Fall 2010

Civilians in Cyberwarfare: Conscripts

Susan W. Brenner
Leo L. Clarke

CONSCRIPTS AND CASUALTIES: CIVILIANS IN CYBERWARFARE PART I

BY

SUSAN W. BRENNER* **WITH LEO L. CLARKE****

*NCR Distinguished Professor of Law and Technology, University of Dayton School of Law. Email: susanwbrenner@yahoo.com

**Associate, Drew, Cooper and Anding, Grand Rapids, Michigan. Email: leolclarke@yahoo.com

Table of Contents

Preface

As the title implies, this is the first of two articles that analyze the legal and policy issues that arise from the inevitable involvement of civilians in cyberwarfare.[1]

We decided to divide our analysis into two articles for several reasons, the most important of which is that these issues fall into two essentially discrete categories:[2] The first is the "conscript" category, which is the focus of this article. The issues we address here go to (i) the need to involve civilians in cyberwarfare and (ii) the legal devices we can use to compel such involvement, when and as necessary.

The other category, which is the focus of our second article, is the "casualty" category. In that article we analyze how law can and should address the consequences that result from involving civilians in cyberwarfare.

---

[1] *See* Susan W. Brenner & Leo L. Clarke, *Conscripts and Casualties: Civilians in Cyberwarfare Part II.* As to why civilian involvement in cyberwarfare is inevitable, *see infra* § II(B).

[2] Another reason is that the two articles are likely to appeal, at least in part, to different constituencies; this article is likely to appeal more to those interested in the operational aspects of cyberwarfare, while our second article is likely to appeal more to those interested in the effects cyberwarfare is likely to have on civilians. A third reason is length; we believe it is better to divide our analysis into two articles, each of which is of moderate length, than to combine them into a very lengthy piece.

I. Introduction

> *Critical infrastructure owners . . . report that their networks and control systems are under repeated cyberattack . . . from . . . foreign nation-states.*[3]

According to one estimate, 140 nations have, or are in the process of developing, the capacity to wage cyberwarfare.[4] Other countries will no doubt 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."[5]

While cyberwarfare will probably not displace traditional, kinetic warfare,[6] it will become an increasingly important weapon in the arsenals of nation-states for several reasons. One is cost: Developing the capacity to wage cyberwar is an inexpensive proposition compared to what is involved in developing and maintaining the capacity to wage twenty-first century kinetic war.[7] Since cyberwarfare

---

[3]McAfee, In the Crossfire: Critical Infrastructure in the Age of Cyber War 3 (2009), http://resources.mcafee.com/content/NACIPReport. "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.

[4]*See, e.g.,* Kevin Coleman, *The Cyber Arms Race Has Begun*, CSO Online (January 28, 2008), http://www.csoonline.com/article/216991/Coleman_The_Cyber_Arms_Race_Has_Begun?page=1. *See also Cyber Crime: A 24/7 Global Battle,* ITP Report (November 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 information warfare, electronic warfare and cyberwar. *See* Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, CRS Report for Congress CRS-1 (March 20, 2007), http://www.fas.org/sgp/**crs**/natsec/RL31787.pdf.

[5]McAfee, In the Crossfire: Critical Infrastructure in the Age of Cyber War, *supra* note 3 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.

[6]"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." Air Force Glossary, Air Force Doctrine Document 1-2 57 (January 11, 2007), http://www.docstoc.com/docs/12530146/Air-Force-Glossary. For a more detailed description of kinetic warfare, *see, e.g.,* Cheng Hang Teo, *The Acme of Skill: Non-Kinetic Warfare* 2-3, Air Command and Staff College – Air University (2007), https://www.afresearch.org/.

[7]*See, e.g.,* Martin C. Libicki, *Cyberdeterrence and Cyberwar* xvi, 177 RAND Corporation (2009); 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); John A. Serabian, Jr., Info. Operations Issue Manager, CIA, Statement for the Record Before the Joint Economic Committee on Cyber Threats and the U.S. Economy (Feb. 23, 2000), https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html.

will for the most part be waged over publicly-accessible networks,[8] the expense involved primarily encompasses training and paying cyberwarriors and purchasing and maintaining the hardware and software they will need to launch and counter cyberattacks.

Another factor that makes cyberwarfare an appealing option for nations is the relative conservation of human and non-human resources. While cyberattacks are likely to generate human casualties and property destruction, the damage inflicted will be far less than the damage that results from kinetic attacks.[9] This conservation of resources erodes 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; they launch cyberattacks from within the territory of their own nation-state, which effectively eliminates the likelihood of their being injured and/or killed in a physical encounter with forces from an opposing nation-state.[10] This means that a nation-state (i) only needs a relatively small cadre of cyberwarriors to wage cyberwarfare and (ii) can assume it will lose few, if any, of those warriors in the conflict.[11]

That brings us to a third reason why nation-states are likely to find cyberwarfare attractive: Since cyberattacks are launched remotely, the sponsoring nation-state may be able to disguise the source of the attacks and thereby avoid responsibility for them.[12] Even if Nation A suspects Nation B is the architect of the cyberattacks that targeted its infrastructures, Nation A probably will not (and under the existing laws of war cannot lawfully) retaliate against Nation B unless and until it can confirm that suspicion.[13]

For these and other reasons, cyberwarfare is a phenomenon nation-states will be forced to deal with in the years and decades to come. Because it is a new phenomenon that differs in a number of

---

[8]*See* § II, *infra*.

[9]*See, e.g.,* Arie J. Schaap, *Cyberwarfare Operations: Development and Use Under International Law*, *supra* note 107 at 158 ("benefits 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* Dorothy E. Denning, *Barriers to Entry: Are They Lower for Cyber Warfare?*, IO Journal 6-10 (April 2009); Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyberwarfare*, 106 Mich. L. Rev. 1427, 1440-1441 (2008).

[10]*See, e.g.,* Dorothy E. Denning, *Barriers to Entry, supra* note 9. *See also* Susan W. Brenner, Cyber Threats: The Emerging Fault Lines of the Nation State 71-126 (2009).

[11]*See supra* note 9.

[12]*See, e.g.,* Stephen J. Cox, Comment, *Confronting Threats through Unconventional Means, supra* note 7. *See also* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. Crim. L. & Criminology 379, 410-429 (2007). It is also possible for a state to disguise cyberwarfare attacks as cybercrime. *See* Brenner, *"At Light Speed" supra*, 97 J. Crim. L. & Criminology at 429-440. And for another related advantage of cyberwarfare, *see* Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law, supra*, note 9 (less likely to run the risk of war-crime accusations or claims of violating international LOAC).

[13]*See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 62-64.

respects from traditional warfare,[14] cyberwarfare raises legal, policy and practical issues nation-states will have to resolve, both individually and collectively.[15]

Our focus in this article is on a subset of those issues: As § II explains, cyberwarfare erodes, and may erase, the distinction that currently exists between combatants (soldiers) and non-combatants (civilians).[16] Under the current law of armed conflict (LOAC), civilians are non-actors, i.e., they have no legitimate role in the conduct of traditional military hostilities.[17]

That may change. As we will see in § II(B), civilians are destined to play an active role in the conduct of 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 nation-state combat without violating Constitutional restrictions on executive and legislative authority.[18] We address this issue in § III[19] and provide a brief conclusion in § IV.

II. Civilians in Warfare

> *The right of the non-combatant population to protection. . . involves . . . a corresponding duty of abstaining from . . . hostilities. . . .*[20]

---

[14]*See* Susan W. Brenner, Cyber Threats, *supra* note 10 at 25-70.

[15]*See, e.g.,* McAfee, Virtual Criminology Report 2009, *supra* note 1 at 28-29.

[16]*See, e.g.,* Dakota S. Rudesill, *Precision War and Responsibility: Transformational Military Technology and the Duty of Care Under the LOAC*, 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").

[17]*See* Susan W. Brenner, Cyber Threats, *supra* note 10 at 55-64.

[18]Other countries may need to do something similar, but some, like China, do not have the constitutional and structural constraints that make it difficult to incorporate civilians into a cyberwarfare effort. *See, e.g.,* The US-China Economic and Security Review Commission, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation 33, 37 (2009). http://www.cfr.org/publication/21054/capability_of_the_peoples_republic_of_china_to_conduct_cyber_warfare_and_computer_network_exploitation.html. *See also* Susan W. Brenner, Cyber Threats, *supra* note 10 at 163-199.

[19]Since compelling civilian participation in cyber hostilities creates the possibility of injury to persons and/or damage to civilian-owned property, we will also need to develop laws that address the related issue of liability for cyberwarfare-related losses. As noted in the Preface, we take up these issues in our second article. *See* Susan W. Brenner & Leo L. Clarke, *Conscripts and Casualties: Civilians in Cyberwarfare Part II.*

[20]Karma Nabulsi, *Evolving Conceptions of Civilians and Belligerants* in Civilians in War 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*, Transactions of the Grotius Society 713 (1871)).

As noted above, this section examines the legal issues we must resolve if civilians are to become combatants in cyberwar. Section II(A) reviews the status of civilians under the existing laws of kinetic warfare; while cyberwarfare will rely on methods other than the use of kinetic force, we will assume it qualifies as war under international law.[21] Section II(B) reviews the need for civilian participation in cyberwar and the roles civilians are likely to play in virtual combat; this section provides an empirical context for the analysis in the next section. Section III then takes up the issue noted above: How can the United States compel recalcitrant civilians to become combatants in cyberwarfare?[22]

A. Warfare

> *. . . the inherent right of . . . self-defence if an armed attack occurs against a [state].* [23]

A historian defines war as having three dimensions: violence; legitimacy; and legality.[24] We all know that war involves violence, and we also probably realize the need for legitimacy.[25] Legitimacy is the ideological device nations use to motivate citizens to fight for their country: to convince them that killing their fellow man in battle is the "right" thing to do. War therefore differs from crime, which can also involve violence, because war "derives legitimacy from a political, societal, or religious source. Men are . . . given license to ignore . . . accepted societal conventions against killing and destroying".[26]

---

[21]Since neither United Nations Charter nor multilateral agreements like the NATO treaty explicitly encompass cyberattacks, there are questions as to whether such assaults qualify as warfare. *See, e.g.,* Robert G. Hanseman, *The Realities and Legalities of Information Warfare,* 42 A.F. L. Rev. 173, 184 (1997). Most commentators conclude that the existing LOAC are malleable enough to encompass cyberwarfare, *See id*. *See also* Richard W. Aldrich, *How Do You Know You Are at War in the Information Age?,* 22 Hous. J. Int'l L. 223 (2000).

[22]We assume, here and throughout the remainder of this article, that 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.

The analysis in § III focuses exclusively on United States law and policy for two reasons: One is space; the parameters of a law review article simply do not permit us to conduct a comparative assessment of how this issue will be resolved by the various nations of the world. The perhaps more compelling reason is our limited expertise; to conduct such an assessment would require a great deal of research into the intricacies of state power and citizen rights in various countries. As noted earlier, some nations would not find it particularly difficult to compel their citizens to become cyber-combatants. *See supra* note 18. Others, however, will find it necessary to address issues similar to those we analyze in § III, *infra*. We hope our analysis of that issue, and of the issues addressed in § III, will spark discussion and research into how these issues can best be addressed in other nations.

[23]U.N. Charter art. 51.

[24]*See* Michael S. Neiberg, Warfare in World History 2-3 (2001).

[25]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.

[26]Michael Neiberg, Warfare in World History, *supra* note at 3.

"Legality" is the dimension that is at issue in our analysis of civilian participation in cyberwarfare. Legality is an ancient requirement that evolved in sophistication over the last millennium.[27] As one observer noted, wars are fought according to "understood sets of rules."[28] These rules have historically been divided into two categories: the *jus ad bellum* and the *jus in bello*.[29] The *jus ad bellum* governs the legality of starting a war; the *jus in bello* governs the legality with which a war is conducted.[30] The modern *jus in bello* is particularly concerned with "protecting civilian populations from the injurious effects of armed conflict."[31]

That concern did not always exist. Many trace its origins to Hugo Grotius' 1625 treatise on "the LOAC and peace" -- *De Jure Belli ac Pacis*.[32] 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 . . . frenzy had openly been set loose for the committing of all crimes".[33]

Grotius, and others who would later express similar sentiments, were reacting to the way wars had been waged. Until "well into" the eighteenth century, armies nation-states fielded "were composed largely of mercenaries, whose pay was intermittent and who . . . had to `live off the country.'"[34] These untrained and undisciplined soldiers brutalized civilians and razed farms and towns in the areas they passed through; during the Thirty Years War in the early seventeenth century, "over half the German-speaking population was wiped out" and most of Europe was left a "shambles".[35]

Grotius' writings and the devastation left by the Thirty Years War led to a number of reforms, one of which was that soldiering was professionalized: Troops were trained, organized in a "chain of command" consisting of "regiments and other standard units," and fed, clothed and paid regularly.[36]

---

[27]Michael Neiberg, Warfare in World History, *supra* at 9-20, 46-58. *See, e.g.,* Chris Jochnick &Roger Normand, *The Legitimation of Violence: A Critical History of the LOAC,* 35 Harv. Int'l L.J. 49, 60 (1994). *See also* Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II,* 47 Naval Law Review 176, 182-187 (2000).

[28]Michael Neiberg, Warfare in World History, *supra* at 3.

[29]*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).

[30]*See 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).

[31]R.J. Araujo, *Anti-Personnel Mines and Peremptory Norms of International Law, supra* note 30 at 7.

[32]*See* Hugo Grotius, The Law of War and Peace (De Jure Belli ac Pacis) (1625), http://www.lonang.com/exlibris/grotius/index.html.

[33]Hugo Grotius, Prolegomena to the Law of War and Peace 21 (Oskar Piest ed., Francis W. Kelsey trans., Liberal Arts Press, Inc. 1957).

[34] Telford Taylor, The Anatomy of the Nuremburg Trials: A Personal Memoir 6 (1992).

[35]*Id.*

[36]*Id.*

Armies added staff to handle supply and transport, and established procedures to maintain discipline among troops.[37] From all this, there developed customs and rules governing soldiers' relationships with civilians and their conduct while occupying foreign territory.[38]

Others echoed Grotius' call for a law of armed conflict -- an LOAC. Rousseau, for example, said that since war was a battle between nation-states, soldiers should "respect the person and property of individuals" who were not involved in combat.[39] There were other calls for reform during the eighteenth century, but the LOAC would remain unwritten until the next century.[40]

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 commissioning Francis Lieber to draft a code governing the conduct of warfare.[41] Article 15 of Lieber's Code made "military necessity" the basis for determining what actions were appropriate during military combat.[42] Under Article 15, military necessity authorized "direct destruction of life or limb of armed enemies" and of others "whose destruction is incidentally unavoidable in the armed contests of the war", as well as capturing enemy soldiers and destroying property.[43] Article 16 qualified this broad grant of authority, explaining that military necessity "does not admit of cruelty - that is, the infliction of suffering for the sake of suffering" or "wanton devastation."[44] And Article 37 of the Lieber Code specifically stated that solders were not to harm civilians or private property "in hostile countries occupied by them".[45]

In 1874, the Union Army's rules governing the conduct of warfare became the basis of a

---

[37]*Id.*

[38]*Id. See also* Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II*, 47 Naval L. Rev. 176, 186-189 (2000).

[39]Jean-Jacques Rousseau, Discourse on Political Economy and The Social Contract 52 (Trans. By Christopher Betts) (1994).

[40]*See, e.g.,* Chris af Jochnick & Roger Normand, *The Legitimation of Violence: A Critical History of the LOAC,* 35 Harv. J. Int'l L. 49, 60-66 (1994). *See also* Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II, supra* note 38 at 189-198.

[41]*See* Francis Lieber, Instruction for the Government of Armies of the United States in the Field, General Order No. 100 (April 24, 1863), http://www.yale.edu/lawweb/avalon/lieber.htm#sec2. *See also* Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II, supra* note 38 at 189-193.

[42]*See* Lieber, Instruction for the Government of Armies of the United States in the Field, *supra* note 41 at Article 15.

[43]*See id.*

[44]*See id.* at Article 16.

[45]*See id.* at Article 37, Other Articles prescribed similar treatment for museums, libraries, hospitals, churches, charities and educational institutions. *See id.* at Articles 34-36.

"Declaration Concerning the Laws and Customs of War," which was drafted at a conference in Brussels.[46] Although the Declaration was never formally adopted (and never became effective), it stimulated a series of efforts that ultimately culminated in the Hague Conference of 1899.[47]

The conference produced the Hague Convention of 1899; while the Convention did little to develop a fully realized LOAC, it formally articulated the principle that during warfare "populations and belligerents remain under the . . . the principles of international law".[48] This statement incorporated a concept that had been evolving over at least two centuries, namely, that civilians and surrendering combatants should be treated as non-combatants.[49] Aside from giving some consideration to non-combatants, 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."[50] The second Hague Conference, held in 1907, produced another Convention that differed very little from its predecessor.[51]

In the aftermath of World War I, countries adopted pacts that outlawed the use of chemical weapons,[52] an effort that seems to have 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.[53] Both Conventions

---

[46]*See* Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II, supra* note 38 at 194.

[47]*See id.* at 194-196.

[48]Preamble of the (Hague II) Convention with Respect to the Laws and Customs of War on Land, The Hague (July 29, 1899), http://www.yale.edu/lawweb/avalon/lawofwar/hague02.htm. *See* Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II, supra* note 38 at 196-197.

[49]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 LOAC: Does Customary International Law Prohibit The Use Of Nuclear Weapons In All Circumstances?,* 20 Fordham International Law Journal 181, 243 n. 426 (1996) (citing Lester Nurick, *The Distinction Between Combatant and Noncombatant in the Law of War,* 39 American Journal of International Law 680, 681 (1945)). But by 1806, Napoleon's minister Talleyrand would write that "`the law of nations does not permit that the rights of war, and of conquest . . . should be applied to peaceable, unarmed citizens'". Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II, supra* note 38 at 1189 (citing Telford Taylor, The Anatomy of the Nuremburg Trials: A Personal Memoir 7 (1992)).

[50]*See* (Hague II) Convention with Respect to the Laws and Customs of War on Land, The Hague (July 29, 1899), http://www.yale.edu/lawweb/avalon/lawofwar/hague02.htm.

[51]Preamble of the (Hague II) Convention with Respect to the Laws and Customs of War on Land, The Hague (July 29, 1899), http://www.yale.edu/lawweb/avalon/lawofwar/hague02.htm. *See* Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II, supra* note 38 at 198-199.

[52]*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.

refined principles concerning the treatment of erstwhile combatants that had been articulated in earlier agreements.[54]

In 1949, the1929 Geneva Conventions were superseded by four new Conventions: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea; Convention (III) Relative to the Treatment of Prisoners of War; and Convention (IV) Relative to the Protection of Civilian Persons in Time of War.[55] 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."[56] Convention IV therefore makes protecting civilians and other noncombatants a binding obligation on countries, which become Parties to the Convention.[57]. One hundred and ninety-four countries have ratified Convention IV.[58]

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 them."[59] Under Article 3, Parties to the Convention must treat those who took no active part in the hostilities "humanely."[60] Those who fall into this category are protected from the commission of the:

---

[53] *See* Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II, supra* note 38 at 199-203.

[54]*See id.* at 202-203.

[55] *See* The LOAC, The Avalon Project at Yale Law School, http://www.yale.edu/lawweb/avalon/lawofwar/lawwar.htm. *See also* Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the LOAC in the Age of Terror*, 153 University of Pennsylvania Law Review 675, 691 (2004) (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").

[56]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 International Committee of the Red Cross, International Humanitarian Law: Answers to Your Questions 8 (2002), http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/p0703).

[57]*See* Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War (1949), http://www.icrc.org/ihl.nsf/WebList?ReadForm&id=380&t=art.

[58]*See* International Committee of the Red Cross, Geneva Conventions of 12 August 1949, http://www.icrc.org/ihl.nsf/WebSign?ReadForm&id=375&ps=P. *See also* Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1977), http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 ("Protocol").

[59]Protocol, *supra* note 58 at Article 2. The 1977 Protocol extended the Convention's provisions to conflicts involving non-nation state actors *See* Protocol, *supra* note 58 at Article I.

[60]*Id*. at Article 3(1).

"violence to life and person" and "outrages upon personal dignity".[61] 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."[62]

The provisions of Convention IV were supplemented in 1977 by an Additional Protocol.[63] Article 51 of the 1977 Protocol says that civilians "enjoy general protection against dangers arising from military operations", which means, among other things, that they "shall not be the object of attack."[64] Under Article 51(3), civilians are entitled to this protection "unless and for such time as they take a direct part in the hostilities",[65] which brings us to the bifurcation between combatants and noncombatants that structures the modern LOAC. Article 48 of the 1977 Protocol says that "in 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."[66]

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."[67] Article 43(1) defines "armed forces of a Party to a conflict" as all of its

> organized armed forces, groups and units which are under a command responsible to that Party for the conduct of 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 compliance with the rules of international law applicable in armed conflict.[68]

Article 4 of Convention III, which deals with the treatment of with prisoners of war,[69] broadens this definition of combatants. Under Article 4, prisoner of war status is afforded to certain combatants, including members of the armed forces of a Party and members of "other militias and other volunteer

---

[61] *Id*. at Article 3(2). Article 3(2) also prohibits the taking of hostages and the passing of sentences and carrying of executions without adequate judicial process. *See id*.

[62] *Id*. at Article 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).

[63] *See supra* note 58.

[64] Protocol, *supra* note 58 at Article 51(1)-(2).

[65] *Id*. at Article 51(3).

[66] *Id*. at Article 48.

[67] *Id*. at Article 43(2).

[68] *Id*. at Article 43(1).

[69] *See* Geneva Convention (III) relative to the Treatment of Prisoners of War (1949), http://www.icrc.org/ihl.nsf/WebART/375-590007?OpenDocument.

corps" who meet certain requirements.[70] 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;
>
> (d) that of conducting their operations in accordance with the laws and customs of war. [71]

Most commentators agree that the Geneva Conventions create "only two categories: lawful combatants, and civilians."[72] The United States, however, takes the position that there are three categories: "lawful combatants, unlawful combatants, and civilians."[73]

A lawful combatant falls into one of the Geneva Convention categories noted above, i.e., qualifies as a "combatant"; lawful combatants are "immune from prosecution for lawful combat activities" and on being captured, receive 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" conducting military hostilities; [75] unlawful combatants forfeit a lawful combatant's immunity from prosecution and prisoner of war status and, on being captured, "may be tried in a military commission" and if convicted, "be punished appropriately."[76] The third category is comprised of civilians: individuals who do not qualify as

---

[70]*Id*. at Article 4. 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. at Article 4(5)-(6).

[71]*Id*. at Article 4(A)(2). *See also* Protocol, *supra* note 58 at Articles 43 & 44. These same conditions appeared in the fourth Hague Convention. *See* Hague Convention (IV): Laws and Customs of War on Land annex art. 1 (October 18, 1907), http://www.yale.edu/lawweb/avalon/lawofwar/hague04.htm.

[72]Curtis A. Bradley, *The United States, Israel & Unlawful Combatants*, 12 Green Bag 397, 398 (2009).

[73]*Id*. at 399 (note omitted).

[74]Joseph P. "Dutch" 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).

[75] W. James Annexstad, *The Detention and Prosecution of Insurgents and Other Non-Traditional Combatants*, 2007-JUL Army Law. 72, 72 (2007).

[76]Joseph P. "Dutch" Bialke, *Al-Qaeda & Taliban Unlawful Combatant Detainees, Unlawful Belligerency, and the International Laws of Armed Conflict, supra* note 74, at 10-11. For more on this distinction and its consequences, *see, e.g.,* Benjamin J. Priester, *Who Is a "Terrorist"? Drawing the Line between Criminal Defendants and Military Enemies,* 2008 Utah L. Rev. 1255, 1280-1283 (2008).

combatants under the Geneva Convention standards outlined above who 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 *qua* civilians have no legitimate role in warfare, at least not in kinetic warfare. In § III, we will consider whether the same state of affairs should exist for cyberwarfare. Before we take up that issue, however, we need to examine why some believe it will be necessary for civilians to take an active role in the conduct of cyberwarfare.

B. Cyberwarfare

> *welcome . . . cyber-warriors. . . . Our nation's future depends on you.*[82]

To understand why civilians may have to become cyber-warriors, one needs to appreciate (i) how and why war has historically differed from other human endeavors and (ii) why these differences are likely to be less pronounced for cyberwarfare. We address these issues in the two sections below.

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".[83] War, as we saw earlier,[84] is a struggle between nation-states.

---

[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).

[78]*See, e.g., 2003-2004 Survey of International Law in the Second Circuit*, 31 Syracuse J. Int'l & Com. 327, 335-336 (2004). *See also* Presbyterian Church of Sudan v. Talisman Energy, Inc., 244 F. Supp.2d 289, 316-321 (S.D.N.Y. 2003).

[79]*Id.* It is not settled as to whether the Geneva Conventions are part of the *jus cogens*, i.e., the "`"intransgressible principles of international customary law"'". *See* Jean-Marie Henchaerts, *The Grave Breaches Regime as Customary International Law*, 7 Int'l Crim. Just. 683, 700-701 (2009).

[80]*See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 54.

[81]In the modern world, armed services are composed of individuals who have more or less willingly chosen to enlist. Once civilians join one of their nation's armed services, they cease to be civilians, an issue we will return to in § III, *infra*.

[82]Major General 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).

[83]The Brig Amy Warwick (The Prize Cases), 67 U.S. 635, 652 (1863).

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 a purely collective undertaking.[85]

There two reasons why war is an activity that is restricted to nation-states. One is conceptual; the other is practical.

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.[86] Individuals struggle to achieve prosperity or prominence or other personal goals. Nation-states struggle to achieve political dominance, a commodity on which they hold a monopoly.[87] Historically, then, war has had three elements: (i) A "contention between at least two" nation-states (ii) which use their armed forces (iii) in an effort to overpower the opposing nation-state(s) and impose "peace on the victor's terms".[88] The enormity of the stakes in war therefore transcends the grasp, and the capacity, of discrete individuals.

That brings us to the other reason why war has been the exclusive province of nation-states: Only sovereign entities have been able to summon and exercise the kinetic force needed to wage these vast struggles.[89] Non-nation-state actors have on occasion declared war on nation-states,[90] but such

---

[84]*See supra* § I.

[85]*See, e.g.*, Willard Hurst, *Treason in the United States,* 58 Harv. L. Rev. 806, (1945) (war "is in its nature a collective activity"; "in 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 Fed. Cas. No. 14,693, at 137 (C. C. D. Va. 1807):

> 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.

[86]*See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 54-65, 68-70. *See also supra* note 85.

[87]*See id*. at 203-204.

[88]Yoram Dinstein, War, Aggression and Self-Defense 4-5 (2005). War has been monopolized by the dominant sovereign entity, which has not always been the nation-state. *See, e.g.,* Martin van Creveld, The Rise and Decline of the State 1-1126 (1999) (tracing evolution of sovereign entities from tribes through city-states and empires to nation-states). *See also* Susan W. Brenner, Cyber Threats, *supra* note 10 at 204-208.

[89]*See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 203-222. *See also* Martin van Creveld, The Rise and Decline of the State, *supra* note 88 at 242-258.

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. Code § 2751. *See also Coping with U.S. Export Controls 2080 - Appendices*, 910 PLI/Comm 485, 581-583 (2008); 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, 627-632 (2002). The Supreme

declarations are merely symbolic gestures; no aggregation of individuals can acquire and implement the kinetic resources needed to credibly wage war with one or more nation-state actors.[91] Since non-state actors who aspire to wage war lack the political authority and tactical capacity to do so, nation-states have treated them as criminals or terrorists.[92]

Traditionally, then, the only legitimate role individuals could play in the process of waging war was as a member of the armed forces of one of the nation-state combatants. This role was not only legitimate; it was essential. Nation-states necessarily act through individuals; aggregations of individuals are one of the tools states use to conduct their struggles with each other.[93]

This state of affairs, though, can exist only as long as the conditions that sustain it continue to exist. If war ceases to be a struggle between nation-states and/or if nation-states no longer monopolize the weapons used to wage war, it may no longer be viable. We take up that issue in the section immediately below.

2. Cyberwarfare

We are structuring this discussion around the roles combatants play in war. More precisely, we derive a dichotomy from the roles combatants traditionally play and then use it to explain why, and how, civilians will become embroiled in cyberwarfare.

Military combatants play two roles: offensive and defensive.[94] 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.[95]

These roles, and the conception of war they derive from, are predicated on the assumption that combatants (for both sides) are segregated from non-combatants.[96] That is, they assume segregation

---

Court has indicated that the Second Amendment does not give U.S. citizens the right to possess military-grade weaponry. *See* District of Columbia v. Heller, 128 S. Ct. 2783, 2816-2817 (2008).

[90]*See, e.g.,* Al Qaeda's Fatwa, Online NewsHour, PBS, http://www.pbs.org/newshour/terrorism/international/fatwa_1998.html (declaring jihad, or holy war, on the United States and Israel).

[91]*See, e.g.,* Martin van Creveld, The Rise and Decline of the State, *supra* note 88 at 242-258. *See also supra* note 85.

[92]*See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 37-42. *See also supra* note 85.

[93]*See supra* note 85.

[94]*See, e.g.,* U.S. Department of the Army, FM 3-0 at §§ 3-37 to 3-52 (offensive) & 3-53 to 3-67 (defensive) (2008).

[95]*See, e.g., id.* at § 3-37 ("Offensive operations are combat operations conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers"). *See also id*. at § 3-53 ("Defensive operations counter enemy offensive operations).

[96]*See supra* § II(A).

between war-space and civilian-space. As we saw earlier, this assumption derives from the LOAC, which require military commanders to protect civilian populations from the "dangers arising from military operations."[97]

While this principle and the assumption it generates can become problematic in kinetic warfare, both continue to be viable components of conventional warfare.[98] Their viability erodes, though, as we move to cyberwarfare. The erosion manifests itself in two ways, each of which is analogous to one of the roles combatants play in warfare. The sections below explain (i) how cyberspace erodes the segregation between war-space and civilian-space and (ii) how that erosion undermines the distinction between combatants and non-combatants. The first section addresses what we are calling the defensive erosion of the divide between combatants and non-combatants; the second addresses the offensive erosion of that divide.

(a) Defensive Engagement

As noted above, it is possible to maintain a level of segregation between war-space and civilian-space in kinetic combat. That possibility is the empirical premise of laws that require military commanders to separate combat from civilians.[99] The viability of segregating combatants and non-combatants is, however, very much a function of physical reality.

Kinetic warfare takes place in real-space, which is fixed, tangible and structured by three physical dimensions.[100] Since physical reality is objective and therefore stable, it is *possible* for commanders to structure combat activity so it has the least possible effect on civilians. The use of new weapons technologies in the twentieth century sometimes complicated the process of segregating war-space and civilian space,[101] but the inherent stability of the context within which combat occurred meant this was still a feasible goal.

The use of cyberspace as the vector for attacks further complicates that process because the combat activity takes place in an unreal, and therefore inherently unstable, environment. Cyberwarfare takes place "in" cyberspace: a "domain characterized by the use of electronics . . . to store, modify, and

---

[97]Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, *supra* note 59. *See also* notes 64-66 & accompanying text, *supra.*

[98]*See, e.g.*, Jack M. Beard, *Law and War in the Virtual Era*, 103 Am. J. Int'l L. 409, 409-410 (2009); R. George Wright, *Combating Civilian Casualties: Rules and Balancing in the Developing Law of War*, 38 Wake Forest L. Rev. 129, 140 (2003).

[99]*See supra* § II(A).

[100]*See, e.g.,* Concise Oxford English Dictionary 1373 (10th ed. Rev.) (J. Pearsall, ed. 2002) (defining "space" as "the dimensions of height, depth and width within which all things exist and move"). *See generally* "Space," Wikipedia, http://en.wikipedia.org/wiki/Space.

[101]In World War II, for example, 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. Nathan A. Canestaro, *Legal and Policy Constraints on the Conduct of Aerial Precision Warfare,* 37 Vand. J. Transnat'l L. 432, 447 (2004).

exchange data via networked systems and associated physical infrastructures."[102] Cyberspace is not a physical "place;" it is a "virtual interactive experience" accessible without regard to geography.[103] It is in effect a fourth dimension – an interactive overlay that is superimposed on, and supersedes, the constraints of physical reality.[104] Given all that, we know cyber-combat will differ in certain respects from the kinetic attacks used in conventional warfare; we also know that the differences will lie not in the goals combat is intended to achieve, but in how combat carried out.[105]

---

[102]"Michael W. Wynne, Secretary 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.af.mil/library/speeches/speech.asp?id=283.

[103]"Cyberspace," Wikipedia, http://en.wikipedia.org/wiki/Cyberspace.

[104]*See, e.g.,* Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?,* 4 Cal. Crim. L. Rev. 1, ¶ 4 11 (2001) (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, 296-297 (2008).

[105]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 an attempt to prevail in a struggle differentiate the two types of warfare.

As to the methods to be used in cyberwarfare, a scene in an episode of the BBC television show *Spooks* illustrates how the two will differ. *See* John Ozimek, *Spooks Foils Fictional Russian Plot*, The Register (November 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 we explain in the text above, an attack like this could be a viable component of a cyberwarfare assault. The problem with the scenario lay not in the result the attack was intended to achieve, but in 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 or submarine or airplane or drone that is delivering a weapon to its target to be physically proximate to that target; here, as *The Register* reporter pointed out, it is not. Physical space is irrelevant in cyberwarfare.

At a basic level, it will involve using computer systems to attack other computer systems.[106] Many, though, think cyberwarfare operations will be much broader than simply attacking computer systems, as such; they believe the victim state's critical infrastructure will be a primary target of a cyberwarfare campaign.[107] Federal law defines "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.[108]

Attacking a nation's critical infrastructure is a way for a hostile state to erode the victim state's internal

---

[106]*See, e.g.,* Timothy Shimeall, Phil Williams & Casey Dunlevey, *Countering Cyber War,* 49 NATO Review 16, 17 (2001) ("In a limited cyber war, the information infrastructure is the medium, target and weapon of attack"). *See also* Steven A. Hildreth, Congressional Research Service Report for Congress, Cyberwarfare 11 (June 19, 2001), http://ww.fas.org/irp/crs/RL30735.pdf. Air Force Policy Directive 10-7 defines "network warfare operations" as the

> 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 Dir. 10-7, Information Operations 23 (2006), http://www.fas.org/irp/doddir/usaf/afpd10-7.pdf.

[107]*See, e.g.,* Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. Rev. 121, 133 (2009) (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, 429-431 (2006). One article distinguishes this type of cyberwar campaign from the more limited type noted above. *See* Timothy Shimeall, Phil Williams & Casey Dunlevey, *Countering Cyber War, supr*a note 106:

> 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.

See also Kevin Coleman, *The Cyber Arms Race Has Begun*, CSO Online (Jan. 28, 2008), http://www2.csoonline.com/exclusives/column.html?CID=33496 (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").

[108]42 U.S. Code § 5195c(e). The Homeland Security Act of 2002 incorporated this definition. *See* 6 U.S. Code § 101(4). A similar definition is incorporated into 50 U.S. Code § 2152(2), 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. McAfee, Virtual Criminology Report 2009, *supra* note 1 at 16.

operational viability and morale;[109] it can also deprive the victim state of "infrastructure that supports military actions".[110]

This is where civilians enter the picture; they tend to own the components of a nation's critical infrastructure.[111] Since critical infrastructures are "likely targets" in cyberwar, private companies are likely to be "caught in the crossfire" of cyberwarfare.[112] Private companies are actually likely to be the specific targets of a deliberate cyberattack; and while it may seem such an attack violates the LOAC, that is far from certain.[113]

As we saw in § II(A), the contemporary LOAC evolved to address the conduct of kinetic warfare; it is therefore triggered by activity that is identical or analogous to the activity involved in kinetic combat. The requirement of an "armed attack" or a "use of force" derives from the modern *jus ad bellum*;[114] the primary source of the contemporary *jus ad bellum* (which is part of the LOAC) is the United Nations

---

[109]*See, e.g.,* Brian M. Mazanec, *The Art of (Cyber) War,* 16 The Journal of International Security Affairs (2009), 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."). *See also id.* (cyberattacks could "wreak economic havoc" on the United States).

[110]Arie J. Schaap, *Cyber Warfare Operations, supra* note 107, at 172. *See also The New Cyber College of International Lawyers,* 95 Am. Soc'y Int'l L. Proc. 173, 182 (2001).

[111]*See* Timothy Shimeall, Phil Williams & Casey Dunlevey, *Countering Cyber War, supr*a note 106. *See also* McAfee, In the Crossfire: Critical Infrastructure in the Age of Cyber War, *supra* note 3 at 25 ("Globally, a majority of critical infra- structure is in the hands of private companies"). *See, e.g.,* The White House, The National Strategy to Secure Cyberspace 1 (2003), http://www.dhs.gov/files/publications/publication_0016.shtm (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.*

[112]McAfee, Virtual Criminology Report 2009, *supra* note 1 at 16. Eight years ago, a CIA representative told Congress that

> [w]e 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.

John A. Serabian, Jr., Statement for the Record Before the Joint Economic Committee on Cyber Threats and the U.S. Economy, *supra* note 7,

[113]*See, e.g.,* Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. Rev. 1, 5-6 (2009) (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).

[114]*See supra* notes 29 - 30 & accompanying text.

Charter.[115] Article 2(4) of the Charter outlaws aggressive war; it prohibits 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."[116]

The Charter creates two exceptions to this prohibition: Security Council action under Article 42 and self-defense under Article 51.[117] Article 51 applies to nation-states; it 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".[118] Under the United Nations Charter, then, "war" involves a "use of force" and/or an "armed attack."[119] The Charter, however, does not define either term.[120]

Because the United Nations Charter was written long before the Internet existed, it was clearly not intended to encompass cyberattacks; and because it was written in the aftermath of two World Wars, it clearly was intended to encompass kinetic attacks, i.e., attacks involving the use of physical force.[121] It is therefore reasonable to assume these are the only type of attacks the Charter encompasses. Since cyberattacks will almost certainly not involve a use of physical force, the Charter, and the contemporary LOAC, probably do not apply to them.[122] If the LOAC do not apply to cyberattacks, a country would not

---

[115]*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").

[116]U.N. Charter art. 2, para. 4.

[117]See U.N. Charter arts. 42 & 51. See *also* Sean M. Condron, *Getting It Right, supra* note 115 at 412.

[118]U.N. Charter art. 51.

[119]This was intended to outlaw aggressive war. *See, e.g.,* 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).

[120]*See, e.g.,* Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. Int'l & Comp. L. Rev. 439, 440-441 (2009); 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).

Article 1 of a related document, the United Nations Declaration 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 says "act of aggression" includes invasion, bombardment, and attacks on the victim state's armed forces or marine or air fleets. Definition of Aggression, Annex to G.A. Res. 3314 (XXIX), U.N. GAOR, 29th Sess., Supp. No. 31, at 143, U.N. Doc. A/9631 (1974). It also includes attacks by "irregulars or mercenaries" that can be attributed to a nation-state). *See id.* at Article 3(g) ("substantial involvement" of a nation-state).

[121]*See supra* note 119.

[122]*See, e.g.,* Arie J. Schaap, *Cyber Warfare Operations, supra* note 107, at 144-147 (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 long sequence of cyberattacks that at least resembled cyberwarfare. *See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 1-6. During the attacks, Estonia struggled to maintain the operational viability of essential systems, and therefore sought assistance from the North Atlantic Treaty Organization. *See, e.g.,* Arie J. Schaap,

commit an illegal act by deliberately launching such attacks at civilian-owned targets, which makes offensive cyberwarfare an attractive option for aggressive nation-states.[123]

Civilian involvement in offensive cyberwarfare will consequently be defensive, at least in part.[124] Whether an attack targets the electrical grid, the financial system, the air traffic control system or any of a host of other infrastructure components, it will involve directing hostile traffic at the computer systems used by the target entities.[125] At that point, the computer staff of the target entities is in a position analogous to that of soldiers who are being attacked by the military forces of enemy nation-state;[126] 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 will be responsible for defending their "territory" from hostile activity; their primary defensive goal will be to keep their systems

---

Cyber Warfare Operations, supra note 107, at 144-145. 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.*

[123]*See, e.g.,* Bruch H. Kobayashi, *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goods*, 14 Sup. Ct. Econ. Rev. 261, 262 (2006). A state's ability to disguise the nature and source of cyberattacks is another factor that makes them an attractive way to pursue aggressive war. *See, e.g.,* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare*, *supra* note 12, at 427-440. 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 McAfee, In the Crossfire: Critical Infrastructure in the Age of Cyber War, *supra* note 3 at 30 (quoting Kimberly Zenz, Russia specialist, iDefense Labs).

Although aggressive cyberwarfare may not quality as unlawful warfare under the United Nations Charter and other aspects of the LOAC, it may still constitute . . . something. It might qualify as state-sponsored terrorism and/or state-sponsored crime. Those issues, however, are outside the scope of this article. For an examination of those issues, *see, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 71-161.

[124]See infra § II(B)(2)(b) for offensive civilian involvement in cyberwar.

[125]For a description of tools likely to be used in such an attack, *see, e.g.,* Richard Stiennon, *Technology and the Advent of Cyber War*, Information Security Resources (December 15, 2009), http://information-security-resources.com/2009/12/15/technology-and-the-advent-of-cyber-war/. *See also* Barbarians Inside the Cyber Gates, FireEye Malware Intelligence Lab (January 14, 2009), http://blog.fireeye.com/research/2009/01/barbarians-inside-the-cyber-gates.html (stealth malware). Distributed denial of service attacks were used in the large-scale attacks on Estonia in 2007, attacks Estonia initially believed were cyberwarfare. *See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 1-6.

[126]*See, e.g.,* "Battle of Baltimore," Wikipedia, http://en.wikipedia.org/wiki/Battle_of_Baltimore (bombardment of Fort Henry).

functioning despite attempts to shut them down.[127]

There are two ways they can do this: (i) try to nullify or minimize the effects of the signals targeting their systems; and/or (ii) try to end the attack by striking back at the attackers. The most likely response is purely defensive, i.e., try to nullify or minimize the effects of the attack; in this mode, the computer staff is in a position analogous to that of civilians in kinetic warfare. Their reactive role is as casualties (or prospective casualties) whose goal is to limit the amount of damage the systems for which they are responsible sustain. 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 is similar to the analogous role civilians play in kinetic warfare but it differs in certain respects, the most significant of which is that these civilians are advertent, rather than inadvertent, targets.[128] As we explain in § III, this and other aspects of civilians' defensive involvement in cyberwar raise legal issues that have not been resolved.[129]

This brings us to the second response option: the defensive-offensive strategy. While this option involves offensive action, i.e., striking back at the attackers in an effort to end the attack, we refer to it as the defensive-offensive strategy because the use of offensive tactics is reactive. It is triggered by an attack and is intended to end the attack, instead of being the type of purely offensive strategy we examine in the next section.

The civilians' response in this mode is more analogous to the response of the soldiers in the analogy we used earlier;[130] like soldiers under attack, they will use both defensive and offensive tactics to withstand and repel the attack. While the use of a defensive-offensive strategy by civilians is not unheard of in the physical world, it is unusual. 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 kinetic

---

[127]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.

McAfee, In the Crossfire: Critical Infrastructure in the Age of Cyber War, *supra* note 3 at 26.

[128]*See supra* § II(A).

[129]The fact 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 but it must still constitute . . . something. If civilians launched attacks such as those hypothesized above, the attacks would constitute cybercrime or cyberterrorism. If they are launched by a nation-state but do not rise to the level of cyberwar, it seems they should qualify either as state-sponsored cybercrime or state-sponsored cyberterrorism. These issues, though, are outside the scope of this article. For an analysis of them, *see, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 152-155.

[130]*See supra* note 126 & accompanying text.

war. There are two reasons why this response is unusual. The first, and perhaps most obvious, is that civilians usually do not have military-grade weaponry they can use to engage the forces of an enemy nation-state effectively.[131] The other, related reason is mounting an offensive, regardless of whether it is effective or not, response can result in punitive reprisals.[132]

Our use of cyberspace erodes, if it does not eliminate, the weapons problem; most computer hardware and software is dual-use technology, i.e., can be and often is used by both civilians and military personnel.[133] As to reprisals, there seems no logical reason why our use of cyberspace should eliminate them as a possibility, though it might reduce their punitive nature. Cyber-mediated reprisals are unlikely to inflict the physical carnage historically associated with reprisals in kinetic warfare.[134] If that is true, the reduction in the physical severity of reprisals might mean civilians will be more willing to resist cyberattacks than they are to resist physical attacks.

We take up the issue of offensive civilian participation in cyberwarfare in the next section. The critical factor differentiating the two types of participation is that defensive civilian engagement is purely reactive, while offensive civilian engagement is aggressive in varying degrees. As we saw in this section, offensive civilian engagement can be part of a defensive response to a cyberattack; here, the use of offensive tactics is intended to repel an attack. It is not a bellicose act, *per se*. In the section below, we examine purely offensive civilian engagement in cyberwarfare.

(b) Offensive Engagement

---

[131] *See, e.g.,* "Warsaw Ghetto Uprising," Wikipedia, http://en.wikipedia.org/wiki/Warsaw_Ghetto_Uprising (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).

[132] *See id.* For the historical view of military reprisals against civilians who resisted their advance, *see, e.g.,* Karma Nabulsi, Traditions of War: Occupation, Resistance and the Law 27-32 (1999).

[133] *See, e.g.,* Arie J. Schaap, *Cyber Warfare Operations, supra* note 107, 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.

(notes omitted). *See also* Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyberwarfare*, *supra* note 9, at 1432; Dakota S. Rudesill, *Precision War and Responsibility: Transformational Military Technology and the Duty of Care Under the LOAC*, *supra* note 16 at 536 n. 110.

[134] *See supra* note 132.

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.'[135]

This brings us to the issue we noted earlier: the impossibility of segregating war-space and civilian-space in cyberwarfare.[136] More precisely, it brings us to the impossibility of segregating combatants and noncombatants in cyberwarfare.

The LOAC's approach to protecting civilians from the ravages of combat is predicated on segregating individuals in two ways: geographically and by role.[137] Under the LOAC, military commanders must maintain a geographical separation between battle-space and the areas where civilians are located.[138] This is a viable strategy in the physical world, but not in the virtual one. As we saw earlier, cyberspace is not a spatial phenomenon; it is an interactive overlay that eradicates the constraints of

---

[135]Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyberwarfare*, *supra* note 9, at 1432 (notes omitted). *See also* Natasha Solce, Comment, *The Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force, supra* note 104 at 297 ("ninety-five percent of the United States military's information transfers, and ninety percent of large companies' information transfers, depend upon . . . civilian networks").

The U.S. military has its own networks: NIPRNET, which is not secure, and SIPRNET, which is secure. *See, e.g.,* Josuha 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* Sean M. Condron, *Getting It Right, supra* note 115 at 407 (military networks "are vulnerable because they depend extensively on civilian networks for connectivity and transferability of information). And the Department of Defense heavily relies on commercial-off-the-shelf software, such as Microsoft products. *See, e.g.,* 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) ("U.S. military uses Microsoft Corporation products to facilitate its communications, work product, and even its [computer network attack] capabilities"). *See also* U.S. Government Accountability Office, Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks 16-18 (2004), http://www.gao.gov/cgi-bin/getrpt?GAO-94-678.

[136]*See supra* § II(B)(2).

[137]*See supra* § II(A).

[138]*See supra* § II(A).

geography.[139] The notion of separating war-space and civilian-space becomes meaningless in a context that has no boundaries, and consequently no way to prevent the two "spaces" from coinciding and interacting.[140]

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.[141] That, in turn, will make it difficult – if not impossible – to maintain the combatant-noncombatant distinction in cyberspace.

In § II(B)(2)(a), we 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 combatant and noncombatant because civilians defending "their" networks are in a position very much analogous to that of soldiers defending a fort or territory to which their country lays claim.[142] The scenarios are not, however, identical; as we saw earlier, this type of civilian participation is distinguishable from that of military combatants insofar as it is purely defensive.[143] Whether that it

---

[139]*See supra* note 104 & accompanying text. As Barlow said, cyberspace "is a world that is both everywhere and nowhere". John Perry Barlow, A Cyberspace Independence Declaration, Ibiblio, http://www.ibiblio.org/netchange/hotstuff/barlow.html.

[140]If the military used its own, dedicated systems, which civilians could not access, and if those systems were the (i) exclusive implements used to wage war and (ii) 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* notes 135 - 136 & accompanying text.

[141]*See, e.g.,* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. Rev. 1023, 1045 (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. . . .

(notes omitted). Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyberwarfare*, *supra* note 9, at 1439 ("the highly interconnected nature of the military and civilian networks . . . renders much of the Internet a dual-use target"). *See also supra* note 133. 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, 487 n. 63 (2006).

[142]*See supra* § II(B)(2)(a).

[143]*See supra* § 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/or on those affiliated with their attackers.

removes it from the category of combatant is an open question.[144]

It may not be left open. In the previous section, we examined defensive civilian participation as if it were an isolated instance: a single event in which employees of the Digi-Data-tex company protected its network from cyberattacks. If the attacks were part of a cyberwarfare campaign, they would not be an isolated event; they would be part of a larger, coordinated assault on systems throughout the United States.[145]

If U.S. computer systems become the targets of large-scale cyberwar attacks, the military will probably 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 do that is to somehow put civilians who have the ability to battle cyberattackers under the control of the military. Since battling cyberattackers will involve the use of offensive as well as defensive measures,[146] bringing civilians into this effort would result in offensive civilian engagement in cyberwarfare and directly raise the issue as to whether those civilians were now combatants.

It would also raise another issue, as we can see from this scenario: It begins with 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. That means that any cyberwarfare initiative must travel

---

[144]*See, e.g.,* Josuha E. Kastenberg, *Changing The Paradigm of Internet Access from Government Information Systems, supra* note 135 at 62 ("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 Third Geneva Convention. *See supra* note 70. If they qualified for prisoner of war status, they would presumably be considered combatants under the LOAC. *See supra* § 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* Clay Wilson, *Information Operations and Cyberwar: Capabilities and Related Policy Issues,* 4-5 Congressional Research Service (2006), http://www.fas.org/irp/crs/RL31787.pdf.

[145]*See, e.g.,* A Letter from Concerned Scientists, PBS Frontline (February 27, 2002), 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.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 71-126.

[146]*See, e.g.,* David E. Sanger, John Markoff & Thom Shanker, *U.S. Steps Up Effort on Digital Defenses,* New York Times (April 27, 2009), http://www.nytimes.com/2009/04/28/us/28cyber.html (United States is developing offensive cyberwarfare tactics). *See also* Shane Harris, *The Cyberwar Plan*, National Journal (November 14, 2009), http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (same).

across civilian-owned networks.[147] What would happen if the network owners refused 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 their being used in cyberwarfare. It is, however, quite possible that the network owners will not want their networks used as implements of war; 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 and/or for other reasons.

This brings us to the issue we address in the next section: If civilian involvement is essential for the United States to wage cyberwarfare, how do we incorporate civilians into a cyberwarfare effort? In analyzing that issue, we will assume civilians do not want to become cyberwarriors.[148] That is, we will assume that (i) civilian participation is essential if the United States is to have a cyberwarfare capability but (ii) civilians will not willingly participate in such an effort.

We realize that the second assumption is almost certainly overbroad, that many civilians will be willing to play at least some role in cyberwarfare. We addressed one aspect of willing civilian participation in the previous section; it is reasonable to assume that many civilians will have little hesitance about protecting the systems with which they are affiliated. It is also, we believe, reasonable to assume that some -- perhaps many -- civilians will not want to become Involved in cyberwarfare for the reasons noted above and/or others. If nothing else, some may be concerned about losing their status as civilians; as we noted above, those who participate in cyberwarfare may be transformed into a combatant, which makes them a legitimate target for enemy strikes.

In the next section we address the two issues this scenario creates: One is the need to incorporate recalcitrant civilians into a cyberwarfare effort; the second is the effect of such incorporation, i.e., whether it transforms a civilian into a combatant under the LOAC.[149]

III. Conscripts

> *`every 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'.*[150]

---

[147]For a cyberwarfare scenario that notes the essential role of telecommunications providers, *see, e.g.,* Doug Hanchard, *Global Cyberwar: Installed in Your PC at Home, the Office and Government,* ZD Net (October 21, 2009), http://government.zdnet.com/?p=5601.

[148]*See, e.g.,* Josuha E. Kastenberg, *Changing The Paradigm of Internet Access from Government Information Systems, supra* note 135 at 62 ("cyber warriors" is a term used "in reference to . . . civilian and military personnel who conduct cyber operations").

[149]There is a residual possibility we do not address: It is that "U.S. forces . . . [will] retaliate [against a cyberattack] through unwitting computer hosts." Clay Wilson, *Information Operations and Cyberwar, supra* note 144 at 5. We do not specifically address this issue because we assume either (i) 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 (ii) 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* § III.

[150]Pennsylvania Constitution of 1776, Article VII, http://avalon.law.yale.edu/18th_century/pa08.asp.

Governments have historically used two methods to integrate civilians into warfare: nationalization and conscription.[151] If neither is a viable way to induce civilians to participate in cyberwarfare, then we would presumably have to develop an alternative. The first two sections below examine the efficacy of each of these methods and assess the need for an alternative.[152] The third section postulates a third, more flexible option – one 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. . . .*[153]

Black's Law Dictionary defines nationalization as the "act of bringing an industry under government control".[154] The first instance of a U.S. President's nationalizing civilian property for use in a war effort apparently 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 . . . confirmed the power of the President to seize railroads and telegraph lines and provided criminal penalties for interference with Government operation.[155]

---

[151]We are seeing the rise of a third method 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 (November 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 ("Raytheon is . . . hiring more cyber warriors to help fight the digital cyber war"). We do 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 218.

[152]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 (November 17, 2009), http://www.europolitics.info/sectorial-policies/dual-usesystems-and-platforms-shared-by-civilian-and-military-sectors-art254406-13.html.

[153]Nueces Valley Town-Side Co. v. McAdoo, 257 F. 143, 143 (D. Tex. 1919).

[154]"Nationalization," Black's Law Dictionary (8th ed. 2004).

[155]Youngstown Sheet & Tube Co. v/. Sawyer, 343 U.S. 579, 685 (1952) (Vinson, C.J., dissenting) (citing War of the Rebellion, Official Records of the Union and Confederate Armies, Series I, Vol. II, pp. 603-604 (1880) & 12 Stat. 334 (1862)).

> 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.'

Since Congress eventually ratified what Lincoln had done, the issue as to whether a President has the constitutional authority to nationalize private businesses did not arise until World War I.

The United States entered the war on April 6, 1917;[156] on December 26, President Wilson took over the nation's railroads, which were simply not up to the task of transporting military personnel and war supplies.[157] He put them under the control of the Director General of the newly created United States Railroad Administration, "severing the railroads `completely' from the control and management of their civilian owners".[158]

Wilson cited three sources as authorizing 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.[159] The 1916 legislation authorized the President

---

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.* Lincoln used the seizure to ensure that rail and telegraph companies "cooperate[d] with war needs". James A. Rawley, Abraham Lincoln and 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. 334 (1862) (quoted in Francis Hoague, Russell M. Brown & Philip Marcus, *Wartime Conscription and Control of Labor,* 54 Harv. L. Rev. 50, 52 n. 5 (1940). The World War I statute that allowed President Wilson to nationalize the railroads did not include "any similar provision for the regulation of employees". *Id*. (citing 39 Stat. 645 (August 29, 1916). *See infra* notes 144 -150 & accompanying text.

[156]*See, e.g.,* ""World War I," Wikipedia, http://en.wikipedia.org/wiki/World_War_I.

[157]*See, e.g.,* 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, 224-225 (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 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. . . .

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.

[158]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. Co. v. Ault, 256 U.S. 554, 557 (1921).

[159]*See* Henry Hull, *Some Legal Aspects of Federal Control of Railways, supra* note 155 at 860.

> 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.[160]

In 1918, Congress adopted the Federal Control Act, which ratified Wilson's actions.[161] Federal control of the railroads ended on March 1, 1920.[162]

Since Congress ratified Wilson's actions, the constitutionality of a President's seizing civilian-owned businesses again never became an issue. It did become an issue in 1952, when President Truman took over the steel industry to prevent a nationwide strike by steelworkers.[163] Truman justified the seizure as necessary to continue the production of materials needed for the Korean War.[164]

The steel companies challenged his actions, ultimately taking the case to the Supreme Court.[165] 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.[166] The Supreme Court disagreed. It

---

[160]Henry Hull, *Some Legal Aspects of Federal Control of Railways, supra* note 155 at 860 (quoting Act of Aug. 29, 1916, Pub. L. No. 64-242, § 1, 39 Stat. 645).

[161]*See* Federal Control Act of 1918, ch. 25, 40 Stat. 451. *See also* Missouri Pac. R. Co. v. Ault, 256 U.S. 554, 557 (1921) (President's "authority was confirmed by the Federal Control Act . . . and the ensuing proclamation of March 29, 1918, 40 Stat. 1763").

[162]*See, e.g.,* 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).

[163]*See, e.g.,* Eric A. White, *Examining Presidential Power through the Rubric of Equity*, 108 Mich. L. Rev. 113, 143 (2009).

[164]*See id.:*

> 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.

(notes omitted) (citing Exec. Order No. 10,340, 17 Fed. Reg. 3139, 3141 (April 10, 1952)).

[165]*See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 583-584 (1952).

[166]*See* Exec. Order No. 10,340, 17 Fed. Reg. 3139, 3141 (April 10, 1952). For an account of why 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, 407 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 shutdown due to strikes. *See* U.S. v. Pewee Coal Co., 341 U.S. 114, 115-116 (1951). 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.

explained that the President's power to issue the order must derive either from an act of Congress or from the Constitution itself, and found that no statute authorized "the President to take possession of property as he did here."[167] The Court noted that not only was using "the seizure technique to solve labor disputes . . . to prevent work stoppages . . . unauthorized by any congressional enactment", Congress had previously rejected legislation that "would have authorized such governmental seizures in case of an emergency."[168]

The Supreme Court then turned to whether the Constitution itself authorized the President to take over the steel companies. 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.

> 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 with faithfulness to our constitutional system hold that the Commander in Chief . . . has the ultimate power . . . to take possession of private property . . . to keep labor disputes from stopping production. This is a job for the Nation's lawmakers. . . .[169]

The Court also rejected the argument that the President's authority derived from "the several constitutional provisions that grant executive power to the President."[170] After noting that the "Constitution is neither silent nor equivocal about who shall make laws which the President is to execute", it held that Congress, not the President, makes the laws "which the President is to execute."[171] It therefore affirmed the district court's issuing an injunction that enjoined the Secretary of Commerce from implementing the President's seizure order.[172]

Given the Supreme 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. There is currently one statute that appears to confer such authority.

See 341 U.S. 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. *See id.* at 118-119.

[167]343 U.S. at 585.

[168]*Id.*

[169]*Id.* at 587.

[170]*Id.*

[171]*Id.* at 587-588.

[172]*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).

Section 606 of Title 47 of the U.S. Code addresses the need to maintain wire and radio communications in wartime. Section 606(a) applies when the United States is already at war; it authorizes the President to order radio and/or wire communications carriers to give priority to national defense communications.[173] Section 606(d) specifically applies to "wire communication" facilities.[174] Under § 606(d), if the President proclaims that a state or threat of war involving the United States exists, he can authorize the closing of a wire communications facility or the use or control of such a facility by any department of the federal government.[175]

While § 606 seems to authorize the President to seize telecommunications networks in the event or threat of cyberwarfare, whether it actually does so depends on how we resolve two issues. The first is constitutionality: A statute must authorize a Presidential seizure of private business for the seizure to be constitutional;[176] section 606 seems to authorize such seizures, but for that authorization to be valid, § 606 must itself be constitutional. We address that issue first. If we decide § 606 is constitutional, we then must address the second issue: whether it actually justifies seizing telecommunications networks as a response to cyberwarfare.

In 1919, the Supreme Court upheld the constitutionality of the original version of what is now 47 U.S. Code § 606. On July 16, 1918, Congress adopted a joint resolution which provided, in part, that the President

> during the continuance of the present war 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. . . .[177]

---

[173]*See* 47 U.S. Code § 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"). Section 606(b) makes it a crime to "obstruct or retard" interstate or foreign communications by radio or wire. 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 or the United States and to close or take control of any station "suitable for use as a navigational aid beyond five miles".

[174]*See* 47 U.S. Code § 606(d).

[175]*See* 47 U.S. Code § 606(d). 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.

[176]*See supra* notes 170 - 172 & accompanying text.

[177]Dakota Cent. Telephone Co. v. State of South Dakota ex rel. Payne, 250 U.S. 163, 182 (1919) (quoting 40 Stat. 904, c. 154 [Comp. St. 1918, § 3115 3/4 x, appendix]). The resolution required that the owners of the systems receive "just compensation" for the takeover, such compensation to be determined by the President. *See id.* The "form of the resolution was borrowed" from the 1916 act that authorized the

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

> `necessary for the national security . . . to . . . 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 undertaken shall be exercised by and through the Postmaster General. * * *'[178]

The Postmaster General "assumed possession and control" of the telephone systems and operated them until August 1, 1919, when the seizure ended.[179]

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.[180] The companies disclaimed responsibility for the rate schedule, since they were operating under government control.[181] The case eventually reached the Supreme Court; South Dakota challenged the constitutionality of the takeover of the phone companies,[182] but the Court upheld it. The Supreme Court held that "under its war power Congress possessed the right to confer upon the President the authority which it gave him".[183] It also rejected South Dakota's argument that President Wilson

---

President to take over the railroads. *See The Telegraph Industry: Monopoly or Competition,* 51 Yale L.J. 629, 634-635 (1942).

[178]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.*

[179]*See id.* at 183. *See also The Telegraph Industry: Monopoly or Competition, supra* note 177 at 633. For how the Postmaster General operated the phone companies, *see id.* at 633-634.

[180]*See* 250 U.S. at 179-180.

[181]*See id.* at 181.

[182]*See id.* at 181.

[183]*Id.* at 183. . (c

exceeded the authority Congress conferred upon him; the Court found that Congress' resolution gave the President the authority "to take complete possession and control" of the U.S. telephone system.[184]

It seems, then, that § 606 is constitutional.[185] We will therefore proceed to the second issue noted above: whether § 606 authorizes the seizure of telecommunications networks for use in conducting cyberwarfare.

There are two issues that arguably undermine its applicability in this context. The first is definitional: Section 606 predicates the authority it confers on the existence of a state or threat of "war."[186] But as we saw earlier, whether cyberwar constitutes "war" under the current LOAC has yet to be resolved.[187] If, as seems likely, cyberwar does not constitute "war" under the LOAC, the provisions of § 606 presumably do not apply to cyberwarfare. 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,[188] the only type of warfare that then existed. It is therefore reasonable to assume that like its predecessors, the current version of § 606 only applies to kinetic war.

The definitional issue could easily be resolved: Congress could revise the relevant provisions of § 606 to make it clear that they apply to cyberwar.[189] The second issue is more intractable: whether a

---

[184]*Id.* at 184. South Dakota had argued that the resolution only authorized a partial takeover. *See id*. at 183. On another note, a state court rejected an argument that the takeover of the phone companies was an unconstitutional taking of property. *See* Read v. Central Union Tel. Co., 213 Ill. App. 246, 1919 WL 1510 *6 (Ill. App. 1919). The Illinois court held that the seizure of the companies was not a taking without due process because (i) the resolution required the payment of just compensation for the property and (ii) 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. See supra* note 166.

[185]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 Sheet and Tube Co.* Court referred to Congress' power to adopt the "laws" the President is to implement. *See supra* note 172 & accompanying text. And President Wilson's seizure of the railroads was authorized by legislation Congress adopted two years earlier. *See supra* note 159. After Wilson exercised that authority, Congress "promptly passed legislation providing in some detail" for the administration of the seizure. *See The Telegraph Industry: Monopoly or Competition, supra* note 177 at 635 (citing Federal Control Act, 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)).

[186]*See supra* notes 171 - 173 & accompanying text. Section 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". Sections 606(a) and 606(d) only apply when there is a state or threat of war. *See* 47 U.S. Code § 606.

[187]*See supra* notes 121 - 123 & accompanying text. *See also* § II(A).

[188]*See supra* note 177 & accompanying text.

[189]Congress did something similar in 1951, in response to a different technology. *See* Senate Report No. 82-549 (June 15, 1951); Oct. 24, 1951, c. 553, §§ 1, 2, 65 Stat. 611.

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.[190] It is often, but not always, a response to war;[191] as we have seen, the United States has nationalized (and sought to nationalize) businesses because they provided services or materials that were essential to the successful implementation of a war effort. The common theme in nationalizations is that the government takes control of an industry to ensure that it continues to perform its functions (sometimes with increased efficiency). [192]

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.[193] The same was true of the takeover of the phone companies; they continued to serve their civilian customers, as well as supporting the war effort.[194]

Nationalization is not transformative, i.e., it does not convert 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."[195] Conscription transforms civilians into combatants; 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, support a war effort. In nationalization, civilians remain civilians.[196]

The nationalizations that have been implemented and attempted in the United States were all predicated on utilizing the industries for their respective civilian purposes. 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.

If a President nationalized the networks that carry Internet traffic, he would not be doing so merely to ensure that they continued to function in their civilian capacity as communication facilities and, in addition, supported a cyberwarfare effort. He would probably be doing this, but he would also be

---

[190] *See supra* note 154 & accompanying text.

[191] *See, e.g.,* "Nationalization," Wikipedia, http://en.wikipedia.org/wiki/Nationalization.

[192] *See id.* (noting examples of nationalization).

[193] *See supra* note 157 & accompanying text.

[194] *See The Telegraph Industry: Monopoly or Competition, supra* note 177 at 634-636.

[195] "Draft," Black's Law Dictionary (8th ed. 2004). *See also* "Conscription," The Columbia Encyclopedia 11652 (6th ed. 2009). We take up the issue of conscription in the next section.

[196] 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. *See supra* note 155. 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. *See id.*

transforming the networks into the virtual equivalent of warplanes: While cyberwar will have consequences in the physical world, it will be fought in the virtual world. Since civilian-owned networks create and sustain cyberspace, they are the means of access to the virtual battle-space. They will carry the traffic used to implement offensive or defensive cyber-attacks, and this alters the status of the network owners and their employees.

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.[197] Under the LOAC, this means, among other things, that the networks become legitimate targets of retaliative attacks by enemy states,[198] 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.

The purposes for which a President would nationalize telecommunications networks in the event of cyberwarfare therefore at least partially exceed the authority conferred by § 606. Since the President's authority to nationalize civilian property derives from statutes, and since § 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, which is not surprising given that it involves far more than simply nationalizing an industry. We could revise § 606 so that it explicitly confers the necessary authority, but such an approach seems inadvisable given the extent to which the tactic being authorized exceeds the conceptual scope of nationalization.[199]

---

[197]*See supra* notes 63 - 72 & accompanying text, *supra*. 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 id.*

[198]*See, e.g.,* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (June 27) (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 supra* note 120.

[199]Nationalization might also be over-inclusive. 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. President Truman had a similar motive in his attempt to nationalize the steel companies; like President Wilson, he, to, wanted to ensure that a civilian industry continued to function (and, in the instance of the railroads, functioned with more efficiency) so it could support a war effort.

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 send over the Internet. *See, e.g.,* The White House – Office of the Press Secretary, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ Nationalizing the networks could therefore be overkill.

The alternative is to use a different theory. Since the goal is to incorporate civilians into a war effort, it seems reasonable to utilize the principle we rely on for that purpose. In the next section, we consider 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.[200]

B. Conscription

> *[Y]ou do not believe in the militarization of industry? . . . I do not. . . .* [201]

As noted earlier, conscription is the compulsory enlistment of civilians into the military.[202] It is a relatively recent development. For much of history sovereigns relied either on voluntary enlistment or impressment to staff their armed forces.[203] Conscription differs from impressment in that it is predicated on induction, rather than abduction: Conscription is the legal process by which civilians are formally incorporated into the military, usually for specific terms; impressment is essentially state-sponsored kidnapping.[204]

---

[200]The discussion in this section focused on telecommunications networks because they are the sole focus of 47 U.S. Code § 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 we saw in § II(B)(2), *supra,* almost any corporate entity can become a target in cyberwarfare, which means it will have to engage the enemy defensively; and as we also noted in that section, the government is also likely to need to utilize the resources of other computer-related corporate entities in waging cyberwarfare.

[201]Seymour Waldman, Death and Profits: A Study of the War Policies Commission 47 (1932) (exchange between Congressman Collins and Bernard Baruch during hearings of the War Policies Commission).

[202]"Draft," Black's Law Dictionary (8th ed. 2004). "Conscription's raison d'être is to fill the ranks of military forces to fight war." Georg Q. Flynn, Conscription and Democracy: The Draft in France, Great Britain and the United States 25 (2002).

[203]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," The Columbia Encyclopedia 23836 (2009):

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

[204]*See supra* note 203 & accompanying text (impressment). *See also* "Impressment," Wikipedia, http://en.wikipedia.org/wiki/Impressment (impressment consisted of "compelling men to serve . . . by force and without notice"). *See generally* "Impressment," Black's Law Dictionary 8th ed. 2004) (defining impressment as the "act of forcibly taking (something) for public service"). For conscription, *see, e.g.,* Casey B. Mulligan & Andrei Shleifer, *Conscription as Regulation, supra* note 203 at 88 ("the legal and regulated form of forced labor for the state"); United States v. Johnson, 314 F. Supp. 88, 89 (D. N.H. 1970) (due process requires that conscription be conducted "in strict compliance with the pertinent regulations").

1. History

Scholars trace the increased use of conscription to the rise of the nation-state and the democratization of warfare.[205] Conscription began to be used in Europe toward the end of the eighteenth century, and became increasingly popular during the nineteenth century.[206] "By the time of World War I, only the United States and Great Britain did not rely on conscription for mobilization."[207]

Great Britain adopted conscription in 1916,[208] and the United States followed suit in 1917.[209] When President Wilson signed legislation implementing the draft, Joseph Arver and five other men refused to register and were charged with violating the new conscription law.[210] 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.[211]

---

[205]*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 (rise of conscription in Europe). Prior to this, at least in Europe, war was conducted by professional soldiers and/or mercenaries, who were recruited "by impressment or bounty". *Id.* at 70. *See also id*. at 54-74.

[206]*See, e.g., id*. at 94-101. *See also* W. Hays Parks, *Air War and the Law of War*, 32 A.F. L. Rev. 1, 123 n. 378 (1990). The modern version of conscription was created during the French Revolution. *See, e.g.,* "Conscription," Wikipedia, http://en.wikipedia.org/wiki/Conscription. *See also* Michael Howard, War in European History, *supra* note 205 at 80-81.

[207]W. Hays Parks, *Air War and the Law of War, supra* at 123 n. 378.

[208]*See, e.g.,* 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). The "armies of the Continental Congress consisted almost entirely of volunteers," as did the army that existed between 1812 and the Civil War. *See, e.g.,* Jason Britt, *Unwilling Warriors: An Examination of the Power to Conscript in Peacetime*, 4 NW J. L. & Soc. Pol'y 400 ¶¶ 5-6 (2009). In 1863, President Lincoln signed conscription legislation, but evasion was rampant and the Union Army relied "overwhelmingly on volunteerism". *Id.* at ¶ 7.

[209]*See* Arver v. United States, 245 U.S. 366, 375 (1918) (Act of May 18, 1917, Public L. No. 12, 65th Congress, c. 15, 40 Stat. 76 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". 245 U.S. at 376.

[210]*See* Arver v. United States, *supra* 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").

[211]*Id.* at 376.

The district court rejected their arguments and the defendants were convicted.[212] They appealed to the Supreme Court, which also upheld the constitutionality of the conscription law. The *Arver* Court noted, initially, that Congress' 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 . . . ; . . . to make rules for the government and regulation of the land and naval forces.' Article 1, § 8. And . . . the authority 'to make all laws which shall be necessary and proper for carrying into execution the foregoing powers.' Article 1, § 8.[213]

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."[214]

> 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 conception 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.[215]

This is the only case in which the Supreme Court has addressed Congress' power to impose conscription in wartime.[216] Since the *Arver* Court upheld its power to conscript "in case of need",[217] conscription is presumptively constitutional when the nation is at war or is facing a threat of war.[218]

---

[212]*See id.* at 377.

[213]*Id.*

[214]*Id.* at 377-378.

[215]*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' power over the militia. *See id.* at 381-390. And, finally, it held that conscription did not constitute "the imposition of involuntary servitude in violation of the . . .Thirteenth Amendment". *Id*. at 390.

[216]*See, e.g.,* Jason Britt, *Unwilling Warriors: An Examination of the Power to Conscript in Peacetime, supra* note 208 at ¶ 13. Lower courts have considered, and rejected, various challenges to the constitutionality of conscription. *See id*. at ¶¶ 14-22.

[217]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 supra* note 156 & accompanying text. *See also supra* note 209.

[218]The Supreme Court has never considered whether Congress has the power to impose conscription "during a time of peace." Jason Britt, *Unwilling Warriors: An Examination of the Power to Conscript in Peacetime, supra* note 208 at ¶ 13. *See* Hamilton v. Regents of the University of California, 293 U.S. 245, 265 (1934) (Cardozo, J., concurring). *See also* United States v. O'Brien, 391 U.S. 367, 389-390 (1968) (Douglas, J., dissenting). Some lower federal courts upheld peacetime conscription, at least whenever Congress "declares that it is necessary or that an emergency exists requiring the raising of an army." Richter v. United States, 181 F.2d 591, 593-593 (9th Cir. 1950). For arguments that peacetime

2. Cyberwarfare

Whether conscription could be used to compel recalcitrant citizens to participate in cyberwar depends on how we resolve several issues.

The first is whether cyberwar constitutes "war" for the purposes of applying Congress' power to institute conscription. As we saw earlier, it is not at all clear that cyberwar constitutes war under the LOAC;[219] if it does not qualify as war, then Congress may not have the power to conscript civilians into a cyberwarfare effort.[220] The Court's decision in *Arver* was concerned with conscription when the United States was involved in a traditional, kinetic war,[221] so it at least arguably does not apply to cyberwar. And since the Supreme Court has never addressed the constitutionality of peacetime conscription,[222] we do not know if Congress has the authority to implement conscription when the United States is not engaged in kinetic warfare.[223]

There is authority for the proposition that "war" is not a unitary concept, i.e., that varying states of war can exist.[224] One line of cases deals with undeclared war; Congress implemented conscription during the Vietnam conflict without formally declaring war.[225] The Supreme Court did not address this

---

conscription may not be constitutional, *see* Jason Britt, *Unwilling Warriors: An Examination of the Power to Conscript in Peacetime, supra* note 208 at ¶¶ 51-53.

[219]*See supra* § II(B)(2).

[220]There is some authority for the proposition that Congress has the authority 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. 265, 265 (1917). Even if we assume that Congress has the power to implement peacetime conscription, that power might not extend to authorizing cyberwarfare conscription. The question would be whether the peacetime conscription authority we are hypothesizing could encompass a cyberwarfare effort. In other words, the issue to be resolved would be whether cyberwarfare, which we are assuming does not constitute "war" under the LOAC, qualifies as a peacetime activity. If we assume that Congress' 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, of course, Congress does not have the power to implement peacetime conscription, the analysis is limited to the single issue addressed in the text above.

[221]*See supra* note 217.

[222]*See supra* note 218.

[223]*See* Jason Britt, *Unwilling Warriors: An Examination of the Power to Conscript in Peacetime, supra* note 208 at ¶¶ 34-42.

[224]*See* Jason Britt, *Unwilling Warriors: An Examination of the Power to Conscript in Peacetime, supra* note 208 at ¶¶ 34-41.

[225]*See id.* at ¶ 3 n. 7 (joint resolution authorized combat involvement in Vietnam).

issue, but lower federal courts held that a state of war existed under Article 1 § 8 clause 11 of the Constitution because Congress (i) had adopted a resolution approving the use of force[226] and (ii) had ratified the President's initiatives by appropriating money "to carry out military operations in Southeast Asia" and implementing conscription knowing conscripts would be "sent to Vietnam."[227]

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.[228] 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 (not the LOAC).[229] The cases could be used to argue that Congress can authorize conscription as part of a cyberwar effort if the circumstances mirror those involved in the Vietnam conflict, i.e., if Congress authorized or ratified the use of military forces in such an effort.[230] If this argument is valid, cyberwarfare conscription would presumably be lawful under U.S. law; questions might remain, though, as to whether it was lawful under the LOAC.[231]

There is also authority for the proposition that war can be "imperfect," i.e, less than total. In *Bas v. Tingy*, 4 U.S. 37 (1800), 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. at 40-41. 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. It is more likely to involve hostilities conducted by a select few (military personnel and civilians) on each side, all of whom "act under [some type] of special authority". *See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 1-6. *See also* Nonie C. Cabana, *Cyber Attack Response: The Military in a Support Role,* Air & Space Power Journal (April 4, 2000), http://www.airpower.maxwell.af.mil/airchronicles/cc/cabana.html.

[226]*See id.*

[227]Orlando v. Laird, 443 F.2d 1039, 1042 (2d Cir. 1971). *See also* Jason Britt, *Unwilling Warriors: An Examination of the Power to Conscript in Peacetime, supra* note 208 at ¶¶ 39-40.

[228]*See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 63.

[229]*See, e.g.,* Mitchell v. Laird, 488 F.2d 611, 615 (D.C. Cir. 1973). The Vietnam era and later cases parsing "war" have also relied on other factors. *See, e.g.,* United States v. Prosperi, 573 F.Supp.2d 436, 449-455 (D. Mass. 2008). 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. *See, e.g.,* United States v. Valentine, 288 F. Supp. 957 (D.P.R. 1968). Courts cited the political question doctrine as their basis for refusing to entertain the defense. *See id.* at 984-987.

[230]*See supra* notes 226 - 227 & accompanying text. Congress might also have to authorize funding for the cyberwarfare effort. *See id.*

[231]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* § II(A).

A second issue concerns what would be involved in conscripting civilians to participate in cyberwar. Conscription has so far involved inducting civilians into the military; inductees report for duty, are sworn in as members of the U.S. military and from that point on are under military command.[232] They wear uniforms when on duty, usually live in military housing and devote their time to military pursuits.[233] Induction, in other words, is absolute; the inductee gives up his/her civilian life and becomes a solider. That, however, is almost certainly not what would be involved in using conscription to compel civilians to participate as combatants in cyberwar.

The traditional model of induction would be counterproductive in a cyberwar conscription effort. Conscription has historically been generic; as noted earlier, the goal of conscription was to induct masses of men into the military where they became the primary "engine of war."[234] The goal of cyberwar conscription would be very different: compelling civilians who have particular technical expertise and work for telecommunications and other Internet-related companies to participate in defensive and/or offensive cyberwar initiatives. The purpose is to *exploit* their civilian status, not deprive them of it. Cyberwar conscription would therefore maintain the status quo, insofar as the conscripts' professional lives are concerned; they would continue to work at their civilian jobs, and would probably continue to wear civilian clothing, instead of uniforms.[235]

Cyberwar conscription would therefore be less than absolute; it might be 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. These additional tasks would probably be cyberwar-specific; the routine tasks the conscripts continued to perform might also be cyber-war related, at least in part. So a

---

[232]*See, e.g.,* 53 Am. Jur. 2d Military and Civil Defense §§ 86-91 & 160-161. *See also* U.S. Army, Becoming a Soldier, http://www.goarmy.com/life/becoming_a_soldier.jsp; U.S. Army, "Being A Soldier, http://www.goarmy.com/life/being_a_soldier.jsp.

[233]*See id*.

[234]Audrey Kurth Cronin, *Cyber-Mobiliation: The New Levee en Masse*, 36 Parameters 77, 77-78 (2006). This was a function of the democratization of warfare. As war became a struggle between nations, it required larger armies. *See supra* note 205. *See also* Richard A. Preston, Sydney F. Wise & Herman O. Werner, Men in Arms: A History of Warfare and Its Interrelationships with Western Society 188-189 (1956) (Napoleon's victories were "due to the mass armies" which the Revolution produced).

[235]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 345-346 (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 371-372. Like the cyberwar conscripts hypothesized above, the contractors who operate drones in combat are civilians who participate in military combat. *See id*. And as Singer notes, there are concerns that these contractors can be considered illegal combatants under the LOAC. *See id. See also* § II(A), *supra. See generally* Daniel P. Ridlon, *Contractors or Illegal Combatants? The Status of Armed Contractors in Iraq*, 62 A.F. L. Rev. 199 (2008).

conscript working for a telecommunications company might find herself carrying out one of her usual tasks but on this particular occasion the task has the added function of supporting a cyberwar initiative.[236]

The semi-conscription we are hypothesizing would generate a host of legal issues. One would be whether this hybrid form of conscription is constitutional; the resolution of that issue might depend on the status of the semi-conscripts. If they are formally inducted into a branch of the military, their status would be more analogous to that of traditional conscripts; that, in turn, would make it possible to justify the effort on the grounds that it is but a variation of the type of conscription that has been held to be constitutional. If the semi-conscripts are not formally inducted into the military but 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 abridging the liberty of civilians who remain civilians.[237]

This brings us to the issue of whether Congress can conscript civilians for purposes other than directly serving in the armed forces.[238] During the Revolutionary War, Congress authorized the Continental Army to conscript services from civilians.[239] This seems to have been the only time in U.S.

---

[236]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. *See, e.g.,* The US-China Economic and Security Review Commission, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation 33 (2009). 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. 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.*, New York Times (May 30, 2009), http://www.nytimes.com/2009/05/31/us/31cyber.html.

[237]If Congress has the authority to implement peacetime conscription, this scenario might be justified as a valid exercise of that authority. *See supra* notes 218 & 220. Courts have held that military conscription does not constitute an unconstitutional violation of an individual's liberty or other interests. *See, e.g.,* United States ex rel. Zucker v. Osborne, 54 F. Supp. 984, 986-987 (D.N.Y. 1944). A few courts have held that peacetime military conscription does not impose an unconstitutional deprivation of liberty. *See, e.g.*, Etcheverry v. United States, 320 F.2d 873, 874 (9th Cir. 1963).

[238]There are cases that have upheld Congress' "power to conscript individuals for work of national importance . . . in time of war." United States ex rel. Zucker v. Osborne, *supra* note 237 at 986. These conscientious objector cases are not, though, 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). Our concern, of course, is with compelling civilians (or quasi-civilians) to support active military initiatives and/or to engage in those initiatives themselves.

[239]*See* E. James Ferguson, The Power of the Purse: A History of American Public Finance 1776-1790 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. *See 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".

history that civilians *qua* civilians were subject to a type of military conscription.[240] In the early 1920s, bills were introduced into Congress that would have authorized "a draft of labor",[241] later, other bills were introduced that would have authorized a "draft of `services'" and/or a "draft of persons in the management or control of industry", but the proposed legislation was never adopted.[242] 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' power to conscript civilians for purposes other than serving in the armed forces.[243]

See id. The certificates "were essentially IOUs", and left Congress facing massive debts after the war ended. *See id. at* 59-66. *See also* J. Gregory Sidak, *The President's Power of the Purse,* 1989 Duke L.J. 1162, 1167 n. 18 (1989) (certificates as IOUs).

It appears that the "`arbitrary and oppressive'" use of impressments during the Revolutionary War contributed to the adoption of the "Compensation Clause" of the Fifth Amendment, i.e., to modern "takings" law. *See* Jed Rubenfield, *Usings*, 102 Yale L.J. 1077, 1122-1133 (1993). *See also* Matthew P. Harrington, *Regulatory Takings and the Original Understanding of the Takings Clause*, 45 Wm. & Mary L. Rev. 2053, 2067 (2004). It seems to follow, then, that conscripting the services of a corporation (along with its property) would constitute a "taking" under the Fifth Amendment. *See, e.g.,* Yulee v. Canova, 11 Fla. 9, 1864 WL 1115 (Fla. 1864).

[240]In *Butler v. Perry*, 240 U.S. 328 (1916), the Supreme Court held that states could conscript civilians to work on roads and bridges in the county where the lived. *See* 240 U.S. at 259-260. 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. *See id*. While the *Butler* case upheld the conscription of labor, it is not relevant to the issue under consideration because it did not involve conscription for the purpose of participating in and/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.

[241]*See* Francis Hoague, Russell M. Brown & Philip Marcus, *Wartime Conscription and Control of Labor,* 54 Harv. L. Rev. 50, 61-62 (1940).

[242]*See id*. at 62-63. The bills all contemplated conscription during a time of war. *See id.* They were part of an attempt to implement a "universal draft" of all "resources, industrial organizations and services over which Government control is necessary" for the "successful termination" of a state of war. Seymour Waldman, Death and Profits: A Study of the War Policies Commission 5 (1932). The primary purpose seems to have been to "`take the profit out of war". *Id.*

[243]*See supra* note 240. It might be possible to derive the existence of such authority from Congress' power to "raise . . . Armies", but the viability of such a strategy would depend on whether we could extrapolate the concept of "Armies" 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. *See* U.S. Constitution Art. I, § 8, cl. 12. For the purposes of this analysis, we will assume 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 being debated in the 1920s, some argued that Congress has the power to conscript civilians to serve in a support role during wartime:

The obvious alternative, then, 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.[244] This would not only resolve the conscription issue, it would also resolve issues that might arise as to whether civilians (or semi-civilians) can be compelled to take orders from military officers;[245] if we induct the employees into the military, they become members of the armed forces and are clearly obligated to obey the commands of superior officers.[246]

> 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. . . . Whether it chooses to . . . execute it is another matter.

Seymour Waldman, Death and Profits: A Study of the War Policies Commission 62 (1932). The Selective Service Act of 1940 gave the government the authority to "commandeer plants" under certain circumstances. 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 (1959). Section 9 of the Selective Service Act of 1940, Pub. L. No. 783, 76th Cong., 3d Sess. (Sept. 16, 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,* 51 Yale L.J. 282, 285 (1941). 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 really seems to have authorized the President to nationalize companies.

Congress clearly realized that "commandeering" companies constituted a "taking" under the Fifth Amendment because § 309 of the Selective Service Act of 1940 stated 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 (1942).

[244]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 therefore 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).

[245]This might not become an issue: Section 802(10) of Title 10 of the U.S. Code 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 toe very punitive article in the UCMA, 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 U. Miami L. Rev. 491, 497 (2008) (notes omitted). A "contingency operation" is a "military operation" that (i) 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 (ii) results "call or order to, or retention on," of members of the armed services. 10 U.S. Code § 101(13).

[246]10 U.S. Code §§ 802 & 892.

But while this option has an appealing simplicity, it raises other issues. One is whether those who have become members of the U.S. military can continue to work for a civilian-owned company. If we induct civilians whose talents and assistance are needed in a cyberwar effort into the military, 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 we saw earlier, induction has always been total; one's status shifts from civilian to member of the armed forces. We could perhaps incorporate a version of this change in status 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.[247] That, however, might create other problems; the erstwhile employers might resist the notion of having their workforces, or a substantial part of their workforces, operating under the aegis of the military. It could also create conflicting chains of command, with the civilian management of the companies and the military officers assigned to the companies vying for control over the workforces.[248]

That brings us to another, related issue -- the question of precisely who and/or what would need to be conscripted in a cyberwar effort. As the scenario outlined above illustrates, we would effectively be conscripting a company, as well as the individuals who work for that company. The corporation that owns the telecommunication or other Internet-related business the employees of which are conscripted in a cyberwarfare effort would still own the business; but conscription would (i) limit its ability to control the company's day-to-day operations and (ii) effectively eliminate its ability to prevent the company's employees and assets from being used in cybercombat. In the analysis above, we implicitly assumed 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. The actual scope of conscription would be much broader; we would be conscripting companies rather than discrete individuals, and that brings us to the final issue we need to address in this section.

The telecommunications networks and other Internet-related businesses whose staff and assets will be essential in a cyberwarfare effort are almost certainly owned by corporations. The issue we really need to address, then, is: Can we conscript a corporation?

---

[247]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, 743 F.2d 481, 482 (8th Cir. 198). 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. The problem with this approach is that the inductees would presumably be devoting most of their time to carrying out their civilian tasks, which implies that their civilian role is the predominant role they continue to play.

We could perhaps resolve these issues by implementing a variation of the instance of 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. Department of Air Force, 999 F.2d 529, 530 (Fed. Cir. 1993). But while 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 529-530. Membership in the military is essentially a qualification for the civilian position. *See id*. The civilian and military roles are, therefore, unlikely to come into conflict.

[248]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*, 55 Harv. L. Rev. 427, 525 (1942).

There is substantial authority for the proposition that a corporation is a "person:" a "legal person" instead of a "natural person."[249] Corporations have consequently been encouraged to "assume the modern obligations of good citizenship", such as paying taxes and abiding by all applicable laws.[250] Since the law recognizes corporations as citizens who share many, if not all of the duties and obligations of citizenship,[251] it might be possible to extrapolate the doctrine of conscription so it encompasses corporate entities.

If we assume, for the purposes of analysis, that such an extrapolation would be valid, we then have to consider what corporate conscription would encompass and how it would differ from nationalization. In other words, if we assume we *can* implement corporate conscription, we then have to consider why we might want to do this and how we might go about doing it. In the remainder of this section, we analyze these two issues, in reverse order.

Although a corporation is a "person," it would not be sufficient to simply conscript the corporate entity itself. Conscripting the corporate entity, as such, 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, however, be sufficient; the government would still need to be able to compel the participation of the employees who have the expertise to carry out cyberwar activities. This means we would need to conscript (i) the corporation itself (for its assets and capabilities) and (ii) some (perhaps all) of its employees.[252] It seems more reasonable to conscript the entire "person," i.e., to conscript all of the

---

[249]*See* 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.

(notes omitted). *See, e.g.*, Citizens United v. Federal Election Com'n, 2010 WL 183856 *20, *29 (2010). *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"). *See generally* Carl J. Mayer, *Personalizing the Impersonal: Corporations and the Bill of Rights*, 41 Hastings L.J. 577 (1990).

[250]A.P. Smith Manufacturing Co. v . Barlow, 98 A.2d 581, 586 (N.J. 1953).

[251]*See supra* note 249.

[252]Some might argue that it would only be necessary to conscript the employees who have the skills needed to launch and/or repel cyberattacks, but that would no doubt be inadequate. The employees who can engage in cyberwar would not be able to do so unless the other employees (whose efforts are essential to its functioning) 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 generally American Economic Mobilization*, 55 Harv. L. Rev. 427, 525 (1942) (notes omitted).

corporate assets and all of its employees. Corporate conscription would therefore be collective conscription. If we conscripted the WorldWeb Telecommunications Corporation, we would be conscripting all of WorldWeb's assets and employees.[253] Corporate conscription would also probably be less than absolute, i.e., would probably resemble the semi-conscription of corporate employees we hypothesized earlier. The corporation would continue to carry out its civilian functions but would on occasion be obliged to participate in cyberwar operations.

Now we come to why we might want to implement corporate conscription. One reason is that it should resolve the conflicting chain of command issues noted earlier by conscripting all of the corporation's employees – management as well as staff.[254] If managers and executives were conscripted, they, too, would be required to obey orders given by the military personnel who had taken charge of the company; that should discourage, if not eliminate, the possibility of conflicting directives from corporate management. Another, related reason is that conscripting the corporation puts it under military control and transforms it, in part, into an implement of war; that, in turn, should make it possible for the military to use the corporate conscripts effectively in cyberwar activities.

There are disadvantages, as well. One is that military personnel would presumably (i) assume control of the corporation (so they can order employees to participate in cyberwar efforts when necessary) or (ii) have the ability to assume such control on very short notice (for the same reason).[255] In either event, military control could interfere with the corporation's ability to carry out its civilian functions effectively, thereby creating a "takings" issue.[256] It could also transform the corporation into a "combatant" under the LOAC, making it a legitimate target for retaliative attacks by a cyber-enemy. This could create a new "takings" issue or exacerbate the effects of the original issue.[257]

There are no doubt other advantages and disadvantages of corporate conscription, as well as other implementation issues we would have to resolve if we adopted this alternative. Our goal is not to attempt

---

[253]*See supra* note 166. We would also be conscripting all of its assets, but we analyze the conscription of corporate property later in this section.

[254]*See supra* note 245.

[255]In "commandeering" companies under the Selective Service Act of 1940, the government relied "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*, 55 Harv. L. Rev. 427, 525 (1942) (notes 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 he put the railroads under the control of the Director General of the new United States Railroad Administration. *See supra* notes 178 & 158 & accompanying text. 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 network and other companies is to utilize their capabilities directly in cybercombat, the seizure should be implement by the military.

[256]*See supra* note 166. We also discuss that issue later in this section.

[257]*See supra* note 166. We also discuss that issue later in this section. 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 255 at 530-535.

to identify and analyze every issue raised by conscripting corporations to participate in cyberwarfare; it is to analyze the permissibility and utility of utilizing corporate conscription as an alternative to nationalization. That discrete goal is, of course, part of a larger undertaking: determining if nationalization or conscription is a satisfactory way of compelling civilian participation in cyberwarfare. We assess their respective suitability for this task and the potential need for another alternative in the next section.

C. A Third Option

As we saw in the previous two sections, 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 ability to take over companies and operate them as part of a war effort, but the government is limited to operating the companies in their civilian capacity. Nationalization does not authorize the government to transform businesses into implements of war or, perhaps more accurately, into combatants.

Conscription gives the government the ability to transform civilians into members of the armed forces. It is not clear if the government's power to conscript civilians encompasses corporations; even if does, implementing conscription becomes problematic for several reasons. One is that, as we saw in the previous section, conscription has traditionally been absolute; it transforms a civilian into a combatant. In conscripting corporations to participate in cyberwar, the government would not want to transform most, if not all, of the companies into combatants, exclusively. It would want them to play a dual role by continuing to provide civilian services and/or products and by participating in cyberwar activities when and to the extent necessary. The first problem with corporate conscription, then, is that conscription has historically not encompassed a civilian, as well as a military, role.

The other problem is, as we saw in the previous section, that a corporation is a collective entity: It is composed of the corporate structure and assets, which are distinct to the corporate entity; but it is also composed of a population of civilian employees, which raises questions about the scope of corporate conscription. If we conscript a corporation, does that automatically conscript all of its employees, as well? If not, does the government then have to conscript those employees into the military?

All of these issues can be resolved. One option is to develop a new concept: a fusion of nationalization and conscription. Another, probably superior approach is to utilize a version of the National Guard – a customized, Cyberwar National Guard.[258] Structurally and operationally, the

---

[258]We could, instead, call the new organization the Cyber Militia, because its structure and function would be quite analogous to the common law militia. As the Illinois Supreme Court explained in *Dunne v. People,* 94 Ill. 120, 138 (Ill. 1879),

> 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.

Cyberwar National Guard would be more analogous to the common law militia than to the contemporary National Guard; unlike the National Guard, which operates according to formal procedures which are analogous to those employed by the U.S. military, the Cyberwar National Guard (or Militia) would necessarily be a more *ad hoc* enterprise. It would, for one thing, not be feasible to call members of the Cyberwar National Guard (CNG) into service for specific periods of time and give them notice as to when they were to report for duty; they, like the members of the common law militias, would have to be ready to serve as soon as they were called into action, and for only as long as they were needed.[259] It is this flexibility that makes a Cyberwar National Guard (or Cyber Militia) an advantageous way to approach the task of incorporating civilians into cyberwar; civilians become combatants when and for as long as needed, and then resume their status of noncombatants.[260]

In *Perpich v. Department of Defense,* 496 U.S. 334 (1990), the Supreme Court noted that modern National Guard members "continue to satisfy this description of a militia" because have both a "civilian hat" and "an army hat – only one of which is worn at any particular time." 496 U.S. at 348.

The Cyber National Guard postulated in the text would be distinct from the U.S. Air Force's Cyber Command and a similar unit proposed by the U.S. Army. *See, e.g.,* Michael Cheek, *Air Force Cyber Command to Go Operational,* The New New Internet (January 27, 2010), http://www.thenewnewinternet.com/2010/01/27/air-force-cyber-command-to-go-operational/; Amber Corrin, *Army Mulls Realignment to Fortify Cybercommand,* Federal Computer Week (January 15, 2010), http://fcw.com/Articles/2010/01/15/Army-mulls-realignment-to-fortify-cyber-command.aspx; Bob Brewin, *Here Comes the Navy Cyber Forces*, Nextgov (January 11, 2010), http://whatsbrewin.nextgov.com/2010/01/here_comes_the_navy_cyber_forces.php?oref=latest_posts. The Department of Defense is also seeking to create its own cybercommand. *See, e.g.,* Sean Gallagher, *New Threats Compel DOD to Rethink Cyber Strategy*, Federal Computer Week (January 25, 2010), http://fcw.com/articles/2010/01/25/cover-story-long-cyber-march.aspx. The Air Force, Army and Navy cyber commands would be composed of members of the U.S. military; the Department of Defense cyber command would apparently be staffed by members of the military and by civilian employees and contractors. *See id*.

[259]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 v. Department of Defense, *supra,* 496 U.S. at 341 (citing 1 Stat. 271). In adopting the statute, Congress acted pursuant to the authority conferred on it by Article I, § 8 cl. 15 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, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 165-174.

[260]This also distinguishes it from the Cyber Force proposed by another author. *See also* Natasha Solce, Comment, *The Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force, supra* note 104 at 313-318. The Cyber Force, as outlined in this article, would be a new military branch – the cyber-equivalent of the Army, Air Force, Marines and Navy. *See id*. This author believe 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. *See id*. As we have explained, we do not see this as a desirable or even an optimal approach to cyberwarfare; unless we intend to militarize every aspect of our society, cyberwarfare will inevitably target civilian-owned entities. We therefore believe the appropriate approach is to return to the historical strategy that was devised to deal with what we might call pervasive

How would we incorporate CNG members into the U.S. military? We could employ a version of the procedure the National Guard utilizes: When someone joins the National Guard, he/she becomes "part of the Enlisted Reserve Corps of the Army".[261] If we created the CNG and required those working for businesses that are likely to have strategic importance in cyberwar to join it,[262] that would give us an efficient way to bring these employees under military control if and when the need arose.

When the President called the CNG units to active duty, they would become members of the U.S. military.[263] There would be certain differences between the two: Unlike National Guard members, who can be called up for long terms, CNG members might only be needed for days, or even hours. We would call them up for only for as long as their participation was needed; once the attack or other military necessity ended, we could release them from active duty until we needed to re-activate them.[264] This would not only create an efficient, flexible way to bring corporate employees under military control, it could at least arguably mitigate the extent to which they (and, perhaps, their corporate employer) were regarded as combatants under the LOAC. The members of the CNG would not be persistent members of the U.S. military; they would be occasional members for the periods when cyberwar was raging and they

---

war, i.e., with combat that occurs when there is no segregation between war-space and civilian-space. *See* notes 96 - 97 & accompanying text, *supra*.

[261]Perpich v. Department of Defense, *supra,* 496 U.S. at 345.

[262]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. *See* note 247 *supra*. We could, perhaps, declare certain types of business as essential to our cyberwar effort and therefore make Cyberwar National Guard membership a prerequisite for being hired. If we imposed this requirement on categories of businesses, that should reduce the possibility that people would seek employment from another company in order to avoid having to join the CNG.

[263]The CNG would have to differ from the National Guard in one important respect. The National Guard has two components: The state National Guards and 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 the United States. *See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 172. *See also* "National Guard of the United States," Wikipedia, http://en.wikipedia.org/wiki/National_Guard_of_the_United_States. "With the consent of state governors," members of a state National Guard unit can be deployed as "federally recognized armed force members", which means they lose their status as members of their state National Guard and become members of the National Guard of the United States. *See, e.g.,* "National Guard of the United States, Wikipedia, *supra.* *See also* Susan W. Brenner, Cyber Threats, *supra* note 10 at 172. 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. *See, e.g.,* "National Guard of the United States, Wikipedia, *supra;* Susan W. Brenner, Cyber Threats, *supra* note 10 at 172. *See also* supra note 262.

[264]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 235.

had been called to active duty. During those times, they would be combatants under the LOAC.[265] At all other times, they would be civilians – pure noncombatants. This might mean that under the LOAC, the company, and its employees, would not be legitimate targets for retaliative strikes when the employees were not on active duty with the CNG.[266]

This strategy should also solve the conflicting chain of command issues we examined earlier. If all of a company's employees are required to be members of the CNG, they would all be subject to military command once -- and for as long as -- they are called to active duty. Logically, then, this should eliminate any opportunity for conflicting civilian-military commands.

IV. Conclusion

---

[265]An issue that could arise as to the combatant status of CNG members who were on active duty is the requirement that combatants identity themselves as such by wearing "the uniform assigned to the regular, uniformed armed units of a" party to the war being waged. Protocol, *supra* note 58 at Article 44(7). *See supra* note 71 & accompanying text. 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 cyber-battle 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 their *bona fides* as lawful combatants under the LOAC. Unless we devise a way to equip bits and bytes with "uniforms," this aspect of the LOAC logically cannot, and probably should not, apply to cyberwarfare. *See, e.g.,* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 Berkeley J. Int'l L. 192, 196 (2009) (""There are no flags . . . in a cyber attack"); Mark R. Shulman, *Discrimination in the Laws of Information Warfare*, 37 Colum. J. Transnat'l L. 939, 956 (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.

[266]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 1977 Protocol to the Geneva Conventions states that it is "illegal to kill, injure or capture an adversary by resort to perfidy." Article 37(1), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1977), *supra* note 58. Article 37(1) defines perfidy as involving various types of deception, one of which is "the feigning of civilian, non-combatant status". *Id.*

An antagonistic nation might claim that CNG members are simply feigning non-combatant 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 non-combatants at all times other than those when they had been activated as members of the United States 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, e.g.,* Geoffrey Best, War and Law Since 1945 288-293 (1997). The United States could also point out that Article 37(1)'s ban on perfidy would not apply to the activities CNG members carry out when they have been activated because they would not seek to, nor would they, "kill, injure or capture" any of their adversaries . . . assuming, of course, that as "adversary" is defined as a human being. 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, e.g.,* Geoffrey Best, War and Law Since 1945, *supra,* at 288-293.

. . . to . . . fight and win . . . in . . . cyberspace.[267]

The issues we analyze in this article may seem speculative and implausible – something out of a bad science fiction story – but they most decidedly are not.[268] The issues we address are the product of two unrelated but interacting forces: One is our ever-increasing dependence on cyberspace as the vector for our activities; as civilian pursuits move into cyberspace, military strategy adapts by seeking ways to exploit cyberspace for martial purposes. We addressed this phenomenon in §§ I and II(B)(2), *supra*.

The other force is the evolving symbiosis between the military and certain civilians that originated in the physical world and has begun to migrate into the virtual world of cyberspace. In the physical world, the civilians involved in this symbiosis fall into two categories: mercenaries and contractors.

A "mercenary" is essentially someone "who accepts money or some benefit for military service."[269] Mercenaries are not members of the regular armed forces of any recognized nation; they fight for money, not for loyalty to a country or a cause.[270]

Mercenaries' role in history is far from insignificant. As one author notes, they "have played a role in warfare, to varying degrees, throughout most of history."[271] The first reported use of mercenaries occurred in the twentieth century BCE; their use continued for over three millennia but declined and had essentially disappeared by the early twentieth century.[272] The decline in the use of mercenaries was due to the rise of the nation-state, which was triggered by the Peace of Westphalia in 1648.[273] Nation-states tended to view "mercenaries as unreliable with questionable loyalty."[274]

---

[267]United States Air Force Mission, U.S. Air Force, http://www.airforce.com/learn-about/our-mission/.

[268]*See, e.g.,* Major General Charles J. Dunlap, Jr., *Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-warriors*, 87 Neb. L. Rev. at 723 ("Cyberspace has evolved . . . to the point that science fiction has become more science than fiction").

[269]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 Rev. 609, 615 (2009). For a more detailed definition, *see* Protocol, *supra* note 58 at Article 47.

[270]*See, e.g.,* "Mercenary," Wikipedia, http://en.wikipedia.org/wiki/Mercenary.

[271]Captain Daniel P. Ridlon, *Contractors or Illegal Combatants? The Status of Armed Contractors in Iraq*, 62 A.F. L. Rev. 199, 211 (2008).

[272]*See id.* at 209-212.

[273]*See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 10 at 201-215 (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).

[274]Captain Daniel P. Ridlon, *Contractors or Illegal Combatants? The Status of Armed Contractors in Iraq, supra* note 271 at 211. As to why nation-states viewed them with distrust while prior sovereigns had not, *see* Susan W. Brenner, Cyber Threats, *supra* note 10 at 201-215

Notwithstanding this, a resurgence in the use of mercenaries began after World War II; it started in Africa, where decolonization left many "governments vulnerable to insurgents who were quick to employ skilled mercenaries."[275] The use of mercenaries continued through the twentieth century and accelerated in the first decade of the twenty-first century.[276] 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."[277] That, as one author noted, "places the United States at the forefront of military outsourcing."[278] Mercenaries, however, are not the only manifestation of military outsourcing.

Like mercenaries, contractors work for pay, not out of loyalty to a cause or country.[279] Some commentators claim that mercenaries and contractors differ in certain respects; others reject the significance of these differences and contend that the two are indistinguishable for all practical purposes.[280] For our purposes, we divide contractors into two categories: (i) those who provide support services to the military but do not participate in combat; [281] and (ii) those who participate in combat.[282] Some argue that contractors who participate in combat are functionally indistinguishable from

---

[275]*See* Captain Daniel P. Ridlon, *Contractors or Illegal Combatants? The Status of Armed Contractors in Iraq, supra* note 271 at 211-212.

[276]*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, 468 (2007) (noting increasing use of mercenaries since 1969).

[277]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).

[278]*Id*. at 290.

[279]Contractors are often citizens of the countries whose militaries they serve, and therefore may have an allegiance to that country in their personal lives. Their professional work for the military, on the other hand, tends to be purely the product of a business arrangement.

[280]*See, e.g.,* Zoe Salzman, *Private Military Contractors and the Taint of a Mercenary Reputation,* 40 N.Y.U.J. Int'l & Pol. 853, 887-889 (2008) (rejecting the argument that contractors differ from mercenaries because they (i) operate from within a corporate structure and/or (ii) "work only for legitimate states"). *See also* 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).

[281]*See, e.g.,* E.L. Gaston, *Mercenarism 2.0? The Rise of the Modern Private Security Industry and Its Implications for International Humanitarian Law Enforcement, supra* note 280 at 225 ("firms 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").

[282]*See, e.g.,* E.L. Gaston, *Mercenarism 2.0? The Rise of the Modern Private Security Industry and Its Implications for International Humanitarian Law Enforcement, supra* note 280 at 225-226 ("private 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.,* Martha Minow. *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy*, 46 B.C. L. Rev. 989, 1015-1016 (2005).

mercenaries, so they are subject to the LOAC.[283] The use of both types of contractors raises difficult questions under the LOAC,[284] issues we will not address here.

For our purposes, the significance of the United States' increasing reliance on mercenaries and/or 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".[285] One 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."[286] A second reason is the emphasis on outsourcing, which began in the 1950s and accelerated as the century drew to an end; as a result, Department of Defense policy now "requires the military departments to utilize commercial support whenever appropriate".[287] The third reason is what one author calls "cradle to grave contracting", which is in large part a function of the increasing complexity of military technology.[288] As she explains,

> [h]istorically, the private sector would . . . develop technology and then relinquish it to the military. . . .
>
> [M]ost 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.[289]

Contractors have been an integral part of the last Iraq war and the war in Afghanistan, providing support services from behind the lines and even accompanying troops into the field.[290]

The bifurcation between civilians and combatants that once existed and upon which the LOAC is predicated has been eroding for years and is well on its way to disappearing in the physical world. The

---

[283] *See, e.g.,* Zoe Salzman, *Private Military Contractors and the Taint of a Mercenary Reputation, supra* note 280 at 880-890.

[284] *See, 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, 257-262 (2008).

[285] 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, supra* note 277 at 290.

[286] Rebecca Rafferty Vernon, *Battlefield Contractors: Facing the Tough Issues,* 33 Pub. Cont. L.J. 369, 374-375(2004).

[287] *Id.* at 376 (citing DoD, Directive 4100.15, Commercial Activities Program ¶ 4.4 (Mar. 3, 1989)).

[288] *See id.* at 377-378.

[289] *See id.* at 377-378 (notes omitted).

[290] *See, e.g.,* David Isenberg, *A Fistful of Contractors*, Research Report – British American Security Information Council 21 (2004), http://www.basicint.org/pubs/Research/2004PMC.htm (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").

accelerating use of contractors is increasingly a function of the factor noted above: the military's use of technology, especially information technology.[291] The military's use of technology forces it to rely on contractors because (i) civilian-owned entities develop and control the technology;[292] and (ii) "the technology of modern warfare often exceeds the ability of militaries to train their personnel" to operate it.[293]

Cyberwar is the next, perhaps ultimate, step in this trend. In the physical realm of combat, the military relies on civilians to develop, implement and operate technologies the sole purpose of which is to wage kinetic war. That circumscribes the scope of civilian involvement and means such involvement can be purely voluntary; the financial rewards of providing and supporting military technology are enough to ensure that interested civilians and civilian-owned entities will step forward to meet the military's needs. There is therefore no need to compel civilian participation with nationalization or conscription.

The cyberwar dynamic is very different. As we saw earlier, cyberspace supersedes the constraints of physical reality and, in so doing, makes it impossible to segregate war-space and civilian-space.[294] Cyberwar will not be fought on a sequestered battlefield occupied by military personnel and civilian contractors; it will be fought in civilian-space. Cyberattackers may target some military systems (especially military systems designed to counter a cyberattack), but their primary targets will be civilian-owned and -operated businesses; utilities owned and operated by local governments may also be one of their primary targets. In effect, cyberwar will be total war; there will be no principled distinction between combatants and non-combatants and between military and civilian targets.[295]

Cyberwar will therefore take the process of integrating civilians into warfare to the next level. Since civilian-owned technology will *be* the battlefield, those who wage cyberwar must have access to the

---

[291]*See, e.g.,* Mark Calaguas, *Military Privatization: Efficiency or Anarchy?,* 6 Chi.-Kent J. Int'l & Comp. L. 58, 63-64 (2006). *See also* P.W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry 62-63 (2003).

[292]*See* Mark Calaguas, *Military Privatization: Efficiency or Anarchy?, supra* note 291 at 63 ("civilian ingenuity, coupled with the rapid pace of development, has [given] non-state entities . . .greater access to technology than the government "). The military has hired contractors to develop the weaponry needed for cyberwar. *See, e.g.,* David E. Sanger, John Markoff & Thom Shanker, *U.S. Steps Up Effort on Digital Defenses,* New York Times (April 27, 2009), http://www.nytimes.com/2009/04/28/us/28cyber.html?pagewanted=1&_r=1

[293]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). *See also id.*

> 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.

[294]*See supra* §§ I & II(B)(2).

[295]*See supra* § I. *See also supra* §§ I & II(B)(2).

technology being used by a particular civilian entity and be able to operate it. The military cannot do that for several reasons. One is that it does not have enough personnel – let alone enough technologically adept personnel – to take on this task. A second, related reason is that even if the military had appropriately trained personnel who could operate the propriety technology used by a particular target, it would not be able to deploy them quickly enough for the response to be effective. In the physical world, militaries can have days, even weeks to regroup and deploy troops; cyberattacks occur in milliseconds.[296] The solution is to have cyberwarriors who are in place on site and ready to be activated.

And while the military *might* have a cadre of personnel who were trained in the use of computer technology, the military cannot train its personnel to operate the technology that will be in use in all of the civilian-owned entities that will become part of a cyberwar battlespace. Many entities will be using idiosyncratic technology or customized versions of commercial-off-the-shelf (COTS) technology. Given the range and number of civilian systems that would at least potentially comprise the U.S. cyberwar battlespace, the military could not deploy troops who would be able to master these technologies, assuming, of course, that civilians would cooperate in allowing them to do so.

This is all moot because the U.S. military cannot, and will not be able to, 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. Aside from anything else, the military cannot compete with the private sector; many of its potential cyberwarriors will opt for the private sector, where they can earn more money and enjoy more personal autonomy.[297]

It seems the only solution is the one we explore in this article: integrating civilians into the military to create an on-site force that is present in every entity that could be drawn into the cyber-battle-space and that is prepared to engage in offensive and/or defensive cyberwarfare whenever activated We are accustomed to consigning war to a distinct, professional military force, but that approach is something of an historical aberration. 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."[298] The "freemen" were called into duty when there was a threat of invasion and then released once the emergency had been dealt with. This system originally known as the fyrd evolved into the militia system, which British colonists brought to this country and which became the basis of the colonial military system.[299] The National Guard is the lineal descendant of the militia; our CNG is, to a great extent, the 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. These territorially based sovereign entities established and

---

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

[297]*See, e.g.,* Christopher Drew & John Markoff, *Contractors Vie for Plum Work, Hacking for U.S., supra* note 236.

[298]M.M. Knappen, *Constitutional and Legal History of England* 36 (1942).

[299]*See, e.g.,* James B. Whisker, The Rise and Decline of the American Militia System 12 (1999).

maintained fixed physical boundaries, which introduced a level of predictability and stability into warfare. Nation-states organized permanent, professional military forces and assigned them the task of maintaining the integrity of their respective borders; an attack on a state's sovereignty usually took the form of an assault upon the territory it controlled. The goal of war often was to seize control of all or a part of the territory another nation-state controlled. The military's primary task was to discourage and, when necessary, repeal intrusions into the territory their sovereign controlled; a subsidiary task was to launch offensive attacks on the territory of other nation-states.

This, as we have explained elsewhere,[300] effectively divided threats into two types: internal (crime) and external (war). Professional law enforcement organizations evolved to deal with internal threats, while the military dealt with external threats. Law enforcement dealt with civilians; the military dealt with other militaries. This is particularly true in the United States, which carefully differentiates the two functions.

Cyberspace is not a physical construct. It is, as we saw earlier,[301] essentially a fourth dimension that overlays the three physical dimensions that have historically been the sole venue for human activities. Since cyberspace is not a physical construct, it cannot be divided up into sovereign "territories," each demarcated by identifiable, stable borders. That, as we have seen,[302] has certain consequences for the law and tactics of warfare. For our purposes, 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.'"[303] Unlike Hobbes' state of nature, cyberspace is populated by individuals who 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 law 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. We believe the approach we have proposed here – a virtual analog of the militia – is one way of achieving such a system.

---

[300]*See* Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. Marshall J. Computer & Info. L. 659, 660-666 (2005). Susan W. Brenner, Cyber Threats, *supra* note 10 at 201-226. The discussion that follows in the text is taken from these sources.

[301]*See supra* note 100.

[302]*See supra* § I. *See also supra* §§ I & II(B)(2).

[303]McAfee, In the Crossfire: Critical Infrastructure in the Age of Cyber War, *supra* note 3 at 25.