University of Dayton

From the SelectedWorks of Susan Brenner

Summer 2010

Civilians in Cyberwarfare: Casualties

Susan W. Brenner
Leo L. Clarke

UNIVERSITY of DAYTON

Available at: https://works.bepress.com/susan_brenner/3/

CIVILIANS IN CYBERWARFARE: CASUALTIES

BY

SUSAN W. BRENNER & LEO L. CLARKE

TABLE OF CONTENTS

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 executives working for critical infrastructure and computer security companies found that "45 percent believed their governments were either `not very' or `not at all' capable of preventing and deterring cyberattacks."[3]

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 is cost: Developing the capacity to wage cyberwar is an inexpensive proposition compared to what is involved in developing and maintaining the capacity to wage twenty-first century kinetic war.[5] Since cyberwarfare will for the most part be waged over publicly-accessible networks,[6] the

---

[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), *https://www.afresearch.org/skins/rims/display.aspx?moduleid=be0e99f3-fc56-4ccb-8dfe-670c0822a153&mode=user&action=researchproject&objectid=e6bcf0d2-6096-41a0-b0bb-e425864be6ca.*

[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 infra* § II.

expense involved primarily encompasses training and paying cyberwarriors and purchasing and maintaining the hardware and software they will need to launch and counter cyberattacks.

In a recent article,[7] we examined the need to involve civilians in cyberwarfare and the legal devices government can use to compel such involvement, when and as necessary. In this article, we address how law can and should address the consequences that result from 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 ameliorate 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 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.[8] 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, especially given the frequency and severity of cyberwar 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 materially different from the risk of cybercrime and other IT hazards, and how civilian executives will react to threats of cyberwar. We argue that, from the civilian's perspective, cyberwar presents different risks 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 were the same, the risk of potential extensive governmental 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 the civilian if its operations are disrupted by either its status as a combatant or victim. We identify the risks of legal liability to shareholders, customers, suppliers, and other stakeholders as well the broader issues of political and reputational risk and consider how civilians might manage those risks. We 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 mal-performance 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 await 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,

---

[7] Susan W. Brenner with Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, __ VANDERBUILT JOURNAL OF TRANSNATIONAL LAW __ (forthcoming 2010), hereafter "*Conscripts.*"

[8] For simplicity, we will refer to both groups as "civilians."

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 5th 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 One Becomes a Casualty

A civilian can suffer direct casualties from a cyberwar in myriad 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 that the reader can put cyberwar risk into a context that allows comparison with more traditional risks of loss.

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 has been an outspoken opponent of the government's treatment of a minority. Or an attack could target a civilian that is perceived as an exploiter of the country's resources.

Second, the civilian could be a target because it is means of attacking others. For example, an electric utility could be targeted to affect a power grid that supplies a telecommunications company that is being 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. Or 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. Attacks on county tax or deeds databases could disrupt real property transfers.

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

- The government might impose new and costly regulations to deter or defend against attacks.[9]

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

- 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.
- The government might conscript specific assets or even the civilian's entire enterprise.[10]

Fifth, a civilian can be a combatant, either because it perceives its own interests as furthered by participation in the cyberwar or because it has been conscripted by the government and thrust into the combat zone.[11] As we demonstrated in *Conscripts*, the difference between combatants and civilians, while traditionally fundamental in kinetic warfare, is more nebulous in the context of cyberwar. For example, if a telecommunications company refuses to cooperate with any governmentally-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 – some packets of information delivered outside the combat zone and some, without its knowledge, in 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, 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 cyberattack 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 or 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

---

[10] *See Conscripts*, *supra* note 6, at ____ ff.

[11] Conscription does not mean the conscript is necessarily a combatant. Lots of draftees have spent their hitches playing ball or oboes.

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.[12] In reality, however, they are simply congeries of assets or, as corporate law scholars proclaim, a "nexus of contracts."[13] There is no body there which can serve as the articulation 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 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 to the Army his pink Cadillac or Graceland, conscription of 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 were adopted, then for analytical purposes it would be preferable 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?

---

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

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

Before proceeding to analyze how civilians should respond to the casualty risk of cyberwar, we must first ask whether cyberwar will or should generate a different response from civilians than the now commonly-accepted risk of cybercrime. After all, virtually every civilian has a substantial IT security program in place and a civilian that is so unaware of cybercrime risk that it lacks prophylactic measures to deal with routine intrusions is unlikely to care about cyberwar.[14]

Moreover, even (and perhaps especially) a civilian with a sophisticated security program might be indifferent to the issue of cyberwar. Security managers could reasonably argue that whether an attack is an isolated exercise by a basement hacker, commercial espionage or theft, cyber-extortion, or full-fledged cyberwar is irrelevant to the task at hand: protection of the civilian's own systems and data and its ability to communicate with the outside world. In other words, from a technical perspective, trying to clarify the source and nature of the attack and the motive and goals of a cyber attacker just wastes time and resources. 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 identified and neutralized the threat, the problem becomes someone else's.[15]

Paradoxically, security managers could also argue that cyberwar presents a less significant technical threat than other forms of cyber attack because security managers can expect the government to devote more and better resources to defend cyberwar attack than it does to "mere" cybercrime, as to which law enforcement resources are spread notoriously thin and greatly hampered by jurisdictional limits.[16] Thus, IT managers might, and often do, shrug off discussion of the risks of cyberwar as just more consultant hype about risks that can be adequately addressed by the application of sound security principles.[17]

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

Such a reasonable technical perspective is not likely, however, to prevail at the level of civilian governance. Directors and executive officers, which we will hereafter lump together under the term "executives," have broader responsibilities than just protecting IT assets.

---

[14] The authors have argued elsewhere 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 (2005).

[15] This arguably short-sighted attitude is not unique to cyberwar, it was probably prevalent when the barbarians sacked Europe.

[16] In contrast, the federal government, at least, is taking cyberwar seriously. *See, e.g.,* Shane Harris, *The Cyberwar Plan*, NATIONAL JOURNAL MAGAZINE, 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, 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,

Executives are also charged with optimizing stakeholder value over both short-term and longer-term horizons, and cyberwar presents unusual short and long term risks for the civilian enterprise.

For example, government sponsorship of cyberwar means that the resources that are likely to be devoted to attacks will result in more frequent, prolonged, and severe threats to the civilian's interests. Also, virulent American patriotism is likely to tie cyberwar to broader public interests, which will have the potential to affect corporate reputation and brands, supplier, customer and employee relationships, and the costs and benefits of governmental regulation in ways that are not present when an attack is directed by private cybercriminals only at the civilian for economic purposes. Third, and most important, the risk of conscription creates novel issues of corporate governance.

1. Executives' Duties and Motivations

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.[18] In general, the duty of due care requires that the executives act as reasonably well-informed and prudent persons in managing the civilian's affairs.[19] The duty of care is often subsumed under the rubric of the "business judgment rule" ("BJR"), which holds that an executive cannot be held liable for a breach of the duty of due care if she makes a good faith effort to become informed and acts in what she believe is in the best interests of the civilian, without acting illegally, fraudulently, or with a conflict of interest.[20]

In other words, under the BJR, executives are not liable for making bad business decisions. Under this minimalist standard, executives face little risk of personal liability for their responses to cyberwar, especially since many states permit corporations to limit shareholders' rights for breach of duty to injunctive relief and since most sizable corporations provide

[18] 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., 202 Ala. 376 (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.

[19] *See, e.g.,* for corporations organized for profit, Model Business Corporations Act, § 8.30, 8.42.

[20] *See, e.g.*, Smith v. Van Gorkum, 488 A.2d 858 (Del. 1985) (holding the decision to approve a merger was not an informed one, precluding a merger); Schlensky v. Wrigley, 237 N.E.2d 776 (Ill. App. Ct. 1968) (holding there was no cause of action for a derivative suit because there was no allegation of fraud or breach of duty).

directors' and officers' insurance that further provides protection against shareholder claims for breach of the duty of care.[21]

These minimal duties under the civilian's organic law are supplemented, for publicly held companies, by the Sarbanes-Oxley Act of 2002 ("SOX"). SOX imposed for the first time a layer of federal regulation that requires the chief executive officer of a covered civilian to certify the existence of adequate internal controls affecting the company's external financial reporting.[22] Because information technology plays such a crucial role in recording and reporting of financial information, it is generally held that the adequacy of a company's information security program is an element to be evaluated in determining SOX compliance. An analysis of the impact of SOX is beyond the scope of this article, but suffice it to say that SOX has provided an additional motivation for executives to consider carefully the impact of potential cyberwars on their institution.

Because executives' responses to cyberwar are unlikely to be motivated by concern for personal liability, they can take a broad view of their "corporate responsibility." 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 deleterious 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.[23] Instead, the major corporations routinely profess commitment to goals which include, but are not limited to, competitive financial returns and long-term stability.[24]

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. Executives are more likely to aim at protecting not just current asset values by raising the barriers to intrusion to the highest cost-effective levels, but might also take into account the value of a reputation for good corporate citizenship by cooperating with governmental authorities as well as incurring costs to protect interests of strategic partners, suppliers, and customers beyond the value of the civilian's interests in affected assets. While doing so will likely protect financial assets such as

---

[21] MBCA, § 8.51. As to "D&O" insurance, *see id.* at § 8.57; Bennett L. Ross, *Protecting Corporate Directors and Officers: Insurance and Other Alternatives*, 40 VAND. L. REV. 775 (1987) (evaluating the effectiveness of D & O policies and its substitutes).

[22] Pub. Law 107-204. The Act is codified at various places in titles 15 and 18 of the U.S. Code. *See,* especially, § 404 of the Act, 15 U.S.C. § 7262 (2006). The Act and the regulations implementing the Act are complex and generated a have literature 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).

[23] *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).

[24] *Id.* at 151-53.

corporate brands and goodwill, financial considerations may not be the primary motivating forces.

For example, larger companies, especially companies in regulated industries and publically held companies, are particularly likely to incur costs that cannot be justified on a strict profit maximization basis because they perceive the long term value of cooperation with the government and good public relations.[25] Thus, executives can act consistently with their fiduciary duties if they comply not just with applicable statutes and regulations, but also with governmental strong arming and jawboning. For the same reason, executives can "over-invest" in responding to cyberwars to the extent they are concerned about potential liability to suppliers, customers, and other third parties. 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 are likely to consider the nature of an intrusion into the civilian's IT system to be of paramount importance in determining the amount and nature of the resources to devote to defense and deterrence of cyber attacks and the most appropriate response to specific attacks. This concern will probably be reflected in written policies and procedures that address at least the following key issues: detection and reporting of attempted intrusions; investigation into whether the intrusions are related to other intrusions into the civilian's system and/or is part of a larger cyber attack; appropriate reporting of any successful intrusion to affected line management; and execution of an appropriate response.

2. Possible Executive Approaches to the Novel Risk of Conscription

Civilians can and do choose to ignore or limit their deterrence and defense of cybercrimes for economic reasons – the potential losses from such crimes (when evaluated in terms of severity and frequency) are outweighed by the costs of prevention and prosecution. However, if we are correct in our conclusion that cyberwar will result in conscription of civilians to defend, and perhaps to launch, attacks,[26] then executives will be required to change their economic calculus. After all, a conscript will not have a choice to avoid 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.[27]

---

[25] 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). The prevailing law does not agree with Mr. Buffett. *See, e.g., Schlensky*, 237 N.E.2d 776 (holding that controlling shareholder of Chicago Cubs did not have to install lights and schedule night games if he believed that doing so would lead to deterioration of the surrounding neighborhood).

[26] *See Conscripts*, *supra* note 6, at __.

[27] In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 966-70 (Del. Ch. 1996).

The risk that a civilian's work force, its equipment, and its intangible assets could be usurped by the government would, especially for a large enterprise, require extensive contingency planning, whether or not the civilian could look to the government for compensation. In a sense, then, 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 potential and actual 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 institutions' goals and risk tolerance.[28]

The first step, risk identification, requires the civilian to identify each way in which a cyber attack can adversely affect the civilian. This includes, for example, adverse impacts on how it operates, on its financial condition and prospects, on its potential legal liabilities, its dealings with governments, and with the public at large. "Operational risk" is sometimes used to refer to the impact of cyberwar on the operations of the civilian and its ability to generate revenues and profits. Discussion of this risk is beyond the scope of this article because of the breadth of the definition of "operational risk" and the virtually unlimited different types of businesses affected by cyberwar. We will, however, address in general terms of "legal," "political," and "reputational" risks.

"Legal risk" refers to the potential that the civilian will be held liable to third parties because it failed to defend against the cyber attack or, even worse from the perspective of the civilian, because it ineptly participated in the defense against the attack or in a counter-attack. "Political risk" refers to the risk that the civilian's response or lack of response to the threat of cyberwar or to cyberwar itself will result in new or additional government regulation, whether by legislation or administrative action. "Reputational risk" refers to the potential impact on a civilian's brands and goodwill. This risk is even harder to quantify than political risk, has perhaps 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 the civilian will suffer if the risk-event occurs. These factors are often referred to as frequency and severity. For example, 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. The range of dollar loss(es) expected from the attack is multiplied by the probability that such an attack will occur to provide an estimated loss.

---

[28] *See, e.g.,* James S. Mullarney, *Arming Yourself, Quantification Strategies*, *in* SCOTT K. LANGE ET AL., *E-RISK*: LIABILITIES IN A WIRED WORLD (2000).

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; and water treatment facility 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 process is essential to effective risk management.

The third step in this risk-management approach is to identify and implement risk prevention, mitigation, and shifting mechanisms that will allow the civilian to reduce the risk of loss to an acceptable level. Risk prevention 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 cyberattack 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 loss shifting are common contractual provisions such as force majeure clauses, limitation on liability and 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, in others 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 casualty.

B. Legal Risk Of Third Party Claims For Cyberwar Damage

1. Contract liability

At present, a civilian does not have statutory obligation to participate in a cyber defense or attack. It will, however, have relationships, contractual or otherwise, with third parties which might be affected by its response to cyberwar. For example, a bank has a duty to its customers to honor properly presented payment orders;[29] and utilities have regulatory and contractual duties to provide services to customers on terms set out in tariffs or contracts.[30]

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

[29] U.C.C. § 4A-209 (2007).

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

services (e.g., electricity, Internet access, water) to its customers.[31] Many civilians attempt to avoid such risk by including in their contracts or tariffs an "act of God" or "force majeure" clause. Such 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, labor strike, and failure of utilities.[32] 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 the breach unavoidable.[33] Good luck to the civilian that claims that a cyber-threat is unforeseeable and that the breach was unavoidable. Although it might be possible for a civilian with a solid IT security program to build an impossibility case, courts are not sympathetic to the doctrine.[34]

The civilian's failure to provide services as a result of damage caused by cyberwar or by the diversion of resources to support a counter-attack 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 those services with far reaching consequences along the lines of the "for want of a nail" nursery rhyme that could destroy the civilian.[35] Similarly, cyberwar could misappropriate private data which is then released in violation of contractual undertakings.

These risks sound worse, however, 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.[36] Therefore, a civilian's failure to defend against an attack or its inept participation in a defense or counter-attack is unlikely to result in

---

[31] 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 an natural gas company to access pipelines so that it can deliver gas to its customers.

[32] 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), http://www.texasbar.com/flashdrive/materials/business_law_section_cle/Business&Corporate_Bergin_Article.pdf.

[33] *See,* RESTATEMENT (SECOND) OF CONTRACS §261 (1981).

[34] *See, e.g.*, Am. Trading & Prod. Corp. v. Shell Int'l. Marine, 453 F.2d 939 (2d Cir. 1972) (finding ocean carrier not discharged of its obligation to deliver goods because of the closing of the Suez Canal on account of the Six Day War of 1967); 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).

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

[36] *See, e.g.,* UCC § 2-719.

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 they accurately describe cyberwar as a "force majeure." Third, the civilian should conduct a pre-need analysis of the ability to prove the factual predicates of the 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 to cover losses caused by third party torts even if the liability arises from contract. Moreover, the civilian may wish to investigate the availability of business interruption insurance that covers loss of revenue caused by an inability to perform (and therefore supposedly be compensated) services as a result of a covered cause.

Cyber attacks can also present contractual legal risk of an entirely different 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 (whether or not intentionally) but that they will also create contractual obligations where none exist. For example, a cyber attacker could change terms of service and legal disclaimers on websites and click-wrap agreements by eliminating disclaimers or adding promises, thereby creating liabilities where none existed.[37]

Another possible scenario is an attack on a broker/dealer that results transfers of investment securities to or from the broker's customers without their authorization with the proceeds transferred 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. Although banks, airlines, utilities, and other sellers of goods and services have virtually vitiated the contractual rights of their customers so that sellers have very

---

[37] 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 ground 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.

little risk for non-performance,[38] 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.[39] That element would presumably be difficult to prove unless the resulting deal was too good to be true.[40]

How should management respond to such a legal risk? Again, better IT security is one answer, but security is never sufficient in itself. 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 so that the frequency and amount of damage can be limited. 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 other than arising from contract that gives rise to civil liability for damages. 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 "ultrahazardous activity" might be held strictly liable for injuries arising from that activity.[41] 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 affect the civilian's relationships with third parties in a way that cause harm to the third parties.

Examples 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 an attack 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 access in American commerce.

---

[38] *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.

[39] RESTATEMENT (SECOND) OF CONTRACTS §153.

[40] 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.

[41] RESTATEMENT OF TORTS § 521(1938), The most recent version 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., 78 N.Y.2d 282 (N.Y. 1991) (holding the owner of a housing project could not recover on a products liability theory against a contractor).

In light of the universe of potential horribles, the typical response of a civilian to potential cyberwars would be, as it is with most potential tort liability risks, to use reasonable efforts to avoid or mitigate third party harm and to buy liability insurance. Whether insurance will be available, however, depends, as indicated above, on whether the insurer has excluded damage caused by cyberwars.

Cyber attacks, however, 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, there is a balancing on the part of the putative tortfeasor, here the civilian, as to 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 utility or risk of harm and the civilian is a victim with no real control over resulting harm. Instead, it 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.[42] 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.[43]

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

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

[43] *Id.*

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.[44]

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.[45] 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).

Many courts disfavor such attenuated theories of liability,[46] and narrow the reach of the doctrines by focusing on whether the alleged participant was acting in the ordinary course of its business, just grinding out "grist for the mill."[47]

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 § 876 liability was not warranted.[48] On the other hand, the Seventh Circuit in an *en banc* decision 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.[49]

While the cyberwar context is not directly analogous since the plaintiff in that case alleged that the defendants knew that the parties they funded were involved in financing terrorism, the case raises the possibility that a civilian that ignores the risk of cyberwars will not escape at least the expense of litigating claims that its failure to take prophylactic action substantially assisted the attacker in accomplishing harm to third parties, including loss of life or extensive property damage or economic loss.

C. Political Risk of Cyberwar

1. Political Risk in General

---

[44] A fine example of this is Halberstam v. Welch, 705 F.2d 472 (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).

[45] *See* Richard C. Mason, *Civil Liability for Aiding and Abetting*, 61 BUS. LAW. 1135, 1146-47 (2006).

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

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

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

[49] Boim v. Holy Land Found. for Relief & Dev., 549 F.3d 685, 704 (7th Cir. 2008).

Civilians will also evaluate the political risk inherent in any response to cyberwar. Political risk takes many different forms, but for purposes of this article, we will focus on the risk that the government will take adverse actions as a result of a civilian's failure to take actions "suggested" by a regulator. Political risk can be far most 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 continue even after the risk of attack has been reasonably addressed.

Therefore, even though political risk is less quantifiable than legal risk, it may well 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 substantially greater political risk for targets because regulators have such broad discretion that they can retaliate for a civilian's failure to cooperate with the defense of a cyber attack or with the launching of a counter-attack in subtle ways unrelated to the attack itself. Examples of regulatory risk-events are 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 counsel against cooperation is the extent to which the civilian operates in jurisdictions with conflicting interests. For example, China is considered a probable cyber-belligerent against the U.S. A U.S. multinational 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 fully cooperate with the U.S. in defending cyber attacks. Instead, its response to U.S. government jawboning may be, "We'd love to 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 request that a civilian provide to government investigators information about suppliers or customers that may have obtained unauthorized access to the civilian's IT system may 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 U.S. 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 but 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 the sanction threatened by the governmental regulator. 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 are perfected, 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 carrots or sticks. Here 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 civilian's 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.[50]

- Following the model of the USA PATRIOT Act,[51] the government could mandate adoption of internal policies and procedures, impose detailed reporting requirements, proscribe dealings with certain individuals or organizations or countries, and impose criminal sanctions for assisting or not sufficiently defending attacks.

- The government could exercise its eminent domain or taking power under the 5th Amendment by taking control and/or ownership (either temporary or permanent) of the civilian's properties, 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.[52]

- 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

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

[51] 18 U.S.C. § 1 *et seq.* (2006).

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

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 (consensual requisition) or conscription, through the acquisition of both technology and individuals or organizations familiar enough with that technology to make it a protective device or successful weapon.[53]

Technology is, of course, the means by which an outcome is accomplished and not the outcome itself. Therefore, the military may have the options 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 with potentially suitable technology that the military will choose its technology. 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.[54]

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 or other favorable procurement terms: "If you won't provide defensive resources for $x, I've got an offer you can't refuse." 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. Perceptions of 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, then, 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

[53] 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.

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

risk dominates the risk profile of a cyber attack launched solely for propaganda purposes because propaganda focuses on respective reputations of attacker and target. It follows that those attacking a civilian as part of a broader strategic propaganda campaign will focus on reputational aspects discrete from those involving the civilian's products. Such attacks may be similar to the attacks on Proctor & Gamble, which accused it of promoting Satanism.[55] For example, cyber attackers could create phishing sites or deface a civilian's own web page to associate it with unpopular causes related to the attackers' enemies.

Given the taint to personal reputations arising from associations with unpopular institutions, we can expect that civilian executives (unlike Scrooge and Midas) 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 and or to 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.[56] 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 operations; and 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 in fact 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 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 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

---

[55] *See* Procter & Gamble v. Amway, 242 F.3d 539, 542 (5th Cir. 2001).

[56] *See Conscripts*, *supra* note 6, at ___.

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 and/or determine that different risk management techniques are appropriate.[57] 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 facts that U.S. law recognizes the separate identity of the foreign subsidiary and the parent has pre-existing fiduciary duties to the subsidiary.[58]

IV. WHO IS GOING TO PAY FOR THIS?: SHIFTING CYBERWAR LOSSES

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 infra-structure 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.[59] 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 shut down 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."

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

[57] This consideration applies to legal risk and political risk as well.

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

[59] *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).

anything near comprehensive coverage even for cybercrime risks.[60] 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.[61] 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.[62] 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 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

> provide for the common defense and general welfare of the United States; to declare war; to raise and support armies to provide and maintain a navy; to make rules for the government and regulation of the land and naval forces; to provide for calling forth the militia to execute the laws of the Union, suppress insurrections and repel invasions; [63]

Article II, Section 2 gives the President unspecified powers as "Commander in Chief." 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

---

[60] 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 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.

[61] ANN KALE, ET AL., CYBER LIABILITY AND INSURANCE: MANAGING THE RISKS OF INTANGIBLE ASSETS,, (2010).

[62] APPLEMAN ON INSURANCE §1.6 (2008).

[63] U.S. CONST. art. I, § 8.

Commander in Chief, while not unlimited,[64] provides the President with sufficient portfolio to authorize military actions related to cyberwar.

On the other hand, the "Takings Clause" of the Fifth Amendment to the Constitution provides ". . . nor shall private property be taken for public use, without just compensation."[65] 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."[66]

The issue thus 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: "In wartime, many losses must be attributed solely to the fortunes of war and not to the sovereign."[67]

At the other end, the government cannot simply appropriate property on the ground it is necessary to prosecute potential wars.[68] Between these extremes is a very wide gray zone. The Supreme Court has been unwilling since the Civil War to find a military taking or to state a bright line test as to when a property owner is entitled to compensation for loss arising from military action.[69] This is not surprising, given the Court's admission that in any context "[t]he

---

[64] *See* 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).

[65] U.S. CONST. amend. V.

[66] Armstrong v. U.S, 364 U. S. 40, 49 (1960).

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

[68] Mitchell v. Harmony, 54 U.S. 115 (1852) (finding 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); U.S. v. Russell, 80 U.S. 623 (1871) (finding a steamboat owner was entitled to compensation for transporting troops during the Civil War).

[69] *See, e.g.*, Nat'l Bd. Young Men's Christian Ass'ns v. U.S., 395 U.S. 85 (1969) (holding building owners were not entitled to compensation for destruction to their building during riots in Panama because the damage occurred during conflict); El-Shifa Pharmaceutical Inds. v. U.S., 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 Young Men's Christian Ass'ns*, 39 F.2d at 472); *see also, id.* at 471: "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."

question of what constitutes a 'taking' for purposes of the Fifth Amendment has proved to be a problem of considerable difficulty."[70]

In our view, the unwillingness of the Court to establish a bright line test reflects both 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 untoward consequences.[71]

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;[72] and *U.S. v. Russell* awarded a steamboat owner compensation for transporting troops during Civil War.[73]

The bench's generosity was, however, short-lived. The seminal modern case is *U.S. v. Pacific R. Co.*,[74] which included a claim for compensation for bridges the Union Army destroyed during the Civil War to impede the advance of the Confederate Army. The Court quoted with approval a message of President Grant vetoing a bill that would have provided compensation for property taken in war. 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 to not admit a legal obligation on their part to compensate the owner."[75]

This principal that all property is 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, once and future Supreme Court Justice, set forth in a speech to the American Bar Association after he lost the 1916 Presidential election to Woodrow Wilson. Hughes,

---

[70] Penn Central Trans. Co. v. New York City, 438 U.S. 104, 123 (1978).

[71] On this point, *see,* Respublica v. Sparhawk, 1 U.S. 357, 363 (1788), in which 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.

[72] 54 U.S. at 135.

[73] 80 U.S. at 629-30.

[74] 120 U.S. 227 (1887).

[75] *Id.* at 238.

recognized that war would require regulation of industries beyond that 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 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 defence 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.[76]

[76] 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).

Since World War II, judicial respect for these necessities of war has only increased. For example, *Lichter v. U. S.*[77] reflects a strong judicial deference to the needs of a nation at war. 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.[78]

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 the Fifth Amendment. 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.[79]

The Court's equating economic regulation of business to 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 "each 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."[80] 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.

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

[77] 334 U.S. 742 (1948).

[78] *Id.* at 746 (footnote omitted).

[79] *Id.* at 754.

[80] *Id.* at 755.

> reasonable return for his wartime services than the Selective Service Act and all its related legislation give to the men in the armed forces.[81]

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."[82] In deciding what process 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, 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."[83] The Court therefore held that the procedures incorporated in the Renegotiation Act provided due process and upheld the constitutionality of the Act.[84]

United States v. Central Eureka Mining Co. is another case in which the Court held that the war power trumped the takings clause.[85] The case involved a takings challenge to an order of the War Production Board (WPB) that essentially made gold mines dormant.

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. 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

---

[81] *Id*. at 765.

[82] *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.

[83] *Lichter*, 334 U.S. at 766.

[84] *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.

[85] 357 U.S. 155, 158 *et seq.* (1958).

> 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 insignificant 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.[86]

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. In *National Board Young Men's Christian Associations v. U.S.* 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.[87] 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.[88]

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:

---

[86] *Id.* at 169 (emphasis added). Justices Frankfurter and Harlan did not view the regulation in the same perspective. Frankfurter thought that the lower court and his brethren both 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. 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 179-80. The WPB however, under the guise of regulation accomplished the equivalent of outright physical seizure of private property. 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.*

[87] 395 U.S. 85, 98-99 (1969).

[88] *Id.* at 92.

> We 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.[89]

In sum, 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.[90] The "CNG" would create a ready workforce of cyber warriors. However, as mentioned above,[91] the CNG would not be effective unless its warriors were armed with appropriate intellectual property and information technology.

Let us assume that the federal government passes a law that prohibits employers from terminating the employment of members of the CNG and requiring 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.[92] 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 their part time services even if doing so deprives the employer of part of the services it has purchased.

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 resolves 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.

---

[89] *Id.* at 93-94. *See also,* Proper v. Clark, 337 U.S. 472 (1949) (blocking owner from access to his assets is not a "taking" because it represented only temporary action).

[90] *Conscripts*, *supra* note 6, at ___.

[91] *See* supra § I.A.2.

[92] *Lichter v. U. S*, 344 U.S. 756, 765-66

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

The authorities discussed above addressed traditional, kinetic war, but their logic applies equally to cyberwar.[93] As in *Eureka*, a military order (at least one 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 WW II – 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,[94] 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 still good law, and they could require compensation for a government action that is too remote in time or in necessity. Recent jurisprudence, such as *El-Shifa Pharmaceutical Ind. v. U.S.,*[95] however, demonstrates a strong judicial deference to the other branches of government to make those nexus decisions.

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 military action inured to the civilian's overall benefit. In 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,[96] it should be equally persuasive as applied to cyber war 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

---

[93] 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); 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).

[94] *See Conscripts* at __.

[95] 820 F.3d 1346 (Fed. Cir. 2004) (Sudanese company alleging destruction of its plant by U.S. military failed to allege a valid takings claim).

[96] *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).

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 taken to deal with the threat of cyberwar should not be deemed too remote in time.

This is especially so because it is unlikely 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, a property interest that the Supreme Court has never accorded much weight, even in non-military situations.[97]

In sum, 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.

[97] *See, e.g.*, *Penn Central Trans. Co. v. New York,* 438 U.S. 104 (1978) (holding 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).