbers, there are not enough military personnel to take over for all the civilians working in computer-related positions. Numerically, the U.S. military could not step in and take over the work being done by the civilians. If they were to do so, this would mean that the government would have to pull all currently-serving and reserve military personnel from their positions and reassign them to replace civilians working in positions integral to cyberwarfare operations.

In addition to the numerical analysis, the impracticability of having military personnel take over for civilian computer personnel in the course of cyberwarfare is inferentially derivable from the fact that, while some military personnel are trained in cyberwarfare, most military personnel are only trained in traditional or guerrilla warfare. The number of personnel who are, or will be trained, in cyberwarfare is uncertain at this writing. *See, e.g.*, J. Nicholas Hoover, *Senate Confirms Military Cybersecurity Chief*, INFO. WK. (May 11, 2010), http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=224701513 ("Some final details of Cyber Command remain to be worked out, such as force size . . . ."). This, of course, means that the majority of current military personnel are simply not qualified to take over the duties of civilian employees in case of cyberwarfare.

332. *See* Lolita C. Baldor, *Report: Cyber Warfare Policies Lack Oversight*, MSNBC, Apr. 29, 2009, http://www.msnbc.msn.com/id/30482502 ("[A] cyber attack can be over in a millisecond . . . .").

333. *See* Spencer Ackerman, *Petraeus: Here's My Afhgan Redeployment Strategy*, WIRED.COM DANGER ROOM (Aug. 18, 2010, 8:47 AM), http://www.wired.com/

occur in milliseconds.[334] The solution to this problem is to have cyberwarriors who are in place on site and ready to be activated.

Moreover, the military cannot train its personnel to operate the vast array of technology that will be in use across all of the civilian-owned entities that could become part of a cyberwar.[335] Many entities will use idiosyncratic technology or customized versions of commercial-off-the-shelf technology. Given the range and number of civilian systems that comprise the U.S. cyberwar battlespace, the military could not deploy troops who would be able to master these technologies, even if civilians cooperate and allow the military to take over. [336]

This discussion is moot because the U.S. military cannot field the military personnel needed to wage cyberwar in what will be a civilian-occupied battlespace: even if Congress increased the military's funding, it would almost certainly not be able to attract individuals with the skills needed to become cyberwarriors.[337] The military cannot compete with the private sector because many of its potential cyberwarriors will opt to work in the private sector where they can earn more money and enjoy more personal autonomy.[338]

---

dangerroom/2010/08/petraeus-afghan-strategy/ (stating that redeploying U.S. troops out of Afghanistan will be a lengthy process).

334. *E.g.*, Baldor, *supra* note 332.

335. *See supra* note 331 and accompanying text. Even if the military were able to overcome the numerical and expertise issues noted above, it would be a wasteful use of resources to have military personnel, in effect, become "shadow" employees of components of the civilian infrastructure. To hire, train, and maintain military personnel whose primary function would be to step into the shoes of civilians who are not only trained to perform particular computer tasks but who are familiar with the idiosyncrasies of specific systems would be duplicative, wasteful, and ultimately unproductive. If the military personnel were to maintain not only the basic computer skills they would need to take over civilian employees' duties, but also familiarity with the current state of the systems with which those employees work, they would have little, if any, time left to perform other duties. They would, in other words, become duplicate, shadow employees, no doubt unable to undertake other military assignments because they would need to be on call to substitute for their civilian counterparts, if and when needed. It would be inherently illogical to create what is essentially a shadow army of military clones simply to ensure that the computers and computer systems involved in cyberwarfare are being operated by enlisted personnel rather than civilian personnel. The logical approach is, as explained above, to transform the essential civilian personnel into members of the military, on either a permanent or transient basis.

336. *See supra* note 331 and accompanying text.

337. *See, e.g.*, Gregory Conti & Jen Easterly, *Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture*, SMALL WARS J., July 29, 2010, at 2–4, http://smallwarsjournal.com/blog/journal/docs-temp/482-conti-easterly.pdf (discussing the difficulty in recruiting qualified cyberwarriors); *see also* Drew & Markoff, *supra* note 258 (noting culture clash between hackers and military).

338. *See* Conti & Easterly, *supra* note 337, at 2–4 (noting that interviews with computer technology professionals demonstrate the differences between government and private sector work); *see generally* Drew & Markoff, *supra* note 258 (describing the advancements made in private sector cybersecurity).

If the military cannot field an adequate force, it seems the only solution is the one proposed in this Article: to integrate civilians into the military to create an onsite force in any part of the nation's critical infrastructure that could be drawn into the cyberwar battlespace. This force must be prepared to engage in offensive or defensive cyberwarfare whenever activated. In recent years, war has been consigned to a distinct and professional military force, but that approach is something of a historical aberration.[339] For millennia, the responsibility to repel hostile forces was the responsibility of the general citizenry. In Anglo-Saxon Britain, it "was the duty of every able-bodied freeman to serve in the army in times of emergency."[340] The "freemen" were called into duty when there was a threat of invasion and then released once the emergency had been addressed.[341] This system, originally known as the fyrd, evolved into the militia system, which British colonists brought to the United States and which became the basis of the colonial military system.[342] The National Guard is the lineal descendant of the militia.[343] The CNG that this Article proposes is essentially a reinvention of the common law militia. Like the common law militia (and unlike the modern National Guard), it would be a dispersed, flexible force that could be called into action quickly and only as needed.

The shift from militias to formally organized military organizations was a product of the shift to nation-states. As nation-states established themselves, they carved the world up into a patchwork of territorially based sovereign entities.[344] These territorially based sovereign entities established and maintained fixed physical boundaries, which introduced a level of predictability and stability into warfare.[345] Nation-states organized permanent,

---

339. *See supra* Part II.A.

340. M.M. KNAPPEN, CONSTITUTIONAL AND LEGAL HISTORY OF ENGLAND 36 (1942).

341. *See id.* (describing the Anglo-Saxon fyrd, made up of freemen, as akin to a modern-day militia). Medieval freemen summoned to military duty seem only to have been obligated to serve a maximum of sixty days in service. *See* C. WARREN HOLLISTER, ANGLO-SAXON MILITARY INSTITUTIONS ON THE EVE OF THE NORMAN CONQUEST 38, 73 (1962) (stating that freemen called into active duty were paid two months wages); HOWARD, *supra* note 225, at 10 (noting that the sixty day obligation was too short for effective campaigning on the Continent).

342. *See* HOLLISTER, *supra* note 341, at 2 ("The fyrd was a rude assemblage of all able-bodied freemen whose service was based upon the old Germanic concept of the nation in arms . . . ."); JAMES B. WHISKER, THE RISE AND DECLINE OF THE AMERICAN MILITIA SYSTEM 12 (1999) (discussing the history of the fyrd in Europe and the American adoption of this practice).

343. Arver v. United States, 245 U.S. 366, 387 (1918); Adam M. Giuliano, *Emergency Federalism: Calling on the States in Perilous Times*, 40 U. MICH. J.L. REFORM 341, 346–47 (2007).

344. *Cf.* BRENNER, *supra* note 8, at 204–08 (describing the rise of the nation-state).

345. *See, e.g.*, *id.* at 208–22 (describing the nation-state's monopoly on power).

professional military forces and assigned them the task of maintaining the integrity of their respective borders.[346] An attack on a state's sovereignty usually took the form of an assault upon the territory it controlled.[347] The goal of war often was to seize control of all or a part of the territory that another nation-state controlled. The military's primary task was to discourage and, when necessary, repel intrusions into the territory that their sovereign controlled. Its subsidiary task was to launch offensive attacks on the territory of other nation-states.

This dynamic effectively divided threats into two types: internal (crime) and external (war).[348] Professional law enforcement organizations evolved to deal with internal threats, while the military dealt with external threats.[349] Law enforcement dealt with civilians and the military dealt with other militaries.[350] This framework is particularly clear in the United States, which carefully differentiates the two functions.

Cyberspace is not a physical construct but rather is essentially a fourth dimension that overlays the three physical dimensions that have historically been the sole venue for human activities. Therefore, cyberspace cannot be divided up into sovereign "territories" demarcated by identifiable, stable borders; this difficulty has certain consequences for the law and tactics of warfare.[351] For the purposes of this Article, the most important of these consequences is the lack of borders. When there are no borders, it is exceedingly difficult, if not impossible, to parse threats into internal (crime) and external (war) and allocate responses between the appropriate organizations (law enforcement and military). It becomes exceedingly difficult, if not impossible, for the military to intercede between attackers acting on behalf of a hostile state and civilians.

The result is that cyberspace "resembles what Hobbes called a state of nature—a 'war of every man against every man.'"[352] Unlike Hobbes's state of nature, cyberspace is populated by individuals who

---

346. *See id.* at 214 (noting that "nation-states had come to rely exclusively on national military forces").

347. *See* G.A. Res. 3314 (XXIX), U.N. GAOR, 29th Sess., Supp. No. 31, U.N. Doc. A/9631, at 142 (Dec. 14, 1974) (definition of "aggression"); ICC, Assembly of States Parties, *Report of the Special Working Group on the Crime of Aggression* app. at 11–12, ICC Doc. ICC–ASP/7/SWGCA/2 (Feb. 12, 2009) (quoted in Michael J. Glennon, *The Blank-Prose Crime of Aggression*, 35 YALE J. INT'L L. 72, 81–82 (2010) (listing conduct that falls under "aggression")).

348. BRENNER, CYBER THREATS, *supra* note 8, at 208–15; *see also* Susan W. Brenner & Leo L. Clarke, *Distributed Security: A New Model of Law Enforcement*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659, 660–66 (2005) (discussing internal and external threats).

349. BRENNER, CYBER THREATS, *supra* note 8, at 208–15.

350. *See, e.g.*, *id.* at 15–23 (discussing the roles of military and law enforcement).

351. *See* discussion *supra* Parts I, II.B.2.

352. BAKER ET AL., *supra* note 1, at 25.

exist in and operate from physical reality and bring their respective allegiances and obligations from that world into cyberspace. Cyberspace presents us with an unstructured, unbounded environment in which nations can play out their various rivalries and seek strategic advantages. The hierarchical, rigid response structures that have evolved over the last few centuries are ineffective in such an environment. To be effective, response mechanisms must be laterally organized, flexible systems that are embedded in the environment. The approach proposed in this Article—a virtual analog of the militia—is one way of achieving such a system.[353]

353. The authors realize that compelling civilians to participate in cyberwarfare can, and no doubt will, have adverse consequences for some of those civilians. These consequences are likely to be particularly significant for the businesses that are conscripted to participate in cyberwar. We do not address the consequential effects of civilian conscription for cyberwar in this article; instead, we will address these "casualty" issues in a separate article we are in the process of completing. Among other things, that article looks at how the Fifth Amendment's Compensation Clause would apply to conscripting corporate property and assets for use in cyberwar. We noted the applicability of the Takings Clause in this Article, but chose to address it in a separate piece because of the complexity of the issues involved. *See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties* (forthcoming) (on file with author).