SMU Science and Technology Law Review

Volume 13 | Number 3 Article 2

January 2010

Civilians in Cyberwarfare: Casualties

Susan W. Brenner

Leo L. Clarke

Civilians in Cyberwarfare: Casualties

Susan W. Brenner & Leo L. Clarke***

I. INTRODUCTION[1]

According to one estimate, 140 nations have, or are in the process of developing, the capacity to wage cyberwarfare.[2] Other countries will no doubt follow suit. A 2009 global survey of IT and security 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 cyber attacks."[3]

While cyberwarfare will probably not displace traditional kinetic warfare,[4] it will become an increasingly important weapon in the arsenals of nation-states for several reasons. One of the primary reasons is cost: developing the capacity to wage cyberwar is inexpensive as compared to the cost of developing and maintaining the capacity to wage twenty-first century ki-

---

* NCR Distinguished Professor of Law & Technology, University of Dayton School of Law. E-mail: susanwbrenner@yahoo.com.

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

1. The authors gratefully acknowledge the invaluable contributions Ms. Alison Gaughenbaugh, JD 2011 University of Dayton School of Law, made to the research and writing of this article.

2. *See, e.g.*, Kevin Coleman, *The Cyber Arms Race Has Begun*, CSO ONLINE, Jan. 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, Nov.29, 2007, http://www.itpreport.com/default.asp?Mode=Show&A=1421&R=GL (stating 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, (2007), http://www.fas.org/sgp/crs/natsec/RL31787.pdf.

3. MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 26 (2009), http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf. Fifty percent of the executives "identified the United States as one of the three countries 'most vulnerable to critical infrastructure cyberattack'." *Id.* at 30.

4. "Kinetic" warfare "involve[s] the forces and energy of moving bodies, including physical damage to or destruction of targets through use of bombs, missiles, bullets, and similar projectiles." Air Force Glossary, Air Force Doctrine Document 1-2 57, http://www.docstoc.com/docs/12530146/Air-Force-Glossary (Jan. 11, 2007). 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), *available at https://www.afresearch.org/skins/rims/display.aspx?moduleid=BE0e99f3-fc56-4ccb-8dfe-670c0822a153&mode=user&action=researchproject&objectid=E6bcf0d2-6096-41a0-b0bb-e425864be6ca.*

netic war.[5] Since cyberwarfare will for the most part be waged over publicly accessible networks,[6] the expense involved primarily encompasses training and paying cyberwarriors, as well as purchasing and maintaining the hardware and software they will need to launch and counter cyber attacks.

In a recent article, we examined the need to involve civilians in cyberwarfare and the legal devices government can use to compel such involvement when necessary.[7] In this article, we explore how law can and should address the consequences of involving civilians in cyberwarfare. First, we consider how civilians are likely to respond to their roles as willing or unwilling combatants, and how they can mitigate the risks that status creates. Second, we consider how the law should allocate the risks of civilian combat between the civilians and the polity in general.

The context of our analysis is the large corporations and institutions that are likely to have the most at stake and to be the most affected by cyberwar. Those civilian combatants will include (1) for-profit entities such as financial institutions, telecommunications and transportation companies, utilities, major internet sellers, and brick and mortar companies crucial to the distribution of the goods and services that characterize American life and (2) non-profit institutions from state and local government agencies, to hospitals, universities, and school districts. Indeed, if one accepts the very reasonable premise that cyberwar is waged not primarily for territory or wealth, but for political and cultural advantage, no segment of American culture can expect to escape casualties in cyberwar. This is especially true given the frequency and severity of cyberwars that experts anticipate over the next few decades.

Our article is divided into three parts. Part I addresses preliminary questions: What is the difference between civilian and conscript status? Whether the risk of cyberwar casualty is materially different from the risk of cybercrime and other IT hazards? And how will civilian executives react to threats of cyberwar? We argue that, from the civilian's perspective, cyberwar presents different hazards than the IT security risks presented by private hackers and other cybercriminals. We also argue that, even if the threats to the civilian's assets are the same, the risk of potential extensive governmen-

5. *See, e.g.*, MARTIN C. LIBICKI, RAND CORPORATION, CYBERDETERRENCE AND CYBERWAR xvi, 177 (2009), http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf; 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.

6. *See* section II *infra*.

7. *See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, VAND. J. TRANSNAT'L L. (forthcoming 2010) hereinafter "*Conscripts*."

tal regulation—or even conscription—requires a program of readiness and response that differs materially from current IT security programs.

Part II analyzes the risks to civilians if their operations are disrupted by either their status as combatants or victims. We identify the risks of legal liability to shareholders, customers, suppliers, and other stakeholders as well as the broader issues of political and reputational risk and consider how civilians might manage those risks. We also consider the possibility of tort and contract theories and conclude that tort remedies will probably be limited by the economic loss doctrine, and that contract remedies will depend on relative bargaining power. As to suppliers, we conclude that most large enterprises will be able to shift the risk of their non-performance, or malperformance, caused by cyber attacks to their customers by means of contractual limitations on liability. However, civilians whose operations involve risks to property and life may have to seek special legislation or wait for the development of viable insurance.

Part III examines the extent to which civilians can recoup economic losses from cyberwar. In light of the prevalence of contractual disclaimers and limitations in the economy, the general unavailability of adequate insurance, and the low probability that Congress will establish a publicly funded compensation fund, we conclude that the primary battleground will be the Fifth Amendment to the U.S. Constitution. The primary issue we address is whether the Constitution requires the federal government to compensate civilians for their costs and losses in the course of cyber combat, including the costs of devoting their personnel, equipment, and other assets—especially intellectual property—to the country's cyberwar effort. We conclude that the Takings Clause of the Fifth Amendment is unlikely to provide a remedy to civilians for the costs and losses imposed by government regulation or conscription, except in the case of a non-regulatory procurement well in advance of an attack.

II. Should Civilians Worry About Becoming Casualties?

A. The Casualties of Cyberwar: Civilians and Combatants

1. How a Civilian Entity Becomes a Casualty

A civilian can suffer direct casualties from a cyberwar in many ways and for many reasons. How the casualty occurs will affect both the civilian's approach to loss management, and its potential rights to compensation. We will therefore offer some brief and simple examples of how casualties might occur so the reader can put cyberwar risk into a context that allows comparison with more traditional risks.

First, a civilian can be a direct target of a cyberwar attack because an attack on the civilian would directly accomplish a strategic or tactical goal of the aggressor. For example, a foreign government might target the website of a university because a faculty member is an outspoken opponent of the government's treatment of a minority. An attack could also target a civilian that is perceived as an exploiter of the country's resources.

Second, the civilian could be a target because it is a means of attacking others. For example, an electric utility could be targeted to affect a power grid that supplies a telecommunications company used to attack the attacker. Or a transportation system could be subjected to repeated, apparently random attacks to create a loss of confidence in the government. Similarly, hospital or school databases could be attacked to disrupt activities at the heart of American personal security.

Third, a civilian can be an indirect victim. For example, an attack on Federal Express that disrupts its services could cause lawyers to miss filing deadlines. Attacks on banks could cause liquidity crises throughout the economy. Successful attacks on county tax or deeds databases could disrupt real property transfers.

Fourth, a civilian can become a victim not of a cyberwar attack, but of its own government's response to the attack. Here are just three examples:

(1) The government might impose new and costly regulations to deter or defend against attacks.[8]

(2) The government could allocate resources, such as telecommunications satellite capacity, in a manner that destroys a civilian's contract rights or otherwise disrupts the civilian's normal business operations.

(3) The government might conscript specific assets or even the civilian's entire enterprise.[9]

Fifth, a civilian can become a combatant because it perceives that participation in the cyberwar can further its own interests. Alternatively, the government conscripts the civilian and thrusts it into the combat zone. As we demonstrated in *Conscripts*, the difference between combatants and civilians, while traditionally distinct in kinetic warfare, is more nebulous in the context of cyberwar.[10] For example, if a telecommunications company refuses to cooperate with any government-sponsored attack beyond providing business services that it has already contractually committed to provide, including those to governmental cyber-defense contractors, is it a combatant or a civilian?

Note the difference here from traditional kinetic warfare. The telecommunications company is not comparable to the telephone company that carries communications to the Pentagon, nor is it clearly analogous to the airline company that delivers troops to the Western front. Rather, its services might be a combination of the two; it will unwittingly deliver some packets of information outside the combat zone and some in the execution of an attack. Because of these ambiguities, we believe that a civilian that is aware it is participating in activities that are supportive of, even if not essential to,

8. The USA PATRIOT Act, 18 U.S.C. § 1 *et seq.* (2006) is a good example of such a response.

9. Brenner & Clarke, *supra* note 7, (forthcoming 2010) (manuscript at 41–54, on file with author).

10. *Id.*

cyberwar, should consider itself a combatant, for that is clearly how it will be perceived by opposing nations. In short, such a quasi-combatant essentially assumes the risk that it will become a direct target of a cyber attack and therefore should manage that risk just as any other direct target.

2. The Peculiar Status of Conscripts

Like Elvis Presley or Muhammad Ali, conscripted civilians face the risk that the government will not employ their talents to the highest and best use, and that conscription will impose both short-term and long-term adverse consequences. During the period of conscription, injuries could occur that permanently reduce future income streams and adversely affect business plans. In addition, the conscription of assets will undoubtedly result in lost opportunities to expand existing business, develop new products, and enter new markets. Unlike the civilian, the conscript is not free to change its mind about participation in the war or how it manages cyberwar risk. But that loss of freedom does not distinguish the institutional conscript from the individual conscript.

Our notion that institutions can be conscripted to assist in cyberwar defense or attacks, however, also creates some unprecedented practical issues regarding casualty risk. The fundamental issue is to define exactly what rights the government acquires by conscription. In the case of an individual who is drafted, we have a fairly intuitive idea of what he or she gives up and what the military acquires. The conscript submits his body and, to a certain extent, his personality and individual freedom to military control, but he does not surrender his property and assets that are discrete from his person.

Organizations are different, however. Corporations and other legal entities—whether for profit, non-profit, or municipal—are often treated as the equivalents of natural persons and even possess some of the same constitutional rights as individuals.[11] In reality, however, a corporation is simply a congeries of assets or, as corporate law scholars proclaim, a "nexus of contracts."[12] A corporation does not have a body that can serve as the manifestation of the thing conscripted. Thus, one of the fundamental decisions that Congress will have to make, if it considers conscription as a possible means of dealing with cyberwar, is how the military will define what is being conscripted. Is it a legal entity as a whole, specific assets (e.g., patents or equipment), lines of business (e.g., cellular phone operations in specific states), or functions (e.g., software design and development, IT security, or power grid management)?

We believe that the most practicable approach to this issue is an analog to individual conscription. The genius of the modern business organization

11. *See* Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876, 900 (2010).

12. *See, e.g.*, Stephen M. Bainbridge, *The Board of Directors as Nexus of Contracts*, 88 IOWA L. REV. 1, 6 (2002) (discussing the view that the board of directors is really a nexus of contracts, from which its powers flow).

is its ability to combine the resources necessary to accomplish tasks that cannot be accomplished by individuals. The need to conscript talent to fight cyberwars requires that the individuals be able to accomplish tasks similar to what they undertake in civilian life. This combination of human capacity and capital (including specialized equipment, intellectual property, and "community know-how") is the organizational equivalent to the natural person, with his or her inherent physical and mental capabilities. Thus, a conscription order should identify specific employees (e.g., by their names, titles, or functions) and require turnover or access to the equipment and capital required to perform their usual duties.

Just as drafting Elvis did not bring the Army his pink Cadillac or Graceland, conscription of the assets of Microsoft should not bring with it those assets unrelated to its ability to perform the conscripted services—unrelated intellectual property, cash, real estate, and line or staff operations. To conscript more assets than needed would only impose unnecessary management burdens on the military, and deprive stakeholders of more of their investments than are necessary to accomplish the purpose of conscription.

If this approach was adopted, it would be preferable for analytical purposes to refer to the conscripted assets (employees and related capital) as though they constituted a single person (civilian) separate from the larger organization from which they came. Whether the military should also conscript the relevant employees in their individual capacities raises issues that are both beyond the scope of this article and unnecessary to decide. Although we envision that it would be most efficient for the military to treat the senior executive responsible for the functions conscripted as the senior officer or the "brain" of the conscripted "person," we also leave that discussion for another day.

B. Does Cyberwar Risk Differ From Cybercrime Risk?

Before analyzing how civilians should respond to the casualty risk of cyberwar, we must first consider whether cyberwar requires a different civilian response than common cybercrime. After all, most civilians have a substantial IT security program in place to combat routine cybercrime intrusions and those lacking such prophylactic measures likely do not care about cyberwar.[13] A civilian who has a sophisticated security program might be indifferent to the threat of cyberwar. Civilian IT managers could reasonably argue that whether or not it is necessary to distinguish between attacks resulting from a basement hacker, commercial espionage or theft, cyber extortion, or full-fledged cyberwar. When protecting a civilian's systems, data, and communication abilities, a security manager might believe that identifying the motive behind or source of a cyber attack is a waste of time and re-

13. The authors have argued elsewhere previously that such security programs should be mandated by law. S. Brenner and L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. OF COMP. & INFO. L. 659, 659 (2005).

sources. This attitude has always influenced targets' willingness to report criminal intrusions and explains victims' lack of enthusiasm for cooperating with law enforcement—once the target has been identified and the threat has been neutralized, the problem becomes someone else's.

Paradoxically, security managers could also argue that a cyberwar is less threatening than other forms of cyber attacks because governments combat cyberwars with more resources than are devoted towards fighting cybercrimes. Further, jurisdictional limits greatly hamper a civilian's protection against cybercrime.[14] Moreover, few law enforcement resources are devoted towards fighting cybercrimes.[15] The Federal government is able to devote more and better resources to defend cyber attacks than it does to "mere" cybercrime, for which law enforcement resources are spread notoriously thin and greatly hampered by jurisdictional limits.[16] Thus, in contrast, the federal government takes cyberwar seriously.[17] As a result, IT managers often shrug off the threat of cyberwar as just consultant hype, believing that the government's sound security principles will adequately address the risks.[18]

C. The Risks and Consequences of Cyberwar Require a Civilian Response

Civilian governance is not likely to share the same indifference towards cyberwar that IT managers may have. Corporate executives have broader responsibilities than just protecting IT assets. They must also seek to increase stakeholder value over both short-term and long-term horizons. However, cyberwar presents unusual short and long-term risks for the civilian enterprise. Because of virtually unlimited resources available to governments, government sponsored cyber attacks on civilians' interests may be frequent, prolonged, and severe. Also, American patriotism is likely to tie cyberwar with the broader public interests, affecting corporate reputation and brands, as well as business and employee relationships. Furthermore, the costs and benefits of governmental regulation will be markedly different than those of private cybercriminals who target only civilians for economic purposes. Third, and most importantly, the risk of conscription, as will be described below, creates interesting issues for corporate governance.

---

14. *See id.* at 669–70.

15. *See id.* at 667–68.

16. In contrast, the federal government, at least, is taking cyberwar seriously. *See, e.g.*, Shane Harris, *The Cyberwar Plan*, NAT'L J. MAG., Nov. 14, 2009 (describing U.S. military's efforts to "hire cyberwarriors"), *available at* http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php.

17. *See id.*

18. *See, e.g.*, Evgeny Morozov, *Battling the Cyber Warmongers*, WALL ST. J., May 10, 2010, at W3, *available at* http://online.wsj.com/article/SB10001424052748704370704575228653351323986.html.

1. The Duties and Motivations of Executives

So what approach should executives take toward cyberwar risk? A good starting point is the executives' fiduciary duty under the law of the civilian's jurisdiction.[19] The Model Business Corporations Act, for example, proscribes that a director or officer of a corporation is relieved of liability if she "act[s] in good faith" and "in a manner [she] reasonably believes to be in the best interests of the corporation."[20] Many courts often direct the triers-of-fact to determine whether a breach of duty occurred given the common-law "business judgment rule" ("BJR").[21] Under the BJR, there exists "a presumption that in making a business decision, the director of a corporation acted on an informed basis, in good faith, and in the honest belief that the action taken was in the best interest of the company."[22] The presumption is eliminated if illegality, fraud, or a conflict of interest existed.[23]

Under the BJR, executives face little risk of personal liability for their inadequate responses to cyberwarfare. Many states also permit corporations to limit shareholders' rights for breach of duty to injunctive relief.[24] Furthermore, most sizable corporations provide executives with insurance that protects them against shareholder claims for breach of the duty of care.[25]

---

19. For non-governmental entities, this is usually the jurisdiction in which the entity is incorporated or otherwise chartered. *See, e.g.*, Folkes v. Cent. of Ga. Ry. Co., 80 So. 458 (Ala. 1918) (precluding a suit in an Alabama court because it was incorporated in another state). The following discussion focuses on non-governmental civilians. For "governmental" civilians, such as schools and state and local governments, one could substitute a discussion of political or public responsibility. In neither case is the executive likely to be motivated by threats of personal liability for damages, but rather by career and reputational interest.

20. Model Bus. Corp. Act, § 8.30, 8.42. (2002).

21. *See, e.g.*, Gantler v. Stephens, 965 A.2d 695, 704–06 (Del. 2009); *see also* Lees Inn of Am. v. William R. Lee Irrevocable Trust, 924 N.E.2d 143, 157 (Ind. Ct. App. 2010).

22. *Lees Inn*, 924 N.E.2d at 157.

23. *See* Shlensky v. Wrigley, 237 N.E.2d 776, 780 (Ill. App. Ct. 1968) (concluding a suit against corporate directors was not sustainable because nothing improper was alleged).

24. *See, e.g.*, Harnett v. Billman, 800 F.2d 1308, 1316 (4th Cir. 1986) (concluding a minority shareholder was limited to injunctive relief in a breach of fiduciary duty suit).

25. For a thorough discussion of this insurance, *see* Bennett L. Ross, *Protecting Corporate Directors and Officers: Insurance and Other Alternatives*, 40 VAND. L. REV. 775, 775 (1987) (evaluating the effectiveness of Directors & Officers policies and its substitutes; *see also* Model Bus. Corp. Act. § 8.57 (2002).

For publicly held companies, the Sarbanes-Oxley Act of 2002 ("SOX") supplements the minimal duties required by the BJR.[26] SOX requires the chief executive officer of a covered civilian to certify the adequacy of the company's internal controls affecting external financial reporting.[27] Because information technology plays such a crucial role in the recording and reporting of financial information, the adequacy of a company's information security program is considered in SOX compliance determinations.[28] While analysis of the impact of SOX is beyond the scope of this article, it is evident that SOX has motivated executives to carefully address the threat of cyberwars.

Although a concern for personal liability is unlikely to motivate an executive, executives may still be motivated by the broader concept of "corporate responsibility" in proactively responding to cyberwars. For example, an executive may consider the deleterious effects on her company's own IT systems and assets as well as the potential risks to strategic partners, suppliers, and customers. Because executives have no legal duty to maximize profit, non-financial exposure to cyberwar should be contemplated as well. At a fundamental level, executives can and should consider not just the value of the civilian's own IT systems and assets, but also the risks to strategic partners, suppliers, and customers because detrimental effects on such parties could ultimately adversely affect the civilian's own financial welfare. Moreover, executives can take in to account even non-financial exposures. Contrary to some ideological views of the responsibility of corporate management, executives have no legal duty to maximize long or short term profits.[29] Instead, major corporations routinely profess commitment to goals that extend beyond achieving competitive financial returns and long-term stability.[30]

These realities mean that executives are likely to respond to the threat of cyberwars more proactively than would be justified by mere concern for IT values. Protecting a company's current asset values might require that an executive do more than raise barriers to competitive entry using the most cost-effective means. She might also need to protect the company's reputa-

26. Sarbanes-Oxley Act of 2002, PL 107-204, 15 U.S.C. § 7262 (2006). The Act and the regulations implementing the Act are complex. For an explanation and critique of the Act, *see*, Roberta Romano, *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance*, 114 YALE L.J. 1521 (2004).

27. *See* 15 U.S.C. § 7262.

28. *See id.*

29. *See* Leo L. Clarke, Bruce P. Frohnen & Edward C. Lyons, *The Practical Soul of Business Ethics: The Corporate Manager's Dilemma and the Social Teaching of the Catholic Church*, 29 SEATTLE U. L. REV. 139, 149–63 (2005) (arguing that corporations have neither a legal nor an ethical duty to maximize profits).

30. *Id.* at 151–53.

tion for good corporate citizenship by cooperating with governmental authorities and by protecting the interests of strategic partners, suppliers, and customers.

For example, larger companies—especially companies in regulated industries and publically-held companies—often incur costs that cannot be justified based on strict profit-maximization. Executives of these companies recognize the long-term value of government cooperation as well as the benefits of good public relations.[31] Thus, executives can act consistently with their fiduciary duties even if they comply with governmental pressure. Another possibility is that executives can be overly concerned with the potential liability of their suppliers, customers, and other third parties to the threat of cyberwar. In short, civilian executives have extremely broad discretion in responding to cyberwars in a fashion that reflects their evaluation of all risks.

As a result of these factors, executives will likely consider an intrusion into a civilian's IT system to be of paramount importance in determining the many resources that should be devoted towards countering these attacks. The executives will probably promulgate written policies and procedures that address at least the following key issues: detection and reporting of attempted intrusions, whether intrusions are related to other intrusions into the civilian's system or part of a larger cyber attack, and how to execute an appropriate response.

2. Possible Executive Approaches to the Risk of Conscription

Economic reasons often prompt civilians to disregard the threat of cybercrime. When evaluated in terms of severity and frequency, the costs of prevention and prosecution are greater than actual losses. However, if we are correct in our conclusion that cyberwar will result in conscription of civilians to defend—and perhaps to launch—attacks,[32] then executives must change their economic calculus. After all, a conscript will no means to avert the combat and will not be able to avoid the related costs. And once a conscription law is passed, civilian managers would have a fiduciary duty to prepare the civilian to respond to and comply with the conscription law.[33] The risk that a civilian's work force, equipment, and intangible assets could be usurped by the government would, especially for a large enterprise, require extensive contingency planning, regardless of government compensation. In

31. This inclination is demonstrated by the prevalence of corporate philanthropy, despite the views of such notable critics as Warren Buffett. Buffett believes that shareholders, not corporate managers, should determine the amount and destination of corporate profits to be used for charitable purposes. *See* Lawrence A. Cunningham, *The Essays of Warren Buffett: Lessons For Corporate America*, 19 CARDOZO L. REV. 5, 47–54 (1997).

32. *See* Brenner & Clarke, *supra* note 7, (manuscript at 63–67).

33. *See In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 966–70 (Del. Ch. 1996).

a sense, the risk of conscription would supplant IT risk as the motivating force to treat cyberwar differently from cybercrime.

III. Dealing With the Threat of Cyberwar: Risk-Based Responses

A. Risk-Management Principles

Our discussion in Part I indicates that civilians will engage in a broad calculus in determining the optimal response to cyberwar. A common methodology for managing cyber-risk is to identify the risks the institution faces, assess the magnitude of those risks, and then attempt to prevent, mitigate, or shift them so that their impact on the institution is deemed acceptable in light of the institution's goals and risk tolerance.[34]

The first step, risk identification, requires that the civilian identify each way in which a cyber attack could adversely affect the civilian. Such negative effects include adverse impacts on its operations, its financial condition and prospects, its potential legal liabilities, its dealings with government, and the effects on the public at large.[35] "Operational risk" is sometimes used to refer to the impact of cyberwar on the civilian's operations and its ability to generate revenues and profits. Because of the breadth of the definition of "operational risk" and the virtually unlimited different types of businesses affected by cyberwar, discussion of this risk is beyond the scope of this article. We will, however, generally address "legal," "political," and "reputational" risks.

"Legal risk" refers to the possibility that the civilian will be held liable to third parties because of a failure to defend against a cyber attack or participate in a counterattack. "Political risk" refers to the risk that the civilian's response or lack of response to the threat of cyberwar will result in government regulation, whether by legislation or administrative action. "Reputational risk" refers to the potential impact on a civilian's brands and goodwill.[36] This risk is even harder to quantify than political risk. It has an even more attenuated relationship to reality and generally has a shorter half-life unless the perceived damage caused by the civilian is sufficient to destroy a brand.

The second step, risk quantification, involves analysis of the probabilities that a risk event will occur and an estimate of the damage that the civilian will suffer if the risk event occurs.[37] The determinative factors used in this calculation are often referred to as frequency and severity.[38] For exam-

34. *See* James S. Mullarney, *Arming Yourself, Quantification Strategies*, *in* Scott K. Lange et al., *e-risk*: Liabilities in a Wired World (2000).

35. *See id.* at 179.

36. *Id.* at 183.

37. *Id.* at 185.

38. *Id.*

ple, a denial-of-service attack that affected an internet seller for three hours would cause a certain loss of revenue and perhaps a certain reputational harm that may affect future business. An estimated loss is determined by multiplying the range of dollar loss expected from the attack and is multiplied by the probability that such an attack will occur.[39]

The civilian would conduct similar evaluations for all potential attacks. Similarly, a hospital would analyze the potential of an attack that could result in loss or corruption of medical records, which in turn could lead to significant personal injuries and resulting lawsuits and liabilities. Water-treatment facilities would measure the frequency and severity of attacks that might allow the introduction of contaminants into the community water supply. The probability of each scenario and the resulting harm are obviously matters of great speculation given our lack of loss-history, but the risk quantification is essential to effective risk management.[40]

The third step in this risk-management approach is to identify and implement risk reduction, mitigation, and shifting mechanisms that will allow the civilian to reduce the risk of loss to an acceptable level.[41] Risk reduction in this context entails primarily IT security measures aimed at preventing intrusions into a civilian's IT system since the civilian has no control over the sources of potential cyber attacks and very little control over the means of delivery of such attacks (typically the telecommunications systems that underlie the Internet). Risk mitigation focuses on reducing the harm that would flow from an intrusion or from other adverse impacts on a civilian from a disruption in its operations or revenues from a successful cyber attack on its vendors or customers.

Risk shifting involves agreements or legislation that either (1) relieves the civilian from liability for harm that would otherwise be imposed, or (2) requires another party to compensate the civilian for its loss. Examples of the first type of risk shifting are common contractual provisions such as force majeure clauses, limitation on liability clauses, liquidated damages clauses, and legislative immunities and exemptions. Examples of the latter are indemnity agreements and insurance contracts.

Any of these diverse risks could cause catastrophic damages to any number of civilians. In some cases the casualties might be random while in others cases, the casualties may be industry-wide or even economy-wide. How should civilian management address these risks? In the remainder of this Part, we will provide some examples of how civilians might employ these principles to manage the risks of cyberwar casualties.

---

39. *See id.* at 189.

40. Mullarney, *supra* note 34, at 186.

41. *Id.* at 189–90.

B. Legal Risk of Third-Party Claims for Cyberwar Damage

1. Contract liability

At present, a civilian does not have a statutory obligation to participate in a cyber defense or attack. Yet the civilian's response to the cyberwar might affect its relationships, contractual or otherwise, with third parties. For example, a bank has a duty to its customers to honor properly presented payment orders.[42] Similarly, utilities have regulatory and contractual duties to provide services to customers on terms set out in tariffs or contracts.[43]

One aspect of legal risk is that an attack—or a civilian's defense against that attack, or its participation in a counter-attack—may cause the civilian to breach its promise to provide goods or services (e.g., electricity, internet access, water) to its customers.[44] Many civilians attempt to avoid such risk by including in their contracts or tariffs an "act-of-God" or "force-majeure" clause. These clauses disclaim any liability for failure to perform the contract because of events or forces beyond the control of the civilian, including war, government regulations, a labor strike, and a failure of utilities.[45] Given the new and seldom understood nature of cyberwars, however, it is entirely possible that a civilian's exculpatory force-majeure provision will not include cyberwar, which constitutes neither war nor insurrection as such terms are traditionally understood. In the absence of such a specific contractual provision, it is likely that a court would apply some variant of the "impossibility" doctrine, which considers whether the cause of the breach was foreseeable and unavoidable.[46] Although it might be possible for a civilian with a solid IT security program to build a case under the impossibility doctrine, courts are not sympathetic.[47]

---

42. U.C.C. § 4A-209 (2007).

43. *See, e.g.*, Con Edison: Rates and Tariffs, http://www.coned.com/rates/ (last visited May 22, 2010).

44. Attacks that are intended to disrupt online services are typically referred to as "denial-of-service attacks." Cyber attacks can also, of course, disrupt services in the physical world—from the inability of a bank branch to verify funds on deposit so that it can honor a validly drawn and presented check to the inability of a natural gas company to access pipelines so that it can deliver gas to its customers.

45. For examples of such a clause, *see* Clauses and Explanations: *Force Majeure*, http://www.library.yale.edu/~llicense/forcecls.shtml (last visited May 29, 2010). For a discussion of the enforceability of force majeure clauses, *see* Edward H. Bergin, Force Majeure And Impossibility Of Performance (2009), *Jones Walker E*Bulletin* September 17, 8 http://www.texasbarjoneswalker.com/flashdrive/materials/business_law_section_cle/Business&Corporate_Bergin_Article.pdfnews-publications-551.html (last visited August 14, 2010).

46. *See* RESTATEMENT (SECOND) OF CONTRACTS § 261 (1981).

47. *See, e.g.*, Am. Trading & Prod. Corp. v. Shell Int'l. Marine, 453 F.2d 939, 942 (2d Cir. 1972) (finding an ocean carrier not discharged of its obligation to de-

The civilian's failure to provide services as a result of damage caused by cyberwar or by the diversion of resources to support a counterattack also creates the specter of liability for consequential damages. For example, the failure to provide adequate IT security to thwart an attack can create disruptions in services with far-reaching consequences along the lines of the "for want of a nail" nursery rhyme that could destroy the civilian.[48] Similarly, private data could be misappropriated and then released, violating contractual undertakings.

These risks sound worse than they are because virtually all civilians disclaim or limit liability for consequential damages, and such disclaimers and limits are generally enforceable regardless of their reasonableness.[49] Therefore, a civilian's failure to defend against an attack or its inept participation in a defense or counterattack is unlikely to result in substantial liability for consequential damage to customers if its contractual limitations apply and are enforceable under applicable law.

How should the existence of these contractual legal risks affect management's attitude toward cyberwars? There are five responses that should be adopted as a matter of course and which should already be in place in some fashion to deal with general security threats. First, management should carefully evaluate IT security's requests for resources since a civilian that is employing anything short of state-of-the-art defenses can hardly claim that it was "impossible" to perform its contracts.

Second, the legal department should be instructed to draft customer and supplier contracts to ensure that the contracts accurately include cyberwar as a force majeure. Third, the civilian should conduct an analysis of its ability to prove the factual predicates of the force majeure defense. Fourth, the civilian should document the nature of threats as they occur to show that any resulting claims can be traced to the unforeseen cause.

Fifth, the civilian's insurance coverage should be reviewed to determine whether risk of liability can be shifted to an insurer. Although breach of contract is typically not insurable and losses from "war" are not insurable, coverage may be available for losses caused by third-party torts even if the liability arises from a contract. Moreover, the civilian may wish to investigate the availability of business-interruption insurance, which would cover the loss of revenue caused by an inability to perform.

---

liver goods because of the closing of the Suez Canal on account of the Six Day War of 1967 because alternative routes, although more expensive, were available for the carrier when traversing through the Suez Canal was not part of the agreement); *see also* Transatlantic Fin. Corp. v. U.S., 363 F.2d 312, 315 (D.C. Cir. 1966) (another Suez closing case in which the court found no force majeure when impossibility was urged based only on expense).

48. *See, e.g.*, Hadley v. Baxendale, 156 Eng. Rep. 145 (1854) (The classic law-school case is in which a carrier's failure to timely deliver a broken mill shaft led to a substantial loss of profits.).

49. *See, e.g.*, U.C.C. § 2–719 (2004).

Cyber attacks can also present contractual legal risks of an entirely new nature. Because cyber attacks are not always economically motivated and can be aimed at wreaking general havoc, it is certainly possible that cyber attackers will not just disrupt existing contractual relationships but also create contractual obligations where none exist. For example, a cyber-attacker could change the terms of service and legal disclaimers on websites and click-wrap agreements by eliminating disclaimers or adding promises, thereby creating liabilities where none existed.[50]

Another possible scenario is an attack on a broker or dealer that transfers investment securities to or from the broker's customers, without the customer's authorization, to the attacker's accounts at foreign banks. Or an airline's schedules and ticketing could be manipulated so that seats are sold on non-existent flights or flight times are randomly changed. One can easily imagine the resulting chaos.

Each of these contingencies would create what would look to the injured party and to the courts as a breach of contract. Banks, airlines, utilities, and other sellers of goods and services have virtually vitiated the contractual rights of their customers so that sellers have very little risk for non-performance.[51] But the elimination of key disclaimers or the addition of specific warranties could create huge liabilities for civilians in targeted industries. Although the civilian might argue that the contract is voidable under the doctrine of "unilateral mistake," that doctrine usually requires that the other party (here, the customer) was at least aware of the fact that the contract did not actually represent the intention of the civilian.[52] That element would presumably be difficult to prove unless the resulting deal was too good to be true.[53]

---

50. For example, one can imagine a situation where cyber attackers changed the "terms of use" of a website or terms of a "click-wrap" agreement to eliminate disclaimers of liability for consequential damages. After all, how often does *anyone* read those terms? Absent a controlling statute, the elimination of the disclaimer would put the civilian in the situation of having to defend claims for consequential damages on the grounds that the damages were not reasonably foreseeable from the breach of contract. The ability of a bank or a utility, for example, to make that argument successfully is far from a certainty.

51. *See* Leo L. Clarke, *Performance Risk, Form Contracts and UCITA*, 7 MICH. TELECOMM. & TECH. L. REV. 1, 14-15 (2001), *available at* http://www.mttlr.org/volseven/clarke.html.

52. RESTATEMENT (SECOND) OF CONTRACTS § 153 (1981).

53. Of course, the attacker could create situations where the civilian did not breach contracts, but instead bestowed windfalls on customers, for example, by changing software to under-price goods or services. The civilian's ability to recoup such windfalls through the usual vehicle of restitution (also called unjust enrichment) might be foiled by the customer's lack of knowledge and by the civilian's own failure to prevent the attack.

How should management respond to such a legal risk? Again, better IT security is one answer, but security alone is rarely sufficient. Similarly, by definition, contract language cannot protect against such attacks. Instead, perhaps the best response might be extremely diligent surveillance of attacks and detection of their impacts in order to limit the amount of damage. The possibility of risk shifting through insurance should also be considered.

2. Managing the Risk of Tort Liability

For present purposes, we can define a tort as an act or omission that does not arise from a contract that gives rise to civil liability. Usually, the imposition of tort liability depends on a wrongful act or omission in violation of a duty imposed by law, although civilians engaged in "ultra-hazardous activity" might be held strictly liable for injuries arising from that activity.[54] Cyber attacks can result in tort liability for the civilian because the attack directly damages the civilian's property or operations in such a way that third parties are damaged by the civilian. Or an attack could be directed at a target other than the civilian, but the attack would affect the civilian's relationships with third parties in a way that causes harm to the third parties.

An example of the former would be an attack on a utility that causes a power substation to explode or a water treatment plant to release contaminated water into the city water supply. Examples of the latter would be attacks on a traffic control system that increases the risk of collisions between a civilian's planes or trucks and third parties or an attack on a utility that causes a hospital to lose connectivity with its records database or key medical equipment. Scenarios of tort liability are almost limitless given the pervasiveness of internet use in American commerce.

In light of the universe of potential risks, the typical response of a civilian to potential cyberwars would be to use reasonable efforts to avoid or mitigate third-party harm and to buy liability insurance. Whether or not insurance will be available depends, as indicated above, on whether the insurer has excluded damage caused by cyberwars.

Cyber attacks also present a non-traditional-tort legal risk, just as was the case with contractual legal risk. Most tortious conduct occurs in the ordinary course of human events—whether business or leisure. Thus, the putative tortfeasor, here the civilian, must balance the utility of the act or omission versus the potential for harm and resulting liability.

This balancing is unlikely to occur in the present context, however, because the initiating cause—the cyber-attacker—cares not a whit about social

54. *See, e.g.*, RESTATEMENT OF TORTS § 521 (1938). The most recent version of the restatement cites these activities as "abnormally dangerous." RESTATEMENT (THIRD) OF TORTS § 20 (2005). Violation of a duty imposed by contract does not usually give rise to tort liability. *See, e.g.*, Bellevue S. Assoc. v. HRH Constr. Corp., 579 N.E. 2d 195, 196 (N.Y. 1991) (holding that the owner of a housing project could not recover on a products liability theory against a contractor).

utility or risk of harm and the civilian is a victim with no real control over resulting harm. Instead, the civilian is likely to be held liable for the resulting harm only because its failure to prevent the effects of the attack violated its duty to use due care and the resulting harm was foreseeable enough to constitute a "proximate cause" of the resulting harm.

In this regard, civilians should be aware of the potential that putative plaintiffs—those harmed by the civilian's product or property as affected by the attack—will likely resort to theories of "secondary liability" to collect damages from the civilian.[55] The Restatement of Torts recognizes three varieties of such liability:

> § 876. Persons Acting In Concert
> For harm resulting to a third person from the tortious conduct of another, one is subject to liability if he
>
> (a) does a tortious act in concert with the other or pursuant to a common design with him, or
>
> (b) knows that the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other so to conduct himself, or
>
> (c) gives substantial assistance to the other in accomplishing a tortious result and his own conduct, separately considered, constitutes a breach of duty to the third person.[56]

Note that this section assumes that the harm underlying the claim for damages results from the tortious conduct of the cyber attacker and not that of the civilian. This means that the civilian can be held liable for severe wrongs (such as wrongful death) even though its own wrongful conduct is mere negligence in failing to prevent access to its systems.[57]

The most likely theories will be "aiding and abetting" and "acting in concert." The former requires proof that the civilian had "actual knowledge" of the attack and "substantially assisted" it.[58] The elements of acting in concert are even more amorphous: simple assistance with a separate breach of duty, which might include something as trivial as allowing access to the civilian's systems (substantial assistance), combined with a failure to maintain the privacy of information (breach of duty).

---

55. *See* RESTATEMENT (SECOND) OF TORTS § 876 (1979) (imposes participant liability using theories of conspiracy, aiding and abetting, and "acting in concert").

56. *Id.*

57. *See, e.g.*, Halberstam v. Welch, 705 F.2d 472, 488 (D.C. Cir. 1983) (wife held liable for wrongful death of doctor murdered by her burglar husband, where she was generally aware that her husband's income resulted from burglaries and assisted her husband in conducting them).

58. *See* Richard C. Mason, *Civil Liability for Aiding and Abetting*, 61 BUS. LAW. 1135, 1146–47 (2006).

Many courts disfavor such attenuated theories of liability[59] and narrow the reach of the doctrines by focusing on whether the alleged participant was acting in the ordinary course of its business and just grinding out "grist for the mill."[60]

Thus, to the extent a civilian did not know of the plans of the attacker or act out of its ordinary course of business in failing to detect the intrusion or attempting to mitigate its effects, a court might hold that Section 876 liability was not warranted.[61] On the other hand the Seventh Circuit, in an *en banc* decision delivered by Judge Posner, recently adopted a broad brush approach to participant liability in a case seeking to impose participant liability on defendants alleged to have funded terrorist organizations that were allegedly responsible for the murder of an American-Israeli citizen.[62] Because the plaintiff in that case alleged that the defendants knew that the parties they funded were involved in financing terrorism, the cyberwar context is not directly analogous to *Boim v. Holy Land Foundation for Relief & Development*. But the case still raises the possibility that a civilian that ignores the risk of cyberwars will not escape at least the expense of litigating claims that arise because of its failure to take prophylactic action.

C. Political Risk of Cyberwar

1. Political Risk in General

Civilians will also evaluate the political risk inherent in any response to cyberwar. Political risk takes a variety of forms, but for the purposes of this article, the focus will be on the risk that the government will take adverse actions as a result of a civilian's failure to follow actions "suggested" by a regulator. Political risk can be far more costly than legal liability risk because its effects are pervasive, prospective, and potentially perpetual. Stated differently, liability to even a large number of customers tends to be a one-time hit to the bottom line, whereas a political response tends to impose entity-wide compliance costs that carry over, even after the risk of attack has been reasonably addressed.

Therefore, although political risk is less quantifiable than legal risk, it may be more significant because the primary targets of cyberwars—including financial institutions, utilities, telecommunications companies, common carriers, and health care providers—are all heavily regulated. Regulation creates a substantially greater political risk for targets, because regulators

59. *See* Casey v. U.S. Bank Nat'l Ass'n., 26 Cal. Rptr. 3d. 401, 412 (Cal. Ct. App. 2005); *see also In re* Sharp Int'l Corp., 403 F.3d 43, 52–53 (2d Cir. 2005).

60. *See, e.g.*, Woodward v. Metro Bank of Dallas, 522 F.2d 84, 96 (5th Cir. 1975).

61. *See, e.g.*, Fletcher v. Atex, Inc., 68 F.3d. 1451, 1465–66 (2d. Cir. 1995) (holding the requisite standard of knowledge was not met in an action against keyboard manufacturers for stress injuries).

62. Boim v. Holy Land Found. for Relief & Dev., 549 F.3d 685, 692–694, 704 (7th Cir. 2008).

have such broad discretion that they can retaliate for a civilian's failure to cooperate with the defense of a cyber attack. Prevalent examples of regulatory-risk events include denials of applications for regulatory approvals or licenses, delays in application processing, approvals subject to burdensome or unanticipated conditions, and unanticipated enforcement actions or sanctions for violations.

For this reason alone, it can be expected that regulated civilians will generally cooperate with governmental regulators, unless the risks of cooperation approach those of non-cooperation. One factor that will weigh against cooperation is the extent to which the civilian operates in jurisdictions with conflicting interests. For example, China is considered a probable cyber-belligerent force against the United States. A U.S.-based multinational entity with substantial connections with China, including valuable franchises in China, and perhaps even a large percentage of its stock held by the Chinese government, may be unwilling to cooperate fully with the United States in defending cyber attacks. Instead, its response to U.S. government encouragement may be, "We would love to cooperate, but we must respect our stakeholders' interests first."

Moreover, cooperation with one government may violate regulations or comparable policies of other governments. For example, a U.S. regulatory agency may request that a civilian provide government investigators with information about suppliers or customers that may have obtained unauthorized access to the civilian's IT system, and such a request could violate European Union privacy regulations. Similarly, a decision by a telecommunications network to terminate service for an alleged attacker, or to carry counter-attack packets for the United States, may violate the terms of its franchise in other countries where transmitting or receiving equipment is located.

In light of these considerations, civilian cooperation with governments will be circumscribed by the fact that political risk cannot be evaluated on a nation-by-nation basis. Political risk analysis must take into account the materiality of the civilian's international interests, the relationships between the governments themselves, and the degree of confidence that the source and nature of the attack can be properly identified.

2. Examples of Political Loss in the Context of Cyberwar

To this crude analysis of political risk must be added the nature of possible government sanctions. Certainly, the mere risk of censure or a modest fine will pale in comparison to a more serious sanction. To date, the frequency and severity of cyberwars are largely matters of guesswork. However, as weapons improve, we can expect to see more blatant and aggressive attacks that use or injure the private sector.

It will be natural for governments to respond to such attacks by attempting to regulate, and perhaps control, civilians that are used as tools or means of delivery of attack weapons. Such government regulation can take the

form of incentives, or alternately, threats. Below are just a few examples of the costs and losses the U.S. government could impose on civilians.

The government might regulate the terms of civilians' contracts with suppliers and customers to shift risks or impose costs related to cyber defense. Even changes that would reduce a civilian's legal risk may not be in the civilian's favor in a globalized economy where adversely affected parties can migrate to competitors from other jurisdictions that do not limit their rights or recourse for disruption to their businesses.[63]

Following the model of the USA PATRIOT Act,[64] the government could mandate adoption of internal policies and procedures, impose detailed reporting requirements, proscribe dealings with certain individuals, organizations, or countries, and impose criminal sanctions for assisting or not sufficiently defending attacks.

The government could exercise its taking power under the Fifth Amendment by taking control and/or ownership (either temporary or permanent) of the civilian's property, ranging from telecommunications networks to patents owned by a university. Whether such action would constitute a constitutional "taking" that would require payment of "just compensation" is discussed below, but even if it were so held, the "just compensation" might not represent a market-return on the lost asset.[65]

The government could simply draft or conscript personnel and property owned by the civilian without payment of compensation. The political risk of conscription requires some explanation.

3. Conscription as a Political Risk

A distinguishing characteristic of information technology is its encapsulation in patents, copyrights, trade secrets, and other forms of intellectual property which entitle the owner of that property to control its use by third persons. The most common forms of such control are licensing agreements and lawsuits for infringement. One effect of this characteristic is that IT capabilities are generally localized to the owner or licensee of a particular property, such that an individual employee cannot accomplish the same output if she is disassociated from her employer.

As a result, it is not as though the military can create a cyber defense by drafting individual IT all-stars. Instead, it must do so either via agreement

63. As suggested above, this factor is not likely to be significant in the consumer context because consumers have no bargaining power in certain situations such as non-price and non-quality terms. However, it might affect commercial transactions, especially those involving technology and other high dependence/high risk products.

64. *See* 18 U.S.C. § 1 *et seq.* (2006).

65. *See* U.S. CONST. amend. V; *see also* Kelo v. City of New London, 545 U.S. 469 (2005) (holding that the taking of property for city development was for public use and did not require just compensation).

(consensual requisition) or conscription, through the acquisition of both technology and individuals or of organizations familiar enough with that technology to make it a protective device or successful weapon.[66]

Technology is, of course, the means by which an outcome is accomplished and not the outcome itself. Therefore, the military may have the option of acquiring many different technologies with which it believes it can equally successfully conduct a cyberwar. The availability of such options creates a political risk for each civilian that may have the technology the military would like to use. Even if the civilian is ultimately persuaded to agree to provide its technology and personnel to the cyberwar effort, rather than risk conscription, the mere risk of conscription is a political risk that can be mitigated through the political process.[67]

Because conscription increases the risk of combatant status and thus increases the magnitude of casualty risk to the civilian, it is logical to expect that civilians will spend substantial resources on attempting to avoid conscription—especially since, as we conclude below, conscription does not equate to compensation. Therefore, we can expect that civilians will attempt to entice the military to contract for, rather than conscript, their services. On the other hand, the military will have every incentive to use the threat of conscription as a bargaining tool to achieve a low procurement cost or other favorable procurement terms. The civilian's most likely response is to use its political access and clout to change the military's attitude.

D. Reputational Risk

1. Reputational Risk in the Context of Cyberwar

Reputational risk includes any potential impact on a civilian's goodwill—from perceptions that cellular service is not reliable to rumors that university faculty members are fellow travelers with foreign despots. Opinions on the reliability, safety, and other attributes of the affected civilian's goods and services will eventually affect the civilian's operations and revenues. To a certain extent, reputational risk is subsumed in the risk categories described above because harm to reputation often leads to reduced revenues and increased litigation and governmental scrutiny.

Nevertheless, it is worthwhile to consider reputational risk separately because doing so tends to bring into clearer focus the intangible aspect of cyberwar. For example, reputational risk dominates the risk profile of a cyber attack launched solely for propaganda purposes because propaganda focuses on the respective reputations of attacker and target. It follows that

66. As an example, one can imagine that a team of Mac programmers would not have the same output of PC programs as a team of PC-experienced programmers.

67. This process is familiar to those who lived through past drafts. Relationships with Congressmen, bureaucrats, friendly doctors, and immigration officials may reduce the political risk of conscription.

those attacking a civilian as part of a broader strategic propaganda campaign will focus on reputational aspects distinct from those involving the civilian's products. Such attacks may be similar to the attacks on Proctor & Gamble, in which it was accused of promoting Satanism.[68] For example, cyber attackers could create phishing sites or deface a civilian's own web page to associate it with unpopular causes.

Given the harm to personal reputations arising from associations with unpopular institutions, we can expect that civilian executives will be motivated to protect their personal reputations and those of their colleagues and investors even at the price of monetary loss to their employers. Since executives and other key stakeholders of civilians that fail to aggressively defend against such attacks or cooperate with the government's cyberwar effort are likely to suffer a loss of reputation, we can expect that they will use their best efforts and discretion to defend against an attacker's propaganda.

2. Reputational Risk in the International Context

Many civilians do business in many countries or have relationships with constituencies that might have adverse loyalties or interests in a cyberwar. This is likely in the case of an ambiguous cyber attack with its uncertain protagonist and objective.[69] For example, an oil company might have supply or output contracts with warring countries or a university might have foreign campuses or programs with adversaries. This may lead such multi-national enterprises to attempt to create a perception of neutrality or a perception of unbiased support for all potential combatants. For example, the oil company might declare that it will continue to honor all contracts but will otherwise not expand its operation. Alternately, the university may attempt to centralize all activities that might impact the cyberwar, including its faculty's consulting contracts with the warring nations.

One potential difficulty of such an approach is that combatants might not accept the civilian's stance and may wage a propaganda war that attempts to show the civilian is actually a combatant or at least a sympathizer. Or they may not attack the civilian's spin, but might directly attack the civilian in order to accomplish a change in behavior. In a sense, then, the multi-national civilian might find that its very attempts at avoiding reputational harm has thrust it into the war as a combatant and therefore increased its operational and other risks.

A conscripted civilian will face different reputational risks because at least part of its business will be under direct government control. Opposing belligerents are unlikely to care about the different motivations and legal niceties that flow from conscription, which will present civilian management with complicated issues of corporate governance. For example, assume the U.S. government conscripted the entire assets of a corporation incorporated

68. *See* Procter & Gamble Co. v. Amway Corp., 242 F.3d 539, 542 (5th Cir. 2001).

69. *See* Brenner & Clarke, *supra* note 7.

in Delaware and that among those assets were the shares in numerous foreign subsidiary entities. The rights of a parent to control its subsidiary's activities are limited by the law of the jurisdiction in which the subsidiary is organized. Foreign corporate law typically does not entitle the parent to exercise day-to-day operational management, regardless of the customary practice that reflects economic reality. Therefore, the parent and non-shareholder stakeholders in the foreign subsidiary may perceive different reputational risks or determine that different risk management techniques are appropriate.[70] They should be free to manage those risks in accordance with the interests of the foreign subsidiary, even if those interests differ from those of the U.S. government. We base this conclusion on the fact that U.S. law recognizes the separate identity of the foreign subsidiary and the parent has pre-existing fiduciary duties to the subsidiary.[71]

IV. Shifting Cyberwar Losses: Who Is Going to pay for This?

A. Potential Targets

In light of the increased evidence of severe cyber attacks, even a civilian employing careful risk prevention and mitigation practices (especially one in the financial services, energy, and other infrastructure industries) can expect to suffer substantial casualties from cyberwar. In this part, we analyze whether a civilian casualty will be likely to recoup its losses from third parties. There are four potential sources:

1. Belligerents. Efforts have been made under U.S. law to hold foreign governments liable for losses suffered by civilians in the course of an attack.[72] The likelihood of significant success against cyber attackers is remote, however, because of the legal issues relating to sovereign immunity and comity, and the practical difficulties of identifying the source of the attack and demonstrating a causal connection between the attack and the harm.

2. Contributors. Parties that caused the casualty tortiously or by breach of contract might also be liable for cyberwar losses. For example, a pharmaceutical manufacturer that suffers a plant shutdown might seek damages from its electrical utility for not taking reasonable efforts to protect the power grid. In our judgment, the ability to shift losses to third parties will be greatly limited by legislation, common law tort principles, and, most importantly, the contractual disclaimers, waivers, and limitations, discussed above. Loss-shifting to other private parties is therefore unlikely, given the almost universal use of contractual limitations and the reluctance of courts to interfere with so-called "freedom of contract."

70. This consideration also applies to legal and political risk.

71. *See* Sinclair Oil Corp. v. Levien, 280 A.2d 717, 720, 722 (Del. 1971).

72. *See, e.g.*, Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428 (1989) (holding there was no exception to sovereign immunity so as to allow recovery for the destruction of an oil tanker).

3. INSURERS. Insurance has been the traditional means of spreading casualty loss for everything from natural disasters to environmental damage and toxic torts. While it is possible to develop insurance to cover cyberwar losses, the insurance industry has yet to provide anything near comprehensive coverage for cybercrime risks.[73] The coverage that can be purchased today is narrowly conscribed to losses that can be readily confirmed and measured, and policy limits are generally modest.[74] More importantly, insurance policies of all types exclude coverage for losses resulting from acts of war or civil unrest, because the potential amount of claims could be catastrophic.[75] Although the insurance industry has developed some re-insurance and refined pooling vehicles for hurricane and earthquake risk, those models are unlikely to be employed for cyberwar risk because the statistical evidence is simply not available to allow actuaries to calculate premiums. Therefore, we conclude that insurance as an avenue for loss shifting is a dead end.

4. GOVERNMENT. The federal government has come to be viewed, rightly or wrongly, as the insurer of last resort. What started with social security and federal deposit insurance has expanded to a broad range of transfer payments for natural disasters, healthcare, unemployment, and bad business decisions even by the largest and wealthiest citizens. However, each of these loss-shifting or pooling mechanisms has been authorized by Congressional action, and it is unlikely that the political will exists to pass legislation providing governmental loss-pooling for cyberwar losses, at least until catastrophic losses have affected the economy. In the meantime, we believe that the primary vehicle to shift cyberwar losses to the government will be the theory that the military's use or destruction of civilian property constituted a "taking" under the Fifth Amendment for which the owner is entitled to compensation. We examine those issues in the remainder of this article.

B. The Takings Clause Meets the War Power: A Sampler of the Jurisprudence

The U.S. Constitution divides the federal government's war powers between the executive and legislative branches. Article 1, Section 8, gives Congress the power to:

---

73. Technically, insurance can take two forms. The first is "loss shifting," where an insured buys, by payment of a premium, the right to shift the loss to the insurer. The second is "loss pooling," where pool members agree to create a fund (pool) from which members' losses will be paid. ROBERT H. JERRY, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 1.08 (2009). While the distinctions would be important in designing an insurance program, they are not material to the present discussion.

74. *See* Ann Kale, et al., CYBER LIABILITY AND INSURANCE: MANAGING THE RISKS OF INTANGIBLE ASSETS (2010).

75. JERRY, *supra* note 73, § 1.6.

> provide for the common [d]efen[s]e and general [w]elfare of the United States; [t]o declare [w]ar; [t]o raise and support [a]rmies; [t]o provide and maintain a Navy; [t]o make [r]ules for the [g]overnment and [r]egulation of the land and naval [f]orces; to provide for calling forth the [m]ilitia to execute the [l]aws of the Union, suppress [i]nsurrections and repel [i]nvasions.[76]

Article II, Section 2 gives the President unspecified powers as "Commander in Chief."[77] We accept as axiomatic that the Congressional power includes providing for defense against cyber attacks and to launch cyber attacks. We also assume that the Presidential power as Commander in Chief, while not unlimited,[78] provides the President with sufficient power to authorize military actions related to cyberwar.

On the other hand, the "Takings Clause" of the Fifth Amendment provides ". . . nor shall private property be taken for public use, without just compensation."[79] The Clause was "designed to bar Government from forcing some people alone to bear public burdens which, in all fairness and justice, should be borne by the public as a whole."[80]

The question then arises: To what extent, if at all, does the Takings Clause limit the power of the government under the War Powers to appropriate, damage, or destroy private property in the course of defending or prosecuting a military action? Two ends of the spectrum can be easily identified. At one end, the government does not ensure that citizens will escape property damage from war: "[I]n wartime, many losses must be attributed solely to the fortunes of war and not to the sovereign."[81]

At the other end, the government cannot appropriate property simply on the grounds that it is necessary to prosecute potential wars.[82] Between these extremes is an extensive gray area. Since the Civil War, the Supreme Court

---

76. *See generally* U.S. CONST. art. I, § 8, cl. 1, 11, 12, 13, 14, 15.

77. U.S. CONST. art. II, § 2, cl.1.

78. *See generally* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952) (finding unconstitutional President's seizure of steel mills to ensure continued production during wartime).

79. U.S. CONST. amend. V.

80. Armstrong v. U.S., 364 U.S. 40, 49 (1960).

81. U.S. v. Caltex, Inc., 344 U.S. 149, 155–56 (1952) (holding that owners of refineries were not entitled to compensation for army's destruction of refineries so that they would not fall into enemy control).

82. *See generally* Mitchell v. Harmony, 54 U.S. 115 (1851) (finding that the owner of mules and wagons who had been allowed to accompany military into Mexico to trade with Mexicans was entitled to compensation for appropriation of property for use in battle); *see also* United States v. Russell, 80 U.S. 623 (1871) (finding that a steamboat owner was entitled to compensation for transporting troops during the Civil War).

has been unwilling to find a military taking or to state a bright-line test for when a property owner is entitled to compensation for a loss arising from military action.[83] This is not surprising given the Court's admission that in any context "[t]he question of what constitutes a 'taking' for purposes of the Fifth Amendment has proved to be a problem of considerable difficulty."[84]

In our view, the unwillingness of the Court to establish a bright-line test reflects an appreciation for the separation of powers, the judiciary's lack of experience with potential scenarios, and the increasing complexity and immediacy of warfare. In other words, the Court is wise in refraining from treading where imposition of liability might have unforeseen consequences.[85]

Courts were not always reticent in requiring compensation for the military's interference with property rights. Early war-takings cases included holdings that required compensation on the ground that the military had not shown a sufficiently imminent necessity. For example, *Mitchell v. Harmony* held that an owner of mules and wagons who had been allowed to accompany troops into Mexico and to trade with Mexicans was entitled to compensation for appropriation of his property for use in battle and for pursuing opposing troops farther into Mexico.[86] And *United States v. Russell* awarded a steamboat owner compensation for transporting troops during the Civil War.[87]

However, the bench's generosity was short lived. The seminal modern case is *United States v. Pacific Railroad Co.*, which included a claim for compensation for bridges the Union Army destroyed during the Civil War to

---

83. *See, e.g.* , Nat'l Bd. of YMCA v. United States, 395 U.S. 85 (1969) (holding that building owners were not entitled to compensation for destruction of their building during riots in Panama because the damage occurred during conflict); *see also* El-Shifa Pharm. Indus. Co. v. United States, 378 F.3d 1346, 1361 (Fed. Cir. 2004), *cert. denied*, 545 U.S. 1139 (2005) (recognizing that the "role of the judiciary branch . . . in the area of military takings . . . has been to draw a 'thin line between sovereign immunity and governmental liability," (quoting Nat'l Bd. of YMCA v. United States, 396 F.2d 467, 472 (Ct. Cl. 1968))); *see also, Nat'l Bd. of YMCA*, 396 F.2d at 471 (stating "in view of the broad language of the fifth amendment and the difficulty we find in determining whether compensation is required in this case, we look to the general principles announced in the decisional law to find the narrow and sometimes indistinct line that separates losses that are necessary incidents of the ravages and burdens of war from those situations where the Government is obliged to pay compensation to the owner of private property that is taken for public use.").

84. Penn Cent. Transp. Co. v. City of N.Y., 438 U.S. 104, 123 (1978).

85. *See* Respublica v. Sparhawk, 1 U.S. 357, 363 (1788) (Chief Justice M'Kean pointed to the "folly" of the mayor in London in 1666 who allowed half the city to burn out of fear that he might be liable for trespass if he ordered the destruction of property that would have stemmed the fire).

86. Mitchell, 54 U.S. at 135.

87. Russell, 80 U.S. at 629-30.

impede the advance of the Confederate Army.[88] The Court quoted a message from President Grant to the Senate when he vetoed a bill that would have provided compensation for property taken in war.[89] General Grant relied on "a general principle of both international and municipal law" that all property is held subject both to the right of the sovereign to take it for public use, upon payment of just compensation, but also "subject to be temporarily occupied, or even actually destroyed, in time of great public danger, and when the public safety demands it; and in this latter case governments [d]o not admit a legal obligation on their part to compensate the owner."[90]

The principal that all property is, at least in some sense, held subject to the common good became even more widely recognized after World War I—the first war that implicated total mobilization of the American economy. An oft-cited perspective is that of Charles Evans Hughes, a future Supreme Court Justice, which he presented in a speech to the American Bar Association after he lost the 1916 Presidential election to Woodrow Wilson. Hughes recognized that war would require regulation of industries beyond what was tolerable in peacetime. He stated:

> The power to wage war is the power to wage war successfully. The framers of the Constitution were under no illusions as to war . . . . In equipping the National Government with the needed authority in war, they tolerated no limitations inconsistent with that object, as they realized that the very existence of the nation might be at stake and that every resource of the people must be at command.
>
> The extraordinary circumstances of war may bring particular business(es) and enterprises clearly into the category of those which are affected with a public interest and which demand immediate and thorough-going public regulation. The production and distribution of foodstuffs, articles of prime necessity, those which have direct relation to military efficiency, those which are absolutely required for the support of the people during the stress of conflict, are plainly of this sort. *Reasonable regulations to safeguard the resources upon which we depend for military success must be regarded as being within the powers confided to Congress to enable it to prosecute a successful war* . . . .
>
> [I]t may be said that the power has been expressly given to Congress to prosecute war, and to pass all laws which shall be necessary and proper for carrying that power into execution. That power explicitly conferred and absolutely essential to the safety of the Nation is not destroyed or impaired by any later provision of the Constitution or by any one of the amendments. These may all

88. United States v. Pacific R.R., 120 U.S. 227 (1887).

89. *Id.* at 238

90. *Id.*

> be construed so as to avoid making the Constitution self-destructive, so as to preserve the rights of the citizen from unwarrantable attack, while assuring beyond all hazard the common defense and the perpetuity of our liberties. These rest upon the preservation of the nation.
>
> It has been said that the Constitution marches. That is, there are constantly new applications of unchanged powers, and it is ascertained that in novel and complex situations, the old grants contain, in their general words and true significance, needed and adequate authority. So, also, we have a fighting Constitution. We cannot at this time fail to appreciate the wisdom of the fathers, as under this charter, one hundred and thirty years old-the Constitution of Washington-the people of the United States fight with the power of unity, as we fight for the freedom of our children and that hereafter the sword of autocrats may never threaten the world.
>
> The war powers of Congress and the President are only those which are to be derived from the Constitution but . . . the primary implication of a war power is that it shall be an effective power to wage the war successfully. Thus, while the constitutional structure and controls of our government are our guides equally in war and in peace, they must be read with the realistic purposes of the entire instrument fully in mind.[91]

Since World War II, judicial respect for these necessities of war has only increased. For example, *Lichter v. United States* reflects a strong judicial deference to the needs of a nation at war.[92] Justice Burton, writing for a 6-2 majority, started his opinion upholding the constitutionality of an excess profits recoupment statute with the following statement:

> The Renegotiation Act, in time of crisis, presented to this nation a new legislative solution of a major phase of the problem of national defense against world-wide aggression. Through its contribution to our production program it sought to enable us to take the leading part in winning World War II on an unprecedented scale of total global warfare without abandoning our traditional faith in and reliance upon private enterprise and individual initiative devoted to the public welfare.[93]

No doubt influenced by this view of the exigencies of war, the Court held that the grant to the Government of the right to recoup "excessive profits" did not constitute a taking of property without due process in violation of

---

91. Charles Evans Hughes, *War Powers Under The Constitution*, 42 A.B.A.REP. 232, 238–39, 247–48 (1917), *reprinted in*, 2 MARQ. L. REV. 3 (1918) (emphasis added).

92. *See* Lichter v. United States, 334 U.S. 742 (1948).

93. *Id.* at 745-46 (footnote omitted).

the Fifth Amendment.[94] The Court's approach to the problems permitting executive discretion to adapt to changing methods of war could have been written with cyberwar in mind:

In total war it is necessary that a civilian make sacrifices of his property and profits with at least the same fortitude as that with which a drafted soldier makes his traditional sacrifices of comfort, security and life itself.[95]

The Court's equating the economic regulation of business to the conscription of soldiers was most significant. The Court recognized that both the economic regulation of the Renegotiation Act and the draft sprang from the war power, and "[e]ach was a part of a national policy adopted in time of crisis in the conduct of total global warfare by a nation dedicated to the preservation, practice and development of the maximum measure of individual freedom consistent with the unity of effort essential to success."[96] Moreover, the Court argued that "mobilized property in the form of equipment and supplies became as essential as mobilized manpower," and that mobilization extended beyond the uniformed armed services to the entire population.[97]

Indeed, the court used the acceptance of the constitutionality of the draft to justify the alleged economic taking:

> The conscription of manpower is a more vital interference with the life, liberty and property of the individual than is the conscription of his property or his profits or any substitute for such conscription of them. For his hazardous, full-time service in the armed forces, a soldier is paid whatever the Government deems to be a fair but modest compensation. Comparatively speaking, the manufacturer of war goods undergoes no such hazard to his personal safety as does a front-line soldier and yet the Renegotiation Act gives him far better assurance of a reasonable return for his wartime services than the Selective Service Act and all its related legislation give to the men in the armed forces.[98]

Having established the government's right to take profits, the Court held that the public interest was satisfied by the imposition of adequate procedural safeguards to conform "to the constitutional limitations under which Congress was permitted to exercise its basic powers."[99] In deciding what process

94. *Id.* at 801–02.

95. *Id.* at 754.

96. *Id.* at 755.

97. *Id.*

98. *Id.* at 756.

99. *Id.* at 765. It should be noted that the payment of normal profits does not mean that there was no taking of excess profits. From the economic viewpoint, the case could be viewed as the equivalent of a finding that the government had taken the goods produced in exchange for "just compensation" in the form of a fair profit.

was due, Justice Burton stated that Congress had two choices: It could have conscripted property and manpower along a totalitarian model or it could have and did opt for a plan of renegotiation that allowed the government to contract now and set the final price later.[100] A choice the Court stated "appears in its true light as the very symbol of a free people united in reaching unequalled productive capacity and yet retaining the maximum of individual freedom consistent with a general mobilization of effort."[101] The Court therefore held that the procedures incorporated in the Renegotiation Act provided due process and upheld the constitutionality of the Act.[102]

United States v. Central Eureka Mining Co. is another case in which the Court held that the war power trumped the takings clause.[103] The case involved a takings challenge to an order of the War Production Board (WPB) that essentially made gold mines dormant.[104] The order classified the industry as "nonessential" to the nation's ability to wage World War II and directed each mine operator to close down its operations except for minimum activity necessary to maintain the mine.[105] The Supreme Court held that the order did not constitute a taking of the mining companies' property, entitling them to compensation under the Fifth Amendment:

> [T]he WPB made a reasoned decision that, under existing circumstances, the Nation's need was such that the unrestricted use of mining equipment and manpower in gold mines was so wasteful of wartime resources that it must be temporarily suspended. Traditionally, we have treated the issue as to whether a particular governmental restriction amounted to a constitutional taking as being a question properly turning upon the particular circumstances of each case. See *Pennsylvania Coal Co.* v. *Mahon*, 260 U. S. 393, 416. In doing so, we have recognized that action in the form of regulation can so diminish the value of property as to constitute a taking. . . . In the context of war, we have been reluctant to find that degree of regulation which, without saying so, requires compensation to be paid for resulting losses of income. . . . The reasons are plain. War, particularly in modern times, demands the strict regulation of nearly all resources. It makes demands which otherwise would be insufferable. But wartime economic restrictions, temporary in character, are insignifi-

100. *See id.*

101. *Id.* at 766.

102. *Id.* at 787. *Lichter* could also be viewed as a due process case. That is, the Court might have found a taking if Congress had not provided sufficient procedural safeguards to ensure that the appropriate profit was fairly determined.

103. *See* United States v. Cent. Eureka Mining Co., 357 U.S. 155 (1958).

104. *Id.* at 156.

105. *Id.*

> cant when compared to the widespread uncompensated loss of life and freedom of action which war traditionally demands.
>
> We do not find in the temporary restrictions here placed on the operation of gold mines a taking of private property that would justify a departure from the trend of the above decisions. The WPB here sought, by reasonable regulation, to conserve the limited supply of equipment used by the mines and it hoped that its order would divert available miners to more essential work. Both purposes were proper objectives; both matters were subject to regulation to the extent of the order. L-208 did not order any disposal of property or transfer of men. Accordingly, since the damage to the mine owners was incidental to the Government's lawful regulation of matters reasonably deemed essential to the war effort, the judgment is reversed.[106]

The most recent opinion addressing takings and military action issued in the context of the U.S. military response to riots in the Panama Canal Zone.[107] In *National Board of YMCA v. United States*, the Court held that building owners were not entitled to compensation when soldiers occupied their buildings while responding to a riot and attempting to protect their property.[108] The Court decided the case on fairly narrow grounds that the soldiers were acting for the benefit of the owners:

> Of course, any protection of private property also serves a broader public purpose. But where, as here, the private party is the particular intended beneficiary of the governmental activity, 'fairness and justice' do not require that losses which may result from that activity 'be borne by the public as a whole,' even though the activity may also be intended incidentally to benefit the public.[109]

---

106. *Id.* at 168–69. Justices Frankfurter and Harlan did not view the regulation in the same perspective. Frankfurter thought that the lower court improperly jumped to the constitutional question before construing the statue pursuant to which the cases were brought to determine whether Congress actually intended to award compensation. *Id.* at 179 (Frankfurter, J., dissenting). Harlan, however, took the bull by the horns and castigated the majority for moving beyond precedent without adequate justification. He argued that previous cases denying compensation for losses resulting from wartime regulatory measures were readily distinguishable because the country was under "conditions of total mobilization" and the matters regulated had ramifications "touching everyone in one degree or another." *Id.* at 183–184 (Harlan, J., dissenting). The WPB, however, under the guise of regulation, accomplished the equivalent of outright physical seizure of private property. *Id.* Thus, Harlan argued, the Court should treat the WPB's order as what it was "in every realistic sense . . . a temporary confiscation of respondents' property." *Id.*

107. Nat'l Board. of YMCA v. United States, 395 U.S. 85 (1969).

108. *Id.* at 92.

109. *Id.*

The Court also found an independent basis for denying the takings claim; the physical occupation by the troops did not deprive the petitioners of any use of their buildings:

> [W]e conclude that the temporary, unplanned occupation of petitioners' buildings in the course of battle does not constitute direct and substantial enough government involvement to warrant compensation under the Fifth Amendment. We have no occasion to decide whether compensation might be required where the Government in some fashion not present here makes private property a particular target for destruction by private parties.[110]

In summary, the Supreme Court has demonstrated substantial reluctance to second-guess military requisitions and actions in wartime. We now turn to the particular case of potential takings justified by the prosecution of cyberwar.

C. Does Conscription of Assets Constitute a Taking?

In *Conscripts*, we described a possible means by which the Federal Government could combat cyberwar by drafting individuals into a Cyberwar National Guard (CNG).[111] The CNG would create a ready workforce of cyber warriors.[112] However, as mentioned above, the CNG would not be effective unless its warriors were armed with appropriate intellectual property and information technology.[113]

Let us assume that the Federal Government passes a law that prohibits employers from terminating the employment of members of the CNG and requires the employer to provide its CNG member-employees with access to and the right to use the IT and equipment normally used in their occupation. Let us further assume that Congress does not include any appropriation for paying the employer for that access and use by the CNG. Is the employer entitled to compensation for the "taking" of its property to support the CNG?

The short answer, based on existing precedent, is "probably not." First, as noted above, the Supreme Court has noted the close analogy between conscription and regulation of property in connection with military activity.[114] If the government can draft the full-time services of individuals and thereby deprive an employer of the conscripts' services, it follows that the government can draft them for their part-time services, even if doing so deprives the employer of part of the services it has purchased.

---

110. *Id.* at 93–94.

111. Brenner & Clarke, *supra* note 7, (manuscript at 56).

112. *See id.*

113. *See* § I(A)(2) *supra.*

114. *Lichter v. United States*, 334 U.S. 742, 765–66 (1948).

Moreover, the mandatory employment concept seems to be the functional equivalent of a taking of the employees' wages—assuming the employer is required to continue paying the employees. Thus, the issue distills to whether the government can require the civilian firm to provide to the conscript the tangible and intangible assets the conscript would otherwise use in the course of her employment. We now turn to that issue.

D. Compensation for Access and Use of Civilian Property in Cyberwar

The authorities discussed above have addressed traditional, kinetic war, but their logic applies equally to cyberwar.[115] As in *Eureka*, a military order (pursuant to a congressionally authorized administrative procedure) requiring a civilian property owner to provide the government with access to and the right to use assets would not permanently deprive the civilian of those assets.

More fundamentally, the Court—even at the distance of thirteen years from WWII—did not see the shutdown of the mine as imposing a burden different than that legitimately imposed on any citizen in wartime. Thus, to the extent that a court is persuaded that a cyber attack is indeed the equivalent of war,[116] the owner will not be entitled to compensation for the government's use of that property in fighting the war (whether in a defensive or offensive mode) or for the government's restriction on the owner's use of the property or even its destruction.

Of course, there is always the possibility that the government's interference with private property will become too attenuated from the conflict. *Mitchell* and *Russell* are often distinguished, but they are still good law. Accordingly, they could still require compensation for a government action that is too remote in time or in necessity. Recent jurisprudence, such as *El-Shifa*, however, demonstrates a strong judicial deference to the other branches of government to make those nexus decisions.[117]

Moreover, it is also likely that the government will be able to offer a credible argument that the increasing co-dependence of markets and competitors supports a finding that the civilian grow inured to military action. In

115. Questions of Presidential power to take military action without Congressional authority are complex and beyond the scope of this article. For an analysis of those issues, *see* Sidney Buchanan, *A Proposed Model for Determining the Validity of the Use of Force Against Foreign Adversaries Under the United States Constitution*, 29 HOUS. L. REV. 379 (1992) (discussing the constitutional scope of both Congress and the President during wartime); *see also* Jules Lobel, *Conflicts Between the Commander in Chief and Congress: Concurrent Power Over the Conduct of War*, 69 OHIO ST. L.J. 391 (2008) (discussing the power between the President and Congress to take action and conduct war).

116. *See* Brenner & Clarke, *supra* note 7.

117. *See* El-Shifa Pharm. Indus. v. United States, 402 F. Supp. 2d 267 (D.D.C. 2005). (Sudanese company alleging destruction of its plant by U.S. military failed to allege a valid takings claim).

other words, the military's taking actually protected the claimant from even greater harm. If this paternalistic argument was persuasive with the 1666 London fire, the 1964 Panamanian riots, and the 1980 blocking of Iranian assets,[118] it should be equally persuasive as applied to cyberwar attacks, which can happen instantaneously, without warning and without relation to military assets.

Courts should be reluctant to find that regulation or required access to civilian property was either premature or unnecessary in fighting a cyberwar. Defense of cyberwar requires thorough investigation, planning, and preparation. That defense is complicated by the complexities of global information networks, the instantaneous nature of attacks, their ambiguity as to source, duration and intent, and the potential consequential damages. Therefore, even conscription or asset requisitions to deal with the threat of cyberwar should not be deemed too remote in time.

This is especially so because it is unlikely that a civilian can show a total deprivation of use before an attack since most IT assets can be used on a non-exclusive basis. Thus, civilians will have a difficult time demonstrating anything more than a temporary loss of income from government regulation. And this is a property interest that the Supreme Court has never accorded much weight, even in non-military situations.[119]

In summary, forced prevention, readiness, and response efforts directed by the military should not be considered takings, at least in the absence of the destruction of assets, permanent foreclosure against use, or arbitrary requisition procedures without possibility of judicial review.

V. Conclusion

Cyberwar is a reality that civilians must address regardless of their confidence in their existing IT security. If government and industry are slow in addressing cyberwarfare risk, it is not because the incentives are not present or the tools unavailable. Executives of civilian private sector enterprises have fiduciary duties to protect enterprise assets and reduce liabilities by employing traditional risk management principles. Managers of governmental civilian enterprises have similar public duties. The urgency of sound risk management is heightened by the lack of loss-shifting alternatives. Although civilians can protect themselves by contract from liabilities to customers arising from cyberwar disruptions and losses, they will not be able, except in rare, fortuitous circumstances, to pass losses up their supply chains, to insurers or to that last recourse, the federal government.

118. *See* Dames & Moore v. Regan, 453 U.S. 654 (1981) (blocking and attachments of assets during the Iranian hostage crises were not an unconstitutional takings).

119. *See, e.g.*, Penn Cent. Trans. Co. v. New York, 438 U.S. 104 (1978) (holding that the denial of approval of construction plans did not constitute a taking because the restrictions were related to the public welfare and permitted reasonable beneficial use).