ARTICLE

Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy

Jerry Brito[1]* *& Tate Watkins***

Abstract

There has been no shortage of attention devoted to cybersecurity, with a wide range of experts warning of potential doomsday scenarios should the government not act to better secure the Internet. But this is not the first time we have been warned of impending dangers; indeed, there are many parallels between present portrayals of cyberthreats and the portrayal of Iraq prior to 2003, or the perceived bomber gap in the late 1950s.

This Article asks for a better justification for the increased resources devoted to cyber threats. It examines the claims made by those calling for increased attention to cybersecurity, and notes the interests of a military-industrial complex in playing up fears of a "cyber Katrina." Cybersecurity is undoubtedly an important policy issue. But with a dearth of information regarding the true nature of the threat, it is quite difficult to determine whether certain government policies are warranted—or if this merely represents the latest iteration of threat inflation benefitting private and parochial political interests.

Introduction

Over the past two years, there has been a steady drumbeat of alarmist rhetoric coming out of Washington about potential catastrophic cyber threats. For example, at a Senate Armed Services Committee hearing last year, Chairman Carl Levin said, "cyberweapons and cyberattacks potentially can be devastating, approaching weapons of mass destruction in

* Senior Research Fellow, Mercatus Center at George Mason University. J.D., George Mason University School of Law, 2005; B.A., Political Science, Florida International University, 1999. The authors would like to thank Jerry Ellig, Jim Harper, Adam Thierer, Dan Rothschild, and Richard Williams for their helpful comments on drafts of this article.
** Research Associate, Mercatus Center at George Mason University. M.A., Economics, Clemson University, 2008; B.A., Economics, Clemson University, 2007.

their effects."[2] Proposed responses include increased federal spending on cybersecurity and the regulation of private network security practices.

Security risks to private and government networks from criminals and malicious state actors are no doubt real and pressing. However, the rhetoric of "cyber doom"[3] employed by proponents of increased federal intervention in cybersecurity implies an almost existential threat that requires instant and immense action. Yet these proponents lack clear evidence of such doomsday threats that can be verified by the public. As a result, the United States may be witnessing a bout of threat inflation similar to that seen in the run-up to the Iraq War. Additionally, a cyber-industrial complex is emerging, much like the military-industrial complex of the Cold War. This complex may serve not only to supply cybersecurity solutions to the federal government, but to drum up demand for those solutions as well.

Part I of this article draws a parallel between today's cybersecurity debate and the run-up to the Iraq War and looks at how an inflated public conception of the threat we face may lead to unnecessary regulation of the Internet. Part II draws a parallel between the emerging cybersecurity establishment and the military-industrial complex of the Cold War and looks at how unwarranted external influence can lead to unnecessary federal spending. Finally, Part III surveys several federal cybersecurity proposals and presents a framework for soberly analyzing the cybersecurity threat.

I. Threat Inflation, the Iraq War, and Parallels to the Present Debate

Threat inflation is a concept in political science that refers to "the attempt by elites to create concern for a threat that goes beyond the scope

---

[2] *Nominations of VADM James A. Winfield, Jr., USN, to be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Defense Command; and LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander U.S. Cyber Command: Before the S. Comm. on Armed Servs.*, 111th Cong. 3 (2010) (statement of Senator Carl Levin), *available at* http://armed-services.senate.gov/Transcripts/2010/04%20April/10-32%20-%204-15-10.pdf [hereinafter *Confirmation Hearings*].

[3] Sean Lawson, *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History* (Mercatus Ctr. at George Mason Univ., Working Paper No. 11-01, 2011), *available at* http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

and urgency that a disinterested analysis would justify."[4] Different actors—including members of Congress; defense contractors; journalists; policy experts; academics; and civilian, military, and intelligence officials—will each have their own motives for contributing to threat inflation. When a threat is inflated, the marketplace of ideas on which a democracy relies to make sound judgments—in particular, the media and popular debate—can become overwhelmed by fallacious information.[5] The result can be unwarranted public support for misguided policies. The run-up to the Iraq War illustrates the dynamic of threat inflation, and the current conversation around cybersecurity exhibits striking parallels to that period.

A. Run-Up to the Iraq War

After 9/11, the Bush Administration decided to invade Iraq to oust Saddam Hussein.[6] Lacking any clear *casus belli*, the administration sought popular and congressional support for war by promoting several rationales that ultimately proved baseless.[7]

---

[4] Jane K. Cramer & A. Trevor Thrall, *Understanding Threat Inflation*, *in* AMERICAN FOREIGN POLICY AND THE POLITICS OF FEAR 1, 1 (A. Trevor Thrall & Jane K. Cramer, eds., 2009).
[5] *Id.*
[6] Joel Roberts, *Plans For Iraq Attack Began On 9/11*, CBS NEWS (Sept. 4, 2002), http://www.cbsnews.com/stories/2002/09/04/september11/main520830.shtml (noting that Defense Secretary Donald Rumsfeld told aides to draw plan for an attack on Iraq hours after the 9/11 attack on the Pentagon). RICHARD A. CLARKE, AGAINST ALL ENEMIES 30–31 (2004) (explaining that during response planning meetings on September 12, 2001, Rumsfeld and other high-level officials advocated an attack on Iraq despite a lack of evidence to suggest a connection to the 9/11 attacks).
[7] For an overview of false and misleading administration claims leading to the Iraq War, see Chaim Kaufmann, *Threat Inflation and the Failure of the Marketplace of Ideas: The Selling of the Iraq War*, 29 INT'L SECURITY 5 (2004); James P. Pfiffner, *Did President Bush Mislead the Country in His Arguments for War with Iraq?*, 34 PRESIDENTIAL STUD. Q. 25 (2004); Murray Waas, *Prewar Intelligence: Insulating Bush*, NAT'L J., Mar. 30, 2006, at 36; *see also* S. SELECT COMM. ON INTELLIGENCE, REPORT ON INTELLIGENCE ACTIVITIES RELATING TO IRAQ CONDUCTED BY THE POLICY COUNTERTERRORISM EVALUATION GROUP AND THE OFFICE OF SPECIAL PLANS WITHIN THE OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR POLICY, S. REP. 110-346 (2008), *available at* http://intelligence.senate.gov/080605/phase2b.pdf; S. SELECT COMM. ON INTELLIGENCE, REPORT ON WHETHER PUBLIC STATEMENTS REGARDING IRAQ BY U.S. GOVERNMENT OFFICIALS WERE SUBSTANTIATED BY INTELLIGENCE INFORMATION, S. REP. 110-345 (2008), *available at* http://intelligence.senate.gov/080605/phase2a.pdf; JOSEPH CIRINCIONE ET AL., CARNEGIE ENDOWMENT FOR INT'L PEACE, WMD IN IRAQ: EVIDENCE AND IMPLICATIONS (2004).

First, the administration implied that the Iraqi regime was connected to the terrorist attacks on 9/11.[8] In a major speech outlining the Iraqi threat in October of 2002, President Bush stated that Iraq and al Qaeda had longstanding links, and that Iraq had provided training and medical treatment to members of al Qaeda.[9] Vice President Cheney on various occasions made the claim that 9/11 hijacker Mohamed Atta had met with an Iraqi official in Prague in 2001.[10] Defense Secretary Donald Rumsfeld called evidence of the link "bulletproof," and Condoleezza Rice echoed those claims.[11]

We now know that there was no solid evidence for those statements.[12] For one thing, al Qaeda, under the direction of Osama Bin Laden, was a fundamentalist Muslim organization that despised the secular government of Saddam Hussein.[13] More specifically, investigations by the Federal Bureau of Investigation, Central Intelligence Agency (CIA), and the United Nations concluded that these links did not exist.[14] Mohamed Atta, for example, was in Florida at the time the alleged Prague meeting took place.[15]

President Bush ultimately admitted that he "had no evidence that Saddam Hussein was involved with September 11th," but he did so only after the Iraq War had commenced.[16] As late as 2006, however, over 40 percent of Americans surveyed still said they believed Saddam Hussein was "personally" involved in the 9/11 attacks.[17]

---

[8] James P. Pfiffner, *supra* note 7, at 28.
[9] President George W. Bush, Remarks by the President on Iraq (Oct. 7, 2002), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2002/10/20021007-8.html.
[10] Pfiffner, *supra* note 7, at 26–27.
[11] Eric Schmitt, *Rumsfeld Says U.S. Has 'Bulletproof' Evidence of Iraq's Links to Al Qaeda*, N.Y. TIMES, Sept. 28, 2002, at A9, *available at* http://www.nytimes.com/2002/09/28/world/threats-responses-intelligence-rumsfeld-says-us-has-bulletproof-evidence-iraq-s.html.
[12] Pfiffner, *supra* note 7, at 27.
[13] *Id.* at 26.
[14] *Id.* at 27.
[15] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 228 (2004).
[16] Pfiffner, *supra* note 7, at 28.
[17] *Poll: Iraq War Could Wound GOP at Polls*, CNN (Sept. 6, 2006), http://articles.cnn.com/2006-09-06/politics/iraq.poll_1_iraq-war-sampling-error-poll-results-show?_s=PM:POLITICS.

Second, the administration also sought to make the case that Iraq threatened its neighbors and the United States with weapons of mass destruction (WMD). By framing the issue in terms of WMD, the administration conflated the threat from nuclear, biological, and chemical weapons.[18] While no doubt terrible, the destructive power of biological and chemical weapons is tiny next to that of a nuclear detonation.[19] Conflating these threats, however, allowed the administration to link the unlikely but serious threat of nuclear weapons to the more likely but less serious threat posed by biological and chemical weapons.[20]

The President, Vice President, and senior members of the administration made the claim that Iraq was close to acquiring nuclear weapons.[21] They made these claims without providing any verifiable evidence. The evidence they did provide—Iraq's alleged pursuit of uranium "yellowcake" from Niger and its purchase of aluminum tubes allegedly meant for uranium enrichment centrifuges—were ultimately determined to be unfounded.[22] The administration was also aware at the time that the evidence it was presenting was problematic. The CIA had investigated the claim that Iraq had attempted to buy yellowcake in Niger and concluded that it was false.[23] Weeks before the invasion, it was revealed that the documents on which the claim had been predicated were forgeries.[24] Similarly, technical experts at the Department of Energy had concluded

---

[18] Pfiffner, *supra* note 7, at 28.

[19] *See* Wolfgang K.H. Panofsky, *Dismantling the Concept Of "Weapons of Mass Destruction"*, ARMS CONTROL TODAY, Apr. 1998, at 3; *see also* KENNETH M. POLLACK, THE THREATENING STORM 179 (2002), *cited in* Pfiffner, *supra* note 7, at 29 n.14.

[20] For example, Vice President Cheney was able to make statements such as: "Many of us are convinced that Saddam will acquire nuclear weapons fairly soon. . . . There is no doubt he is amassing [WMD] to use against our friends, against our allies, and against us." Pfiffner, *supra* note 7, at 29 (quoting Vice President Richard Cheney, Remarks by the Vice President to the Veterans of Foreign Wars 103rd National Convention, Aug. 26, 2002, *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2002/08/20020826.html).

[21] *Id.*

[22] Pfiffner, *supra* note 7, at 30–36; Barton Gellman & Walter Pincus, *Depiction of Threat Outgrew Supporting Evidence*, WASH. POST, Aug. 10, 2003, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200932.html.

[23] Pfiffner, *supra* note 7, at 31–32; Joseph C. Wilson IV, *What I Didn't Find in Africa*, N.Y. TIMES, July 6, 2003, at F8, *available at* http://www.nytimes.com/2003/07/06/opinion/what-i-didn-t-find-in-africa.html?pagewanted=all&src=pm.

[24] Pfiffner, *supra* note 7, at 32.

that the aluminum tubes that had been purchased by Iraq were not suitable for uranium enrichment and were likely meant to build artillery rockets.[25]

Despite the lack of verifiable evidence to support the administration's claims, the news media tended to report them unquestioned.[26] The initial reporting on the aluminum tubes claim, for example, came in the form of a front page *New York Times* article by Judith Miller and Michael Gordon that relied entirely on anonymous administration sources.[27] The article gave the impression that there was consensus that the tubes were meant for uranium enrichment.[28] Later reporting by Miller and Gordon noted that, in fact, there were dissenting opinions on the purpose of the tubes among government experts.[29] However, they were quick to dismiss those views, citing "other, more senior, officials" who insisted that the skeptics represented a minority view.[30]

One reason why the *New York Times* reports have been criticized so strongly is that they were later cited by the administration in making its case for war.[31] Appearing on *Meet the Press*, Vice President Cheney answered a question about evidence of a reconstituted Iraqi nuclear program by stating:

> There's a story in *The New York Times* this morning—this is—I don't—and I want to attribute *The Times*. I don't want to talk about, obviously, specific intelligence sources, but it's now public that, in fact, [Saddam Hussein] has been seeking to acquire, and we have been able to intercept and prevent him from acquiring through this particular channel, the kinds of tubes that are necessary to build a centrifuge.[32]

---

[25] *Id.* at 35–36.
[26] CALVIN F. EXOO, THE PEN AND THE SWORD: PRESS, WAR, AND TERROR IN THE 21ST CENTURY 97 (2010); Michael Massing, *Now They Tell Us*, N.Y. REV. OF BOOKS, Feb. 26, 2004, *available at* http://www.nybooks.com/articles/archives/2004/feb/26/now-they-tell-us.
[27] Michael R. Gordon & Judith Miller, *U.S. Says Hussein Intensifies Quest For A-Bomb Parts*, N.Y. TIMES, Sept. 8, 2002, at A1, *available at* http://www.nytimes.com/2002/09/08/world/threats-responses-iraqis-us-says-hussein-intensifies-quest-for-bomb-parts.html?pagewanted=all&src=pm; Massing, *supra* note 26.
[28] Massing, *supra* note 26.
[29] *Id.*
[30] *Id.*
[31] MICHAEL ISIKOFF & DAVID CORN, HUBRIS 33–34 (2006).
[32] *Meet the Press* (NBC television broadcast Sept. 8, 2002), *available at*

The administration was able to cite its own leak—with the added imprimatur of the *Times*—as a rationale for war.

Miller, who was criticized after the invasion for her credulous reporting, has defended herself by stating that as a reporter, "my job isn't to assess the government's information and be an independent intelligence analyst myself. My job is to tell readers of *The New York Times* what the government thought about Iraq's arsenal."[33] This view of reporting as mere conduit for anonymous administration officials is dangerous because it can serve to give the endorsement of an independent media on controlled leaks by government insiders.[34]

Most members of Congress similarly took the administration at its word and were uncritical of the evidence underpinning the rationales for war. As Ronald R. Krebs and Jennifer Lobasz write,

> A large and critical group of Democrats, whose national profiles might have bolstered the opposition to war, shied away from criticizing the popular president leading the War on Terror: while a handful jumped enthusiastically on the Iraq bandwagon, many others quietly favored invasion or at most criticized unilateral action.[35]

While there are competing theories why it may have been the case,[36] the fact is that our system of checks and balances failed to test the evidence of a serious threat from Iraq.

B. Cyber Threat Inflation

Over the past two years, there has been a drive for increased federal involvement in cybersecurity. This drive is evidenced by the introduction of several comprehensive cybersecurity bills in Congress,[37] the initiation of

---

http://www.mtholyoke.edu/acad/intrel/bush/meet.htm.

[33] Massing, *supra* note 26.

[34] *Id.* (noting that Cheney, Rice, and others pointed to the *New York Times* report as evidence of WMD).

[35] Ronald R. Krebs & Jennifer Lobasz, *The Sound of Silence: Rhetorical Coercion, Democratic Acquiescence, and the Iraq War*, *in* AMERICAN FOREIGN POLICY AND THE POLITICS OF FEAR 117, 123 (A. Trevor Thrall & Jane K. Cramer, eds., 2009).

[36] *Id.* at 120.

[37] *See, e.g.*, Protecting Cybersecurity as a National Asset Act of 2010, S. 3480, 111th Cong.

several regulatory proceedings related to cybersecurity by the Federal Communications Commission and Commerce Department,[38] and increased coverage of the issue in the media.[39] The official consensus in Congress seems to be that the United States is facing a grave and immediate threat that only quick federal intervention can address.[40] This narrative has gone largely unchallenged by members of Congress or the press, and it has inflated the threat.

There is very little verifiable evidence to substantiate the threats claimed, and the most vocal proponents of a threat engage in rhetoric that can only be characterized as alarmist. Cyber threat inflation parallels what we saw in the run-up to the Iraq War.

1. The CSIS Commission Report

One of the most widely cited arguments for increased federal involvement in cybersecurity can be found in the report of the Commission on Cybersecurity for the 44th Presidency.[41] The Commission was convened

---

(2010); Cybersecurity Act of 2009, S. 773, 111th Cong. (2009).

[38] *See, e.g.*, FED. COMMC'NS. COMM'N, NATIONAL BROADBAND PLAN ch. 16 (2010), *available at* http://download.broadband.gov/plan/national-broadband-plan-chapter-16-public-safety.pdf; *see also* FED. COMMC'NS COMM'N, PUBLIC NOTICE ON CYBERSECURITY ROADMAP (Sept. 23, 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-10-1354A1.pdf; DEP'T OF COMMERCE, NOTICE OF INQUIRY ON CYBERSECURITY, INNOVATION, AND THE INTERNET ECONOMY, (July 28, 2010), *available at* http://www.nist.gov/itl/csd/upload/Cybersecurity_NOI_0722101.pdf; FED. COMMC'NS COMM'N, NOTICE OF INQUIRY ON PROPOSED CYBER SECURITY CERTIFICATION PROGRAM FOR COMMUNICATIONS SERVICE PROVIDERS (Apr. 21, 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-63A1.pdf.

[39] *Google Trends, "cybersecurity,"* GOOGLE (Mar. 18, 2011), http://www.google.com/trends?q=cybersecurity&ctab=0&geo=us&date=all&sort=0.

[40] For example, in a letter to President Obama last year, seven Senators noted that "[t]hreats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century" and wrote "[they] believ[ed] that there is an urgent need for action to address these vulnerabilities by the Administration, by Congress, and by the array of entities affected by cyber threats." Letter from Sens. Harry Reid, Patrick Leahy, Carl Levin, John Kerry, John Rockefeller, Joseph Lieberman, and Dianne Feinstein to Barack Obama, President of the United States (July 1, 2010), *available at* http://fcw.com/blogs/cybersecurity/2010/07/~/media/GIG/GIG_Shared_PDF_Library/Editorial%20PDFs/Letter_President_Cyber_Security070110.ashx.

[41] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (Dec. 2008) [hereinafter Commission Report]; Eric Chabrow, *Cyber*

by the Center for Strategic and International Studies (CSIS), a Washington think tank focused on foreign policy and defense. It was chaired by two members of Congress and composed of representatives of the IT industry, security consultants, academics, and former government officials.[42] Beginning in February 2008, the Commission acted as a self-appointed transition team for whoever the next president would be. It held a series of open and closed-door meetings, received classified briefings from government officials,[43] and in December issued its report warning that "cybersecurity is now a major national security problem for the United States,"[44] and recommending that the federal government "regulate cyberspace."[45]

In its report, the Commission makes assertions about the nature of the threat, such as, "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. It is . . . a battle fought mainly in the shadows. It is a battle we are losing."[46] Unfortunately, the report provides little evidence to support such assertions. There is a brief recitation of various instances of cyber-espionage conducted against government computer systems.[47] However, it does not explain how these particular breaches demonstrate a national security crisis, or that "we are losing."

The report notes that Department of Defense computers are "probed hundreds of thousands of times each day."[48] This is a fact that proponents of increased federal involvement in cybersecurity often cite as evidence for a looming threat.[49] However, probing and scanning networks

---

Commission Has a Hard Act to Follow, GOVINFOSECURITY.COM (Aug. 4, 2010), http://www.govinfosecurity.com/articles.php?art_id=2814 (noting that the Commission Report is highly regarded and has "served as the basis for President Obama's Cyberspace Policy Review and key cybersecurity bills before Congress").

[42] Commission Report, *supra* note 41, app. A.

[43] *Id.* app. C.

[44] *Id.* at 1.

[45] *Id.* at 2.

[46] *Id.* at 11.

[47] *Id.* at 12–13.

[48] *Id.* at 12. We should note that evidence presented in support of regulation of private networks is often that of attacks perpetrated upon government systems. In our view this improperly conflates the two spheres.

[49] For example, while defending a cybersecurity bill that he co-sponsored, Senator Joseph Lieberman claimed that the Internet was "constantly being probed by other countries for weaknesses." Deborah Solomon, *Lieberman Dismisses Concerns Over Internet Bill*, WALL ST. J.,

are the digital equivalent of trying doorknobs to see if they are unlocked—a maneuver available to even the most unsophisticated would-be hackers.[50] The number of times a computer network is probed is not evidence of an attack, a breach, or even of a problem.[51]

> More ominously, the report states that
>
> Porous information systems have allowed opponents to map our vulnerabilities and plan their attacks. Depriving Americans of electricity, communications, and financial services may not be enough to provide the margin of victory in a conflict, but it could damage our ability to respond and our will to resist. We should expect that exploiting

---

Jun. 20, 2010, *available at* http://blogs.wsj.com/washwire/2010/06/20/lieberman-dismisses-concerns-over-internet-bill/tab/print/. U.S. Deputy Secretary of Defense William Lynn III wrote in *Foreign Affairs*: "Over the past ten years, the frequency and sophistication of intrusions into U.S. military networks have increased exponentially. Every day, U.S. military and civilian networks are probed thousands of times and scanned millions of times." William J. Lynn III, *Defending a New Domain*, FOREIGN AFF., Sept.–Oct. 2010, *available at* http://www.foreignaffairs.com/print/66687. When asked how often federal networks are targeted or probed each day, Representative Adam Smith of Washington replied, "[n]orth of a million times." Joel Connelly, *Cyber Attacks: The Next Big Security Threat?*, SEATTLE POST INTELLIGENCER (Apr. 11, 2010), http://www.seattlepi.com/default/article/Cyber-attacks-The-next-big-security-threat-891683.php. Robert Lentz, Chief Information Assurance Officer for the Department of Defense, has said that Defense Department networks are probed 360 million times each day. Declan McCullagh, *NSA Chief Downplays Cybersecurity Power Grab Reports*, CNET (Apr. 21, 2009), http://news.cnet.com/8301-13578_3-10224579-38.html.

[50] For example, in response to claims that U.S. networks have been penetrated by "cyberwarriors from 'hostile powers,'" security expert Marcus Ranum notes that "all websites are constantly probed for weaknesses by robotic worms, spammers, hackers, and maybe even a government agent or two." Marcus Ranum, *Cyberwar Rhetoric Is Scarier Than Threat of Foreign Attack*, U.S. NEWS AND WORLD REP., Mar. 29, 2010, *available at* http://www.usnews.com/opinion/articles/2010/03/29/cyberwar-rhetoric-is-scarier-than-threat-of-foreign-attack_print.html. Evgeny Morozov, visiting scholar in the Liberation Technology Program at Stanford University, notes that the claim that U.S. networks are probed is "so vague that even some of the most basic attacks available via the Internet—including those organized by 'script kiddies,' or amateurs who use scripts and programs developed by professional hackers—fall under this category." Evgeny Morozov, *Battling the Cyber Warmongers*, WALL ST. J., May 8, 2010, at W3, *available at* http://online.wsj.com/article/SB10001424052748704370704575228653351323986.html. *See also* Sean Lawson, *Just How Big Is The Cyber Threat To The Department Of Defense?*, FORBES: THE FIREWALL (Jun. 4, 2010), http://blogs.forbes.com/firewall/2010/06/04/just-how-big-is-the-cyber-threat-to-dod.

[51] Lawson, *supra* note 50.

> vulnerabilities in cyber infrastructure will be part of any future conflict.[52]

An enemy able to take down our electric, communications, and financial networks at will could be a serious national security threat. And it may well be the case that the state of security in government and private networks is deplorable. But the CSIS report advances no reviewable evidence to substantiate this supposed threat. There is no evidence in the report that opponents have "mapped vulnerabilities" and "planned attacks." The probing of DoD computers and the specific cases of cyber espionage that the report cites do not bear on the probability of a successful attack on the electrical grid.

Nevertheless, the Commission report and the cybersecurity bills it inspired prescribe regulation of the Internet. The report asserts plainly: "It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives."[53] But without any verifiable evidence of a threat, how is one to know what exactly is the "appropriate level of cybersecurity" and whether market forces are providing it? How is one to judge whether the recommendations that make up the bulk of the Commission's report are necessary or appropriate?

Although never clearly stated, the implication seems to be that the report's authors are working from classified sources, which might explain the dearth of verifiable evidence.[54] To its credit, the Commission laments what it considers the "overclassification" of information related to cybersecurity.[55] But this should not serve as an excuse. If our past experience with threat inflation teaches us anything, it is that we should be wary of accepting the word of government officials with access to classified information as the sole source of evidence for the existence or scope of a threat. The watchword is "trust but verify." Until those who seek regulation can produce clear reviewable evidence of a threat, we should discount assertions such as "[t]he evidence is both compelling and overwhelming,"[56]

---

[52] Commission Report, *supra* note 41, at 13.
[53] *Id.* at 50.
[54] *E.g. id.* at 12–13 (citing unnamed government officials and alleged espionage).
[55] *Id.* at 27–28.
[56] *Id.* at 13.

and, [t]his is a strategic issue on par with weapons of mass destruction and global jihad."[57]

2. Cyber War

While the CSIS Commission report may be one of the most cited documents suggesting that we face a grave cyber threat requiring an immediate federal response, the most popular brief for this view is the 2010 bestselling book *Cyber War*.[58] In it, former presidential cybersecurity advisor Richard A. Clarke and Council on Foreign Relations fellow Richard K. Knake make the case that the United States and its infrastructure is extremely vulnerable to military cyber attack by enemy states. They offer a set of recommendations that includes increased regulation of Internet service providers (ISPs) and electrical utilities.[59]

Clarke and Knake are clear about the threat they foresee. "Obviously, we have not had a full-scale cyber war yet," they write, "but we have a good idea what it would look like if we were on the receiving end."[60] The picture they paint includes the collapse of the government's classified and unclassified networks, refinery fires and explosions in cities across the country, the release of "lethal clouds of chlorine gas" from chemical plants, the midair collision of 737s, train derailments, the destruction of major financial computer networks, suburban gas pipeline explosions, a nationwide power blackout, and satellites in space spinning out of control.[61] They explain somberly about the scene:

> Several thousand Americans have already died, multiples of that number are injured and trying to get to hospitals. . . . In the days ahead, cities will run out of food because of the train-system failures and the jumbling of data at trucking and distribution centers. Power will not come back up because nuclear plants have gone into secure lockdown and many conventional plants have had their generators permanently damaged. High-tension transmission lines on several key routes have caught fire and melted. Unable to get cash from

---

[57] *Id.* at 15.
[58] RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR (2010).
[59] *Id.* at 160, 167.
[60] *Id.* at 64.
[61] *Id.* at 66–67.

> ATMs or bank branches, some Americans will begin to loot stores. . . . In all the wars America has fought, no nation has ever done this kind of damage to our cities. A sophisticated cyber war attack by one of several nation-states could do that today, in fifteen minutes, without a single terrorist or soldier appearing in this country.[62]

According to Clarke and Knake, that is the threat we face unless the federal government takes immediate action. Readers of their bestselling book would no doubt be as frightened at the prospect of a cyber attack as they might have been at the prospect of Iraq passing nuclear weapons to al Qaeda. Yet Clarke and Knake assure us, "These are not hypotheticals."[63] Unfortunately, they present little, if any, evidence.[64]

The only verifiable evidence they present to support the possibility of a cyber doomsday relates to several well-known distributed denial of service (DDOS) attacks. A DDOS attack works by flooding a server on the Internet with more requests than it can handle, thereby causing it to malfunction. For example, the web server that hosts www.gmu.edu has a certain limited bandwidth and processing capacity with which to serve George Mason University's home page to visitors.[65] If several dozen persons were browsing university web pages and simultaneously requested GMU's homepage, the server would likely perform perfectly well. However, if the server encountered a hundred thousand requests for the home page every second, it would be overwhelmed and would likely shut down.

A person carrying out a DDOS attack will almost certainly employ a botnet to cause the massive flood of requests on the attacked server. A botnet is a network of computers that have been compromised without their users' knowledge, usually through a computer virus.[66] The attacker remotely controls these computers and commands them to carry out the attack.[67]

---

[62] *Id.* at 67–68.
[63] *Id.* at 70.
[64] Apart from the sorry state of the evidence they do present, the book does not have footnotes, a bibliography, or even an index.
[65] Different organizations will secure different capacities depending on the traffic they receive. *The New York Times* or Amazon.com, for example, would secure much more capacity than George Mason University for their web servers.
[66] Michel van Eeten & Johannes M. Bauer, *Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications*, 17 J. OF CONTINGENCIES & CRISIS MGT. 221, 222 (2009).
[67] *Id.*

Experts have estimated that over 25 percent of personal computers are compromised and form part of a botnet.[68]

Clarke and Knake point to several well-known DDOS attacks as evidence of a threat. Specifically, they cite attacks on Estonia in 2007 and Georgia in 2008, both suspected by many to have been coordinated by Russia.[69] They also mention an attack on U.S. and North Atlantic Treaty Organization (NATO) websites after the 1999 accidental bombing of the Chinese embassy in Belgrade,[70] and a July 4, 2009 attack on U.S. and South Korean websites widely attributed to North Korea.[71] These reputedly state-sponsored attacks, along with the hundreds of thousands of other DDOS attacks by criminals and vandals seen each year,[72] are evidence of the sorry state of consumer computer security and of how vulnerable publicly accessible servers can be. They are not, however, evidence of the type of capability necessary to derail trains, release chlorine gas, or bring down the power grid.

The authors admit that a DDOS attack is often little more than a nuisance.[73] The 1999 attack saw websites temporarily taken down or defaced, but "did little damage to U.S. military or government operations."[74] Similarly, the 2009 attacks against the United States and South Korea caused several government agency websites, as well as the websites of NASDAQ, the New York Stock Exchange, and the *Washington Post* to be intermittently inaccessible for a few hours, but did not threaten the integrity of those institutions.[75] In fact, Clarke points out that the White

---

[68] *See* Byron Acohido & Jon Swartz, *Botnet Scams are Exploding*, USA TODAY, March 16, 2008, at B1 (quoting experts suggesting that up to 40% of computers are part of a botnet); Tim Weber, *Criminals 'May Overwhelm the Web'*, BBC NEWS (Jan. 25, 2007), http://news.bbc.co.uk/2/hi/business/6298641.stm (quoting several computer experts suggesting that up to a quarter of computers may part of a botnet).

[69] CLARKE & KNAKE, *supra* note 58, at 13, 15, & 18–20.

[70] *Id.* at 54–55.

[71] *Id.* at 24–25.

[72] Network security firm Arbor Networks' worldwide systems measured more than 300,000 "DDOS events" in 2010. Email from Jose Nazario, Senior Manager of Security Research, Arbor Networks (Jan. 4, 2011).

[73] CLARKE & KNAKE, *supra* note 58, at 55.

[74] *Id.*

[75] *Id.* at 24–25 ("The attack did not attempt to gain control of any government systems, nor did it disrupt any essential services."); Choe Sang-Hun & John Markoff, *Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea*, N.Y. TIMES, July 9, 2009, at A4 (noting that the attacks were "relatively minor, and all but two of the sites were fully

House's servers were able to easily deflect the attack thanks to the simple technique of "edge caching," which he had arranged as cybersecurity coordinator.[76]

Without any formal regulation mandating that it be done, the affected agencies and businesses worked with Internet service providers to filter out the attacks.[77] Once the attackers realized they were no longer having an effect, the attacks stopped.[78] Georgia similarly addressed attacks on its websites by moving them to more resilient servers hosted outside of the country.[79]

Clarke and Knake recognize that DDOS is an unsophisticated and "primitive" form of attack that would not pose a major threat to national security.[80] Nevertheless, reference to DDOS attacks make up the bulk of the verifiable evidence they present. They assert, however, that the reason we have no verifiable evidence of a greater threat is that "attackers did not want to reveal their more sophisticated capabilities, yet."[81] Specifically referring to the Georgian and Estonian episodes, they write that "[t]he Russians are probably saving their best cyber weapons for when they really need them, in a conflict in which NATO and the United States are involved."[82] The implication is eerily reminiscent of the suggestion before the invasion of Iraq that although we lacked the type of evidence of WMD that might lead us to action, we would not want "the smoking gun to be a mushroom cloud."[83]

Clarke and Knake present no proof to corroborate the type of vulnerabilities that could pose a serious national security risk. For example,

---

functional within a few hours").

[76] CLARKE & KNAKE, *supra* note 58, at 24.

[77] *Id.* at 25.

[78] *Id.*

[79] *Id.* at 19. Clarke and Knake also mention that banking, settlement, and mobile phone systems were disrupted by DDOS. *Id.* at 20. However, there is no footnote or other verifiable reference and Internet searches have returned no mention of phone system malfunction. Additionally, the in-depth post-incident report released by NATO does not mention such a malfuntion. *See* NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, CYBER ATTACKS AGAINST GEORGIA: LEGAL LESSONS IDENTIFIED (Nov. 2008), *available at* http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

[80] CLARKE & KNAKE, *supra* note 58, at 30, 55, 103, 191 & 257.

[81] *Id.* at 31.

[82] *Id.* at 21.

[83] Pfiffner, *supra* note 8, at 29.

one of the threats they identify as most serious is a sustained nationwide power outage.[84] The evidence they offer is either not reviewable or easily debunked.

To show that the electrical grid is vulnerable, they suggest that the Northeast power blackout of 2003 was caused in part by the "Slammer" worm, which had been spreading across the Internet around that time.[85] However, the final report of the joint U.S.–Canadian task force that investigated the blackout explained clearly in 2004 that no virus, worm, or other malicious software contributed to the power failure.[86] Clarke and Knake also point to a 2007 blackout in Brazil, which they believe was the result of criminal hacking of the power system.[87] However, separate investigations by the utility company involved, Brazil's independent systems operator, and the energy regulator all concluded that the power failure was the result of soot and dust deposits on high voltage insulators on transmission lines.[88]

Given the weakness of the public evidence they offer, it is difficult to trust the evidence Clarke and Knake present based on anonymous sources. Specifically, they write that countries such as China have "laced U.S. infrastructure with logic bombs."[89] That is, hackers have penetrated the control systems of utilities, including the electrical grid, and left behind computer programs that can later be triggered remotely to cause damage.[90] Depending on the scope of the intrusions and which systems are

---

[84] CLARKE & KNAKE, *supra* note 58, at 98.
[85] *Id.* at 99.
[86] U.S.–CANADA POWER SYSTEM OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS 133 (Apr. 2004), *available at* https://reports.energy.gov/BlackoutFinal-Web.pdf. The cause of the blackout was ultimately attributed to, among other things, overgrown trees making contact with power lines, which contributed to a cascading failure. *Id.* at 57–64.
[87] CLARKE & KNAKE, *supra* note 58, at 99.
[88] Marcelo Soares, *Brazilian Blackout Traced to Sooty Insulators, Not Hackers*, WIRED: THREAT LEVEL (Nov. 9, 2009), http://www.wired.com/threatlevel/2009/11/brazil_blackout. Days after the *60 Minutes* broadcast, Brazil was hit with another blackout, but a secret State Department cable released by Wikileaks shows that the U.S. embassy in Brasilia determined that it too was not the work of hackers. Brian Krebs, *Cable: No Cyber Attack in Brazilian '09 Blackout*, KREBS ON SECURITY (Dec. 3, 2010), http://krebsonsecurity.com/2010/12/cable-no-cyber-attack-in-brazilian-09-blackout.
[89] CLARKE & KNAKE, *supra* note 58, at 54, 59, & 62.
[90] *Id.* at 92.

compromised, this could pose a serious threat. However, Clarke and Knake present only suppositions, not evidence.

We are told that "America's national security agencies are now getting worried about logic bombs, since they *seem* to have found them all over our electric grid,"[91] and that "[enemies] have *probably* done everything short of a few keystrokes of what they would do in real cyber war."[92] This is speculation.

The notion that our power grid, air traffic control system, and financial networks are rigged to blow at the press of a button would be terrifying if it were true. But fear should not be a basis for public policy making. We learned after the invasion of Iraq to be wary of conflated threats and flimsy evidence. If we are to pursue the type of regulation of Internet service providers and utilities that Clarke and Knake advocate, we should demand more precise evidence of the threat against which we intend to guard, and of the probability that such a threat can be realized.

One piece of evidence unavailable to Clarke and Knake when they were writing their book was the emergence of Stuxnet, a highly sophisticated worm discovered in June 2010.[93] Stuxnet targets a particular type of Siemens industrial control system, and many believe it was created by a state to target Iran's nuclear program.[94] The Stuxnet worm, and the effect it is widely believed to have had on Iran's Bushehr nuclear enrichment plant, is exactly the type of evidence that officials and the public should seek. The malware has been isolated and decompiled and its code is available for examination. Its effect on Iran's centrifuges has also been largely confirmed.[95] As a result, Stuxnet represents a verifiable threat, not mere conjecture.

---

[91] *Id.* at 92 (emphasis added).
[92] *Id.* at 191 (emphasis added).
[93] Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED: THREAT LEVEL (Jul. 11, 2011), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet.
[94] *Id.*
[95] *Id. See also* Kim Zetter, *Iran: Computer Malware Sabotaged Uranium Centrifuges*, WIRED: THREAT LEVEL (Nov. 29, 2010), http://www.wired.com/threatlevel/2010/11/stuxnet-sabotage-centrifuges.

It should be noted, however, that Stuxnet is simply one data point. As many have pointed out,[96] including Clarke,[97] Stuxnet is the first-of-its-kind example of such a cyber weapon. The fact of its existence tells us only that such weapons are a possible threat. It tells us nothing about the probability that such weapons could or would be used to take down power grids or derail trains. Nor does it tell us whether any specific regulation would help mitigate such a threat.

Clarke and Knake lament their position when they write, "How do you convince someone that they have a problem when there is no evidence you can give them?"[98] Like the CSIS Commission, they recognize that there is insufficient public debate because much of the information about the state of cybersecurity is classified.[99] Citizens should trust but verify, as they are able to do with the Stuxnet worm. That will require declassification and a more candid, on-the-record discussion of the threat by government officials.

3. The Media and Other Experts

Much as in the run-up to the Iraq War, some in the media may be contributing to threat inflation by reporting the alarmist view of a possible threat in a generally uncritical fashion. For example, while Clarke and Knake's *Cyber War* has been widely criticized in the security trade press,[100]

---

[96] *See*, *e.g.*, Jim Wolf, *Special Report: The Pentagon's New Cyber Warriors*, REUTERS (Oct. 5, 2010), http://www.reuters.com/article/2010/10/05/us-usa-cyberwar-idUSTRE69433120101005 ("Experts describe the code as a first-of-its-kind guided cyber missile."); Mortimer Zuckerman, *How To Fight And Win The Cyberwar*, WALL ST. J., Dec. 6, 2010, at A19 ("It is the world's first-known super cyberweapon designed specifically to destroy a real-world target."); Farhad Manjoo, *Don't Stick It In: The dangers of USB drives*, SLATE (Oct. 5, 2010), http://www.slate.com/articles/technology/technology/2010/10/dont_stick_it_in.html ("it's the first digital worm known to infiltrate and secretly reprogram machines that run sensitive industrial processes").

[97] ITWeb, *Focus on Cyber War Defence: Expert*, DEFENCEWEB (Oct. 14, 2010), http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=10037 (Quoting Clarke: "Stuxnet is the first example of a malicious attack involving SCADA systems.").

[98] CLARKE & KNAKE, *supra* note 58, at 123.

[99] *Id*. at 262.

[100] *See*, *e.g.*, Bruce Schneier, *Book Review: Cyber War*, SCHNEIER ON SECURITY (Dec. 21, 2009), http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html; Ryan Singel, Richard Clarke's *Cyberwar: File Under Fiction*, WIRED: THREAT LEVEL (Apr. 22, 2010), http://www.wired.com/threatlevel/2010/04/cyberwar-richard-clarke; Mike Masnick, *Dear Journalists: There Is No Cyberwar*, TECHDIRT (Apr. 9, 2010),

the popular media took the book at its word. Writing in the *Wall Street Journal*, Mort Zuckerman warned that enemy hackers could easily "spill oil, vent gas, blow up generators, derail trains, crash airplanes, cause missiles to detonate, and wipe out reams of financial and supply-chain data."[101] The sole source for his column, and for his recommendation that the federal government establish a federal cybersecurity agency to regulate private networks, was Clarke's "revealing" book.[102]

The *New York Times*'s review was also approving, sweeping aside skepticism of the book's doomsday scenarios by noting that Clarke, who had previously warned the Bush and Clinton administrations about the threat from al Qaeda before 9/11, had been right in the past.[103] The review also noted that the *Wall Street Journal* had recently reported that the power grid had been penetrated by Chinese and Russian hackers and laced with logic bombs, as Clarke and Knake had contended.[104]

That front page *Wall Street Journal* article from April 2009 is often cited as evidence for the proposition that the power grid is rigged to blow, but it could just as easily be cited as an example of "mere conduit" reporting.[105] Similar to Judith Miller's Iraq WMD articles, the only sources for the article's claim that key infrastructure has been compromised are anonymous U.S. intelligence officials.[106] With little specificity about the alleged infiltrations, readers—whether academics, journalists, or the lay

---

http://www.techdirt.com/articles/20100407/1640278917.shtml.

[101] Zuckerman, *supra* note 96. Law professor and blog pundit Glenn Reynolds had also previously reviewed the book approvingly. Glenn Harlan Reynolds, *Tinker, Tailor, Soldier, Hacker*, WALL ST. J., Apr. 21, 2010, at A19.

[102] Zuckerman, *supra* note 96.

[103] Michiko Kakutani, *The Attack Coming From Bytes, Not Bombs*, N.Y. TIMES, Apr. 27, 2010, at C1.

[104] *Id.*

[105] Siobhan Gorman, *Electricity Grid in U.S. Penetrated By Spies*, WALL ST. J., Apr. 8, 2009, at A1. At a July 2009 hearing, Representative Yvette Clarke, chair of the Emerging Threats, Cybersecurity, Science and Technology subcommittee, stated: "If you believe intelligence sources, our grid is already compromised. An April 2009 article in the *Wall Street Journal* cited intelligence forces who claim that 'the grid has already been penetrated by cyber intruders from Russia and China, who are positioned to activate malicious code that could destroy portions of the grid at their command.'" *Securing the Modern Electric Grid from Physical and Cyber Attacks: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech. of the H. Comm. on Homeland Sec.*, 111th Cong. 2 (2009) (statement of Representative Yvette D. Clark, Chairwoman, Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech. of the H. Comm. on Homeland Sec.).

[106] Gorman, *supra* note 105, at A1.

public—are left with no way to verify the claims. The article does cite a public pronouncement by senior CIA official Tom Donahue that a cyber attack had caused multiple power outages overseas.[107] But Donahue's pronouncement is what Clarke and Knake cite for their claim that cyber attacks caused a blackout in Brazil, which we now know is untrue.[108]

The author of the article, Siobhan Gorman, also contributed to another front-page *Wall Street Journal* cybersecurity scoop reporting that spies had infiltrated Pentagon computers and had stolen terabytes of data related to the F-35 Joint Strike Fighter.[109] The only sources for that report were "current and former government officials familiar with the attacks."[110] Later reporting by the Associated Press, also citing anonymous officials, found that no classified information was compromised in the breach.[111] Unfortunately, without any official statement on the matter, the result of these reports can well be to raise public alarm without offering a clear sense of the scope or magnitude of the threat.

The now-debunked Brazil blackout was also the subject of a CBS *60 Minutes* exposé on cyber war.[112] For its claim that the blackouts were the result of cyber attacks, the newsmagazine cited only anonymous "prominent intelligence sources."[113] The *60 Minutes* report, however, did feature an interview with former National Security Agency (NSA) chief, now Booz Allen Hamilton vice president, Mike McConnell, who said a blackout was within reach of foreign hackers and that the United States was not prepared for such an attack.[114]

In February of 2010, the *Washington Post* granted McConnell a rare 1,400-word essay in its Sunday opinion section in which he made the cyber war case. He told readers, "If an enemy disrupted our financial and accounting transactions, our equities and bond markets or our retail commerce—or created confusion about the legitimacy of those

---

[107] *Id.*
[108] CLARKE & KNAKE, *supra* note 58, at 99; Krebs, *supra* note 88; Soares, *supra* note 88.
[109] Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, at A1.
[110] *Id.*
[111] Lolita C. Baldor, *Cyber Hackers Breached Jet Fighter Program*, ASSOCIATED PRESS, Apr. 21, 2009, *available at* Factiva, Doc. No. APRS000020090422e54m00008.
[112] *60 Minutes: Cyber War: Sabotaging the System* (CBS television broadcast June 15, 2010).
[113] *Id.*
[114] *Id.*

transactions—chaos would result. Our power grids, air and ground transportation, telecommunications, and water-filtration systems are in jeopardy as well."[115] While he did not provide any specific evidence to corroborate this fear, McConnell did point to corporate espionage generally, and specifically the then-recent incident in which Google's Gmail service had been compromised—another instance of espionage attributed to China—as evidence of a cyber threat.[116] The result is more conflation of possible cyber threats.

In July 2010, the cover of the *Economist* magazine featured a city consumed by a pixelated mushroom cloud overlaid with the words, "Cyberwar: The Threat from the Internet."[117] The popular conception of cyber threats fostered by the media, often relying on anonymous government sources and the pronouncements of defense contractors and consultants, can be said to be more alarming than the verifiable evidence available would suggest. And as this Article will show, anonymously sourced threats and expert assertions reported in the media are later cited by officials as rationales for regulation.

4. Congress

Congress has also been quick to adopt the alarmist rhetoric of cyber doom espoused by the proponents of government intervention.[118] For example, writing in the *Wall Street Journal* in support of their co-sponsored cybersecurity bill, Sens. Jay Rockefeller and Olympia Snowe warned citizens about the potential of "catastrophic economic loss and social havoc" from cyber attack.[119] However, they provided no specifics of the threat and instead argued from authority that "[a]s members of both the Senate Commerce and Intelligence committees, we know our national security and

---

[115] Mike McConnell, *Mike McConnell on How to Win the Cyber-war We're Losing*, WASH. POST (Feb. 28, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.
[116] *Id.*
[117] *Cyberwar*, THE ECONOMIST (July 1, 2010), http://www.economist.com/node/16481504.
[118] Jaikumar Vijayan, *Senators Ramp up Cyberwar Rhetoric*, FOXBUSINESS.COM (Apr. 2, 2010), http://www.foxbusiness.com/personal-finance/2010/04/02/senators-ramp-cyberwar-rhetoric.
[119] Jay Rockefeller & Olympia Snowe, *Now Is the Time to Prepare for Cyberwar,* WALL ST. J., Apr. 2, 2010, at A15.

our economic security is at risk."[120] In the very first sentence of their piece, the Senators use another familiar authority, and quote Mike McConnell's oft-repeated warning: "If the nation went to war today in a cyberwar, we would lose."[121]

Members of Congress have used the same rhetoric at hearings on cybersecurity. In one such hearing, Senator Rockefeller stated,

> It would be very easy to make train switches so that two trains collide, affect or disrupt water and electricity, or release water from dams, where the computers are involved. How our money moves, they could stop that. Any part of the country, all of the country is vulnerable. How the Internet and telephone communication systems work, attackers could handle that rather easily.[122]

At another hearing, Senator Rockefeller noted that "a major cyber attack could shut down our Nation's most critical infrastructure: our power grid, telecommunications, financial services; *you just think of it, and they can do it*."[123] Senator Snowe agreed, adding that "if we fail to take swift action, we risk a cybercalamity of epic proportions, with devastating implications for our Nation."[124]

Other members of Congress have adopted similarly alarmist rhetoric.[125] Speaking at a hearing, Senate Armed Services Committee Chairman Carl Levin stated, "cyber weapons and cyber attacks potentially can be devastating, approaching weapons of mass destruction in their

---

[120] *Id.*
[121] *Id.*
[122] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearing Before S. Comm. on Commerce, Sci., and Transp.,* 111th Cong. 2, (2009) (statement of Senator John D. Rockefeller, Chairman, S. Comm. on Commerce, Sci., and Transp.).
[123] *Cybersecurity: Next Steps to Protect Our Critical Infrastructure: Hearing Before S. Comm. on Commerce, Sci., and Transp.,* 111th Cong. 2, (2010) (statement of Senator John D. Rockefeller, Chairman, S. Comm. on Commerce, Sci., and Transp.) (emphasis added), *available at* http://www.fas.org/irp/congress/2010_hr/cybersec.pdf.
[124] *Id.* at 4.
[125] Similarly, then CIA director Leon Panetta told Congress in February that "the potential for the next Pearl Harbor could very well be a cyber attack." Richard A. Serrano, *U.S. Intelligence Officials Concerned About Cyber Attack*, L.A. TIMES (Feb. 11, 2011), http://www.latimes.com/news/nationworld/nation/la-na-intel-hearing-20110211,0,2209934.story.

effects."[126] Rep. Yvette Clarke, chairwoman of the House committee focused on cybersecurity, has said, "There is no more significant threat to our national and economic security than that which we face in cyberspace."[127] In each of these instances, members of Congress have not offered any reviewable evidence to support their claims.

The potential for cyber threat inflation remains high. Countless legislators and executive branch officials have called for increased federal involvement in cybersecurity, citing cyber-doom scenarios as their rationale. But they have not presented verifiable evidence of the existential threats they warn about. The influential CSIS Commission Report conflates cyber threats and asserts without evidence that wide-reaching federal cybersecurity legislation is imperative. Clarke and Knake make similar assertions in *Cyber War*, but also fail to differentiate the disparate cyber threats or offer evidence to bolster their claims of cyber catastrophe. Credulous reporting by major media outlets that often cite only anonymous sources further inflates threats, even though many of these stories are hyperbolic or later debunked. Still, members of Congress have cited such accounts in proposing legislation, often warning of potential cyber catastrophes but rarely presenting verifiable evidence of catastrophic threats. Before the federal government's role in cybersecurity policy can be determined, doomsayers must present verifiable evidence of the types of threats they warn about to the public.

II. The Military-Industrial Complex, the Cold War, and Parallels to the Cyber Debate

Threat inflation helped draw the United States into war in Iraq, and a similar dynamic is taking shape in the cyber realm. If not outright war, threat inflation related to cybersecurity may lead the American people and their representatives to accept unjustified regulation of the Internet and increased federal spending on cybersecurity. Since WWII, a military-industrial complex has emerged that encourages superfluous defense spending and, at times, places special interests before the public interest. We may similarly be seeing the creation of a cyber-industrial complex.

---

[126] *Confirmation Hearings*, *supra* note 2, at 3.

[127] *Reviewing the Federal Cybersecurity Mission: Hearing Before the Subcomm. On Emerging Threats, Cybersecurity, and Sci. and Tech. of the H. Comm. On Homeland Sec.*, 111th Cong. 2 (2009) (statement of Representative Yvette D. Clark, Chairwoman, Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech. of the H. Comm. on Homeland Sec.).

In his farewell address to the nation, President Dwight Eisenhower warned against the dangers of unwarranted influence of a military-industrial complex.[128] This was a novel concern because the United States historically resisted having a large military.[129] In fact, rather than having peacetime standing armies, the Founding Fathers preferred that the country assemble troops only to fight wars and then draw down forces after conflicts.[130] Only after World War II did a giant military establishment persist.[131] It was this establishment that Eisenhower labeled the military-industrial complex, describing it as the "conjunction of an immense military establishment and a large arms industry."[132] Today, the complex seems to be evolving into a "military-cyber-intelligence mash-up" as defense contractors and the military, intelligence, and civilian security agencies turn their attention to cybersecurity.[133]

Eisenhower feared that a close relationship between government, military, and industry would lead to an unnecessary expansion of military forces, superfluous defense spending, and a breakdown of checks and balances within the public policymaking process.[134] He feared that the influence of such an establishment would allow special interests to profit under the guise of national security.[135]

A homogenous interest group—in this case, defense contractors—has a vested interest in increasing spending or favorable regulation that will transfer wealth from government to the group.[136] Increased government

---

[128] President Dwight D. Eisenhower, Farewell Address to the Nation (Jan. 17, 1961).
[129] ISMAEL, HOSSEIN-ZADEH, THE POLITICAL ECONOMY OF US MILITARISM 11 (2006); Eisenhower also noted the novelty of the military-industrial complex, calling it "new in the American experience." Eisenhower, *supra* note 128.
[130] HOSSEIN-ZADEH, *supra* note 129, at 11–12.
[131] *Id.* at 12.
[132] Eisenhower, *supra* note 128.
[133] Jim Wolf, *The Pentagon's New Cyber Warriors*, REUTERS Oct. 5, 2010, *available at* http://www.reuters.com/article/idUSTRE69433120101005.
[134] James Fallows, *The Military-Industrial Complex*, FOREIGN POLICY, Nov.–Dec., 2002, 46, 46–47.
[135] *Id.*
[136] *See* George J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. OF ECON. & MGMT. SCI. 3, 3 (1971); Sam Peltzman, *Toward a More General Theory of Regulation*, 19 J. OF L. & ECON. 211, 212 (1976). For discussion on the interest group theory of government see Robert D. Tollison, *Rent Seeking*, in PERSPECTIVES ON PUBLIC CHOICE: A HANDBOOK 506, 522–24 (Dennis C. Mueller ed., 1997).

spending on an industry directly benefits producers in that industry, and regulation that favors an interest group can have a comparable effect.[137]

Special interests therefore invest in rent-seeking capabilities that help them garner wealth transfers from government, whether through spending or legislation or regulation.[138] Rent seeking, such as lobbying that greases the rails of the political process, is socially wasteful and, perhaps more importantly, can cause government to place interest groups' desires before the public interest.[139]

When government grants a wealth transfer to a concentrated interest group—for instance, by appropriating spending to a particular industry or compelling private companies to purchase certain products or services—the cost is dispersed across millions of taxpayers. None of them individually cares enough to oppose the wealth transfer, even though it may not serve the public interest.[140] In fact, the cost to each citizen is so small that hardly any of them notice. Yet a small cost counted millions of times can be substantial.[141]

Furthermore, politicians trying to increase reelection prospects respond logically to pleas from interest groups—they often assent to them.[142] Legislators can also increase goodwill back home by channeling pork-barrel spending and jobs to their districts or states. Politicians consequently fight to bring spending to constituents and comply with interest groups' requests, and they are often afforded political cover by claiming their actions are in the interest of national security or the public good. These dynamics can combine to influence government in ways that do not serve the public interest.

When examining the military-industrial complex, it is apparent that the various participants have shared interests. Military expansion increases

---

[137] Stigler, *supra* note 136, at 5 (explaining that industry will lobby for regulation that enables it to control the entry of new rivals).
[138] The seminal article on rent seeking is Gordon Tullock, *The Welfare Costs of Tariffs, Monopolies, and Theft,* 5 W. ECON. J. 224 (1967).
[139] *Id.*
[140] Peltzman, *supra* note 136; *see generally*, MANCUR OLSON, JR, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1965) (discussing the collective action problem).
[141] *See* Peltzman, *supra* note 135, at 213.
[142] *See id.* at 231.

the Pentagon's budget and helps provide steady revenues to defense contractors.[143] It also allows congressmen to win constituents' approval by sending appropriations and jobs back home.[144]

Eisenhower believed that such an alliance between industry and the military could corrupt democratic decision-making, so he warned against unwarranted influence from a military-industrial complex. During the bomber and missile gap episodes of his presidency, he had seen firsthand the complex's propensity to trumpet and inflate foreign threats, the needless military spending that resulted, and the political clout and industry profits gained through the process.[145]

A decade after Eisenhower's address, one economist outlined the dangers of the military-industrial complex:

> [G]overnment not only permits and facilitates the entrenchment of private power but serves as its fountainhead. . . . It buys at prices for which there is little precedent and hardly any yardsticks. It deals with contractors, a large percentage of whose business is locked into supplying defense, space, or atomic energy needs. . . . [I]n an atmosphere shrouded by multilateral uncertainty and constant warnings about imminent aggression. . . . [l]acking any viable institutional competition, the government becomes—in the extreme—subservient to the private and special interests whose entrenched power bears the government seal.[146]

Eisenhower's warning was prescient. The military-industrial complex thrived throughout the Cold War,[147] and today defense spending continues to grow to historically high levels.[148]

---

[143] Fallows, *supra* note 134, at 47.
[144] *Id.*
[145] *Id.* at 46.
[146] Walter Adams, *The Military-Industrial Complex and the New Industrial State*, 58 THE AM. ECON. REV. 652, 654–55 (1968).
[147] ROBERT HIGGS, CRISIS AND LEVIATHAN: CRITICAL EPISODES IN THE GROWTH OF AMERICAN GOVERNMENT 238 (1987).
[148] HOSSEIN-ZADEH, *supra* note 129, at 14; Veronique de Rugy, *Cutting the Pentagon Budget*, REASON (July 2010), http://reason.com/archives/2010/06/11/cutting-the-pentagon-budget.

A. Cold War Military-Industrial Complex

The military-industrial complex that emerged after WWII, coupled with inflated Soviet threats, produced unnecessary defense spending and militarization. The bomber and missile gaps are classic examples.

During the 1956 elections, Democrats accused President Eisenhower of allowing a bomber gap to emerge between the United States and the Soviet Union.[149] Eisenhower had cut funding for the Air Force's B-70 bomber, which enraged many members of Congress who represented states or districts home to aviation industries.[150]

In a history of the arms race, a former Pentagon research physicist[151] notes how wide reaching the B-70 program was:

> Before the first full year under [the B-70] contract was over, there were more than forty first- and second-tier subcontractors, and approximately two thousand vendors and suppliers were by then involved in the total program. Seventy of the then ninety-six United States Senators had a major part of the program in their states, and something like a majority of the Congressional districts had at least one supplier of consequence.[152]

Soon after the funding was cut, House Armed Services Committee Chairman Carl Vinson claimed, "by cutting back the B-70 we have increased the danger to our survival."[153] Senator Barry Goldwater, also an Air Force Reserve Brigadier General, personally called on the President to reconsider the cuts.[154] Senator Clair Engle of California, also an officer in the Air Force Reserve, said that curbing spending on the B-70 was a

---

[149] William D. Hartung, *Eisenhower's Warning the Military-Industrial Complex Forty Years Later*, 18 WORLD POL'Y JOURNAL, April 1, 2001, at 39, 39.
[150] Jack Raymond, *B-70 Stirs a Wide Ranging Controversy*, N.Y. TIMES, Mar. 11, 1962, at E5.
[151] William Grimes, *Herbert York, 87, Top Nuclear Physicist Who Was Arms Control Advocate, Dies*, N.Y. TIMES, May 25, 2009, at A12.
[152] HERBERT YORK, RACE TO OBLIVION: A PARTICIPANT'S VIEW OF THE ARMS RACE 53 (1970).
[153] *Id.* at 55–56.
[154] *Id.* at 56.

"blunder which may have the gravest consequences to our national security."[155]

In the days before the 1960 presidential election, the Eisenhower Administration buckled and agreed to practically double the B-70 budget.[156] The Los Angeles-based manufacturer of the jet lauded the increased spending, as it would quell declining employment in southern California.[157]

But in 1959, the Air Force chief of staff had refuted the bomber gap theory. He had told the Senate Foreign Relations Committee, "Congress was convinced that there was going to be a gap in bombers and instead we are way ahead of them."[158] But the chief's claim was ignored. Politicians from both sides of the aisle continued to demand an increase in B-70 funding. The eventual increase channeled money and jobs to constituents—contractors and vendors across the country and the aviation manufacturer in southern California. Because of the exaggerated bomber gap, Congress wasted billions of dollars commissioning superfluous bombers.[159]

Later, as a candidate in the 1960 presidential election, John F. Kennedy accused Republicans of putting the United States at risk by allowing another gap to emerge—the missile gap.[160] Kennedy claimed, "We are facing a gap on which we are gambling with our survival."[161] Senator Stuart Symington, the first Secretary of the Air Force and a long-time advocate for military spending, said, "A very substantial missile gap does exist and the Eisenhower Administration apparently is going to permit this gap to increase."[162]

Both the Air Force and the Strategic Air Command—the military units in charge of building and controlling long-range missiles—supported

---

[155] *Id.*
[156] *Id.*
[157] *Id.*
[158] Lars-Erik Nelson, *Military-Industrial Man*, N.Y. REV. OF BOOKS, Dec. 21, 2000, at 6.
[159] John Prados, *Whose Soviet Threat?*, N.Y. TIMES, June 7, 1982, at A19.
[160] Hartung, *supra* note 149, at 39.
[161] *Defense: The Missile Gap Flap*, TIME (Feb. 17, 1961), http://www.time.com/time/magazine/article/0,9171,826840,00.html.
[162] *Id.*; For background on Symington's reputation re military spending, see Eric Pace, *Stuart Symington, 4-Term Senator Who Ran for President, Dies at 87*, N.Y. TIMES, Dec. 15, 1988, at D26.

the Senators' assertions.[163] The units estimated that the Soviets had between 500 and 1,000 long-range missiles.[164] If the Soviets really had significantly more missiles than the United States, the Air Force had a strong argument for diverting funds from the Army and Navy to itself to build more missiles.[165] The CIA, however, simultaneously estimated the number of Soviet missiles to be 50.[166]

In his last speech before Congress, Eisenhower said, "The bomber gap of several years ago was always a fiction, and the missile gap shows every sign of being the same."[167] At the peak of the Cuban missile crisis, the United States had 2,000 long-range missiles; the Soviets had fewer than 100.[168] Shortly after Kennedy took office, Secretary of Defense Robert McNamara said that "[i]t took us about three weeks to determine, yes, there was a gap. But the gap was in our favor. It was a totally erroneous charge that Eisenhower had allowed the Soviets to develop a superior missile force."[169]

B. Cyber-Industrial Complex

An industrial complex reminiscent of the Cold War's may be emerging in cybersecurity today. Some serious threats may exist, but we have also seen evidence of threat inflation. Alarm raised over potential cyber threats has led to a cyber industry build-up and political competition over cyber pork.

---

[163] Fred Kaplan, *The Rumsfeld Intelligence Agency*, SLATE (Oct. 28, 2002, 5:42 PM), http://www.slate.com/id/2073238/.
[164] *Id.*
[165] *Id.*
[166] *Id.*
[167] *Defense: The Missile Gap Flap*, *supra* note 161.
[168] *Missiles of October, Then and Now*, N.Y. TIMES, Aug. 30, 1987, at E26.
[169] Tim Weiner, *Robert McNamara, Architect of a Futile War, Dies at 93*, N.Y. TIMES, July 7, 2009, at A1, *available at* http://www.nytimes.com/2009/07/07/us/07mcnamara.html?pagewanted=all. In *Cyber War*, Clarke and Knake warn of a "cyber war gap" that exists between the United States and countries like Russia, China, Iran, and North Korea. CLARKE & KNAKE, *supra* note 58 at 149. The authors claim that the United States' weak cyber defense capabilities and heavy dependence on online systems foster the gap. We should, however, keep our "gaps" history in mind when evaluating the authors' assertion.

1. Build-up

In many cases, those now inflating the scope and probability of cyber threats might well benefit from increased regulation and more government spending on information security. Cybersecurity is a big and booming industry.[170] The U.S. government is expected to spend $10.5 billion per year on information security by 2015, and analysts have estimated the worldwide market to be as much as $140 billion per year.[171] The Department of Defense has also said it is seeking more than $3.2 billion in cybersecurity funding for 2012.[172]

In recent years, in addition to traditional information security providers like MacAfee, Symantec, and Checkpoint, defense contractors and consulting firms have recognized lucrative opportunities in cybersecurity.[173] To weather probable cuts on traditional defense spending, and to take advantage of the growing market, these firms have positioned themselves to compete with information security firms for government contracts.[174] Lockheed Martin, Boeing, L-3 Communications, SAIC, and BAE Systems have all launched cybersecurity business divisions in recent years.[175]

Other traditional defense contractors, like Northrop Grumman, Raytheon, and ManTech International, have also invested in information

---

[170] Marjorie Censer & Tom Temin, *The Cybersecurity Boom*, WASH. POST (May 10, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/05/07/AR2010050704503.html.
[171] Jim Wolf, *Pentagon Seeks Tight Ties with Cyber Contractors*, REUTERS (Oct. 21, 2010), http://www.reuters.com/article/idUSTRE69J4OW20101021; *U.S. cybersecurity spending to rise*, HOMELAND SECURITY NEWSWIRE (Mar. 31, 2010), http://homelandsecuritynewswire.com/us-cybersecurity-spending-rise.
[172] *Cyber Spending at Defense*, NEXTGOV.COM (Mar. 29, 2011), http://www.nextgov.com/nextgov/ng_20110329_1325.php.
[173] Censer & Temin, *supra* note 170; Aaron Ricdela, *Symantec, McAfee, Checkpoint Await Spending Surge*, BLOOMBERG BUSINESSWEEK, (Jan. 18, 2010, 10:19 PM), http://www.businessweek.com/print/technology/content/jan2010/tc20100115_453540.htm; Gopal Ratnam, *Lockheed, Boeing Tap $11 Billion Cybersecurity Market (Update2)*, BLOOMBERG, (Dec. 30, 2008, 4:18 PM), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=an2_Z6u1JPGw.
[174] August Cole & Siobhan Gorman, *Defense Firms Pursue Cyber-Security Work*, WALL ST. J., Mar. 18, 2009, at A4, *available at* http://online.wsj.com/article/SB123733224282463205.html; Ratnam, *supra* note 173.
[175] Censer & Temin, *supra* note 170; Wolf, *supra* note 171; Ratnam, *supra* note 173.

security products and services.[176] Such investments appear to have positioned defense firms well. In 2009, the top 10 information technology federal contractors included Lockheed Martin, Boeing, Northrop Grumman, General Dynamics, Raytheon, SAIC, L-3 Communications, and Booz Allen Hamilton.[177]

Traditional IT firms also see more opportunities to profit from cybersecurity business in both the public and private sectors.[178] Earlier this year, a software security company executive noted "a very large rise in interest in spending on computer security by the government."[179] And as one IT market analyst put it: "It's a cyber war and we're fighting it. In order to fight it, you need to spend more money, and some of the core beneficiaries of that trend will be the security software companies."[180]

Some companies from diverse industries have also combined forces in the cybersecurity buildup. In 2009, a combination of defense, security, and tech companies, including Lockheed, McAfee, Symantec, Cisco, Dell, Hewlett-Packard, Intel, Juniper Networks, and Microsoft, formed a cybersecurity technology alliance to study threats and create solutions.[181]

IT lobbyists too have looked forward to cybersecurity budget increases, to the dismay of at least one executive at a small tech firm, who claimed, "Money gets spent on the vendors who spend millions lobbying Congress."[182]

---

[176] Wolf, *supra* note 171.
[177] Tom Barry, *Synergy in Security: The Rise of the National Security Complex*, DOLLARS & SENSE (Mar./Apr. 2010), http://www.dollarsandsense.org/archives/2010/0310barry.html.
[178] Ricdela, *supra* note 173.
[179] *Id.*
[180] *Id.*
[181] Dan Lohrmann, *New Cybersecurity Technology Alliance Points the Way*, GOVERNMENT TECHNOLOGY BLOGS (Nov. 13, 2009, 3:46 AM) http://www.govtech.com/blogs/lohrmann-on-infrastructure/New-Cyber-Security-Technology.html.
[182] John Leyden, *US and UK Gov Cyber Defences = Big Boys' Trough-Slurp*, THE REGISTER (Oct. 22, 2010, 2:15 PM), http://www.theregister.co.uk/2010/10/22/firewall_guru_interview/; Kate Gerwig, *Cyber-Security Policy Locks Down Lobbyist Job Security*, IT KNOWLEDGE EXCHANGE (Jan. 26, 2009, 2:15 AM), http://itknowledgeexchange.techtarget.com/telecom-timeout-blog/cyber-security-policy-boon-to-lobbyist-job-security/.

There are serious real online threats, and security firms, government agencies, the military, and private companies clearly must invest to protect against such threats. But as with the Cold War bomber and missile gap frenzies, we must be wary of parties with vested interests exaggerating threats, leading to unjustified and superfluous defense spending in the name of national security.

2. Cyber Pork

Private firms are not the only ones to have noticed increased cybersecurity spending. Politicians and government officials have also taken notice and likely see it as an opportunity to bring federal dollars to their states and districts.

In spring of 2010, the Air Force officially established Cyber Command, a new unit in charge of the military's offensive and defensive cyber capabilities.[183] Cyber Command allows the military to protect its critical networks and coordinate its cyber capabilities, an important function.[184] But the pork feeding frenzy that Cyber Command precipitated offers a useful example of what could happen if legislators or regulators call for similar buildup related to private networks.

Beginning in early 2008, towns across the country sought to lure the permanent headquarters of Cyber Command.[185] In recent years, the Air Force had significantly trimmed its active duty force, and the branch is still trying to reduce its numbers to reflect a Congressional mandate.[186] Amid such cuts, and with calls to cut traditional defense spending, the military has looked to cyberspace as a new spending front.[187] It was estimated that

---

[183] Ellen Nakashima, *Gen. Keith Alexander Confirmed to Head Cyber-Command*, WASH. POST, May 11, 2010, at A13, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/05/10/AR2010051005251.html.
[184] Gautham Nagesh, *Gates Officially Establishes U.S. Cyber Command*, THE HILL (May 24, 2010, 11:43 AM), http://thehill.com/blogs/hillicon-valley/technology/99481-gates-officially-establishes-us-cyber-command.
[185] Marty Graham, *Welcome to Cyberwar Country, USA*, WIRED (Feb. 11, 2008), http://www.wired.com/politics/security/news/2008/02/cyber_command.
[186] Bruce Rolfsen, *Drawdown: Force to be Cut by 6,000 airmen*, AIR FORCE TIMES (Apr. 12, 2010, 8:58 AM), http://www.airforcetimes.com/news/2010/04/airforce_drawdown_041210w/.
[187] Graham, *supra* note 185; *War on New Fronts: Different Tactics are Needed to Profit from a Slowdown in Defence Spending*, THE ECONOMIST (Nov. 4, 2010), http://www.economist.com/node/17420367; Ratnam, *supra* note 173.

Cyber Command headquarters would bring at least 10,000 direct and ancillary jobs, billions of dollars in contracts, and millions in local spending.[188]

Politicians naturally saw the Command as an opportunity to boost local economies. Governors pitched their respective states to the secretary of the Air Force, a dozen congressional delegations lobbied for the Command, and Louisiana Governor Bobby Jindal even lobbied President Bush during a meeting on Hurricane Katrina recovery.[189] Eventually communities in 18 states were vying for the Command,[190] many offering gifts of land, infrastructure, and tax breaks.[191]

The city of Bossier, Louisiana, proposed a $100 million "Cyber Innovation Center" office complex next to Barksdale AFB in hopes of luring Cyber Command there.[192] It began by building an $11 million bomb-resistant "cyber fortress" complete with a moat.[193] In Yuba City, California, community leaders gathered 53 signatures from the state's congressional delegation and preached the merits of nearby Silicon Valley in their effort to lure the Command.[194] Colorado Springs touted the hardened location of Cheyenne Mountain, NORAD headquarters.[195]

In Nebraska, the Omaha Development Foundation purchased 136 acres of land just south of Offutt Air Force Base and offered it as a site for the Command.[196] The president of a local chamber of commerce said, "It's all political, where they decide to put it. We're clearly the best situated and equipped. But that doesn't mean we'll get it."[197]

The Air Force ultimately established Cyber Command headquarters at Fort Meade, Maryland, integrated with the NSA headquarters.[198]

---

[188] Graham, *supra* note 185.
[189] *Id.*
[190] Erik Holmes, *18 States Vie for Cyber Command Headquarters*, AIR FORCE TIMES (Mar. 9, 2008, 2:36 PM), http://www.airforcetimes.com/news/2008/03/airforce_cyber_command_030908/.
[191] Graham, *supra* note 185.
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] *Id.*
[197] *Id.*
[198] Nagesh, *supra* note 184; Nakashima, *supra* note 183.

Maryland politicians who had touted the cyber threat and sought the Command welcomed this. Senator Barbara Mikulski had previously proclaimed, "We are at war, we are being attacked, and we are being hacked."[199] Governor Martin O'Malley has noted, "We not only think that Maryland can be the national epicenter for cybersecurity; the fact of the matter is, our state already is the epicenter for our country."[200]

After the announcement that Cyber Command would be established at Fort Meade, O'Malley praised the decision as one that would bolster national security and provide "endless economic opportunity and job creation."[201] His press statement estimated the Command would bring more than 21,000 military and civilian jobs to the area.[202] Local defense contractors and tech firms also relished the announcement and the $15 to $30 billion in expected spending it would bring over the next five years.[203]

Other recent examples highlight what could be a trend toward more cyber pork. In January 2011, the NSA and Army Corps of Engineers broke ground on a $1.2 billion dollar data center outside of Salt Lake City for which Senator Orrin Hatch lobbied.[204] The same month, DHS announced that it would invest $16 million to test security solutions at the University of Southern California.[205]

Proposed cybersecurity legislation also presents opportunities for congressional pork barrel spending. For example, the Cybersecurity Act of

---

[199] Gus Sentementes, *O'Malley to Promote Md. as U.S. Cybersecurity Hub*, BALT. SUN, Jan. 12, 2010, at 10A, *available at* http://articles.baltimoresun.com/2010-01-12/business/bal-bz.cybersecurity12jan12_1_cyber-security-homeland-security-work-force.
[200] *Id.*
[201] Statement from Governor Martin O'Malley on Establishment of Cyber Command in Maryland, OFFICE OF GOVERNOR MARTIN O'MALLEY, May 21, 2010, *available at* http://www.governor.maryland.gov/pressreleases/100521e.asp.
[202] *Id.*
[203] Daniel Sernovitz, *Tech Firms Flock to Fort Meade for Cyber Warfare Work*, BALT. BUSINESS J. (July 12, 2010), http://www.bizjournals.com/baltimore/stories/2010/07/12/story12.html; Sonny Goldreich, *Commercial Real Estate: Cyber Command to bring jobs to Fort Meade*, GAZETTE.NET (May 28, 2010), http://www.gazette.net/stories/05282010/businew174314_32560.php.
[204] Pam Benson, *Utah Will be Site of Huge Cyber Protection Facility*, CNN (Jan. 12, 2011), http://articles.cnn.com/2011-01-12/politics/cyber.defense.center_1_cyber-security-homeland-security-utah.
[205] *DHS invests $16M in Cybersecurity Testbed*, SECURITYINFOWATCH (Jan. 17, 2011), http://www.securityinfowatch.com/node/1319202.

2010 proposed by Senators Jay Rockefeller and Olympia Snowe called for the creation of regional cybersecurity centers across the country, a cyber scholarship-for-service program, and myriad cybersecurity research and development grants.[206]

The military-industrial complex was born out of exaggerated Soviet threats, a defense industry closely allied with the military and Department of Defense, and politicians striving to bring pork and jobs home to constituents. A similar cyber-industrial complex may be emerging today, and its players call for government involvement that may be superfluous and definitely allows for rent seeking and pork barreling.

III. Policy Implications

So far we have seen the potential of threat inflation in the cybersecurity arena and how it may result in a new cyber-industrial complex. In this final Part we will examine the proposals made by advocates of federal intervention and the rationales presented for those proposals. We will also suggest a simple framework for determining whether government intervention is indeed necessary.

A. Proposals and Rationales

Calls for federal involvement in Internet security run the gamut from simple requests for more research funding to serious interventions in the business practices of infrastructure providers. However, they often do not consider the costs or consequences associated with such interventions.

At one end of the spectrum are calls to scrap the Internet as we know it. For example, Mike McConnell has suggested that "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment—who did it, from where, why and what was the result—more manageable."[207] Richard Clarke has recommended the same: "Instead of spending money on security solutions, maybe we need to seriously think of redesigning network architecture, giving money for research into the next protocols, maybe even think about another, more secure Internet."[208]

---

[206] Cybersecurity Act of 2009, S. 773, § 5(a), § 12(a), § 11(e) (2009).
[207] McConnell, *supra* note 115.
[208] ITWEB, *Focus on Cyber War Defence: Expert*, DEFENCEWEB (Oct. 14, 2010),

A "reengineered," more secure Internet is likely a very different Internet than the open and innovative network we know today. It might be an Internet on which information flows are much more easily controlled by government, and in which anonymity is impossible, posing a threat to free speech.[209] This is so because the ability to attribute malicious behavior to individuals would require that individuals identify themselves when logging on.[210] A capability to track and attribute malicious activities could just as easily be employed to track and control any other type of activity.

We have also seen proposals to require tier 1 Internet service providers to engage in deep packet inspection of Internet traffic in order to filter out malicious data.[211] The federal government already engages in deep packet inspection on its own networks through the Department of Homeland Security's "EINSTEIN" program.[212] The idea would be to require the same type of monitoring from the Internet's private backbone operators.[213] Such approaches likely threaten user privacy. Deep packet inspection is essentially eavesdropping and, just as it can be used to identify

---

http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=10037.

[209] *See* Marjory S. Blumenthal & David D. Clark, *Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World*, 1 ACM TRANSACTIONS ON INTERNET TECH. 70, 76 (2001). *See also* Testimony of Marc Rotenberg, *Planning for the Future of Cyber Attack Attribution: Hearing Before Subcomm. On Technology and Innovation of the Comm. On Science and Technology*, 111th Cong., July 15, 2010, *available at* http://epic.org/privacy/cybersecurity/EPIC_HouseSci_Testimony_2010-07-15.pdf.

[210] THE WHITE HOUSE, CYBERSPACE POLICY REVIEW 33 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (noting that "[w]e cannot improve cybersecurity without improving authentication, and identity management is not just about authenticating people. Authentication mechanisms also can help ensure that online transactions only involve trustworthy data, hardware, and software for networks and devices"). Another concern is that authentication will fail to prevent malicious activities because criminals will simply hijack legitimate identities before committing crimes and attacks.

[211] CLARKE & KNAKE, *supra* note 58, at 162–64. Deep packet inspection means examining the content of data packets—in this case looking for security threats—as they pass an inspection point. Doing so at the "tier 1" level means that it would happen at the Internet's backbone, where almost all traffic will pass.

[212] THE WHITE HOUSE, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE 3 (2010), *available at* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[213] CLARKE & KNAKE, *supra* note 58, at 120, 273–75. Columbia computer science professor and security expert Steven Bellovin has critiqued Clarke and Knake's deep packet inspection suggestion, explaining that it may not even be technically possible. Steven Bellowin, *Clarke and Knake's "Cyberwar,"* CIRCLEID (Jul. 14, 2010), http://www.circleid.com/posts/print/clarke_and_knakes_cyberwar.

malicious data, it can be used to identify other classes of communication.

There have also been proposals at the FCC and in Congress for the certification or licensing of network security professionals, as well as calls for mandated security standards. For example, the Rockefeller-Snowe bill would require the Department of Commerce to develop "a national licensing, certification, and periodic recertification program for cybersecurity professionals," and would make certification mandatory for anyone engaged in cybersecurity.[214] While certification may seem harmless, occupational licensing mandates should never be taken lightly. They have the potential to restrict entry, reduce competition, and hamper innovation.[215]

Finally, there have been calls for subsidies—including the creation of regional cybersecurity centers across the country to help medium-sized businesses protect their networks—as well as calls for more federal dollars for education and research and development.[216]

Given the sweeping nature of these proposals, one would imagine that their proponents carefully justify them. Unfortunately, the rationales offered are generally mere assertions employing the rhetoric of threat inflation. At a general level, there is a tendency by cybersecurity experts to report that markets are incapable of providing adequate security without providing any evidence for the claim. More specifically, Congressional sponsors of legislation simply cite the testimony of consultants and anonymously sourced press reports to justify their bills.

For example, the CSIS Commission Report is very clear that what it seeks is the regulation of cyberspace. It argues that market forces "will never provide the level of security necessary to achieve national security objectives,"[217] yet it does not provide any empirical evidence for this assertion. Instead the Commission simply makes the argument that national defense is a public good, and points out that private firms "have little

---

[214] Cybersecurity Act of 2009, § 7(a)–(b) (2009).
[215] *See generally* MORRIS M. KLEINER, LICENSING OCCUPATIONS: ENSURING QUALITY OR RESTRICTING COMPETITION? (2006).
[216] Cybersecurity Act of 2009, § 11(e); Commission Report, *supra* note 41, at 74.
[217] Commission Report, *supra* note 41, at 50. *See also id.* at 2, 10, & 49.

incentive to spend on national defense as they bear all of the cost but do not reap all of the return."[218]

Of course, a firm need not "reap all of the return" in order to have an incentive to spend on security. As long as they are able to internalize enough of the return to justify their expenditure, they may do so even if in the process they produce a positive externality that they cannot capture.[219] Therefore, whether there is market failure or not is an empirical question and, as we will see below, one that is part of a proper regulatory analysis. Unfortunately the CSIS Commission report does not engage in such an analysis.

Mike McConnell has argued that regulation is justified simply because cybersecurity is a significant issue. Testifying before Congress, he stated that "cyber has become so important to the lives of our citizens and the functioning of our economy that gone are the days when Silicon Valley could say 'hands off' to a Government role."[220] He provided no further analysis for this claim.

Clarke and Knake, for their part, seem to suggest that regulations need not be justified at all. They criticize the cybersecurity initiatives of the Clinton, Bush, and Obama Administrations for "eschewing regulation."[221] For example, Clarke bemoans that a Presidential Decision Document outlining the Clinton Administration's cybersecurity policy, which he helped draft, ultimately included a statement indicating that the first choice to address cybersecurity concerns should be "incentives that the market provides" and that "regulation will be used only in the face of a material failure of the market."[222]

It is interesting to note, however, that the experts understand the limitations of their positions. Clarke and Knake admit that the types of regulations that they propose make it easier for government to violate the privacy of citizens, and they point out recent episodes of just such abuse,

---

[218] *Id.* at 50.
[219] OLSON, *supra* note 140, at 49–51.
[220] *Cybersecurity: Next Steps to Protect Our Critical Infrastructure*, *supra* note 123.
[221] CLARKE & KNAKE, *supra* note 58, at 108–09 (critiquing Clinton), 113 (critiquing Bush), & 116–18 (critiquing Obama).
[222] *Id.* at 108. *See also*, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 1998, *available at* http://clinton4.nara.gov/WH/EOP/NSC/html/documents/NSCDoc3.html.

including the alleged illegal NSA wiretapping during the Bush Administration.[223] They nevertheless conclude, "There may be times, however, as in the case of cyber war, when we should examine whether effective safeguards can be put in place so that we can start new programs that entail some risk."[224]

Similarly, both Clarke and Knake and the CSIS Commission Report admit that regulatory solutions tend to be inflexible, slow to change, and have the potential to stifle innovation.[225] However, both also make the case that the type of regulation they have in mind would be immune to the political realities that have traditionally made regulation of such a fast-moving sphere ineffective.[226]

To justify their particular bills, members of Congress do not generally engage in much analysis, and simply tend to cite press reports and the assertions of experts. For example, the Rockefeller-Snowe bill includes a findings section outlining the reasons why government intervention in cybersecurity is ostensibly necessary.[227] It cites Mike McConnell's warning that had the 9/11 terrorists chosen laptops rather than airplanes, the economic fallout of the attacks would have been orders of magnitude greater, as well as the CSIS Commission Report, and Paul Kurtz, Richard Clarke's security consulting partner.[228]

Introducing on the Senate floor the comprehensive cybersecurity bill that she co-authored with Senator Joe Lieberman, Senator Susan Collins sought to make the case for federal intervention by providing a list of "disturbing" recent cyber attacks.[229] She began with two familiar examples:

> Press reports a year ago stated that China and Russia had penetrated the computer systems of America's electrical grid. The hackers allegedly left behind malicious hidden software

---

[223] CLARKE & KNAKE, *supra* note 58, at 134.
[224] *Id*. at 134–35.
[225] Commission Report, *supra* note 41, at 51; CLARKE & KNAKE, *supra* note 58, at 133–34.
[226] Commission Report, *supra* note 41, at 51-53; CLARKE& KNAKE, *supra* note 58, at 134.
[227] Cybersecurity Act of 2009, § 2.
[228] *Id.* § 2(10). *But see* Lawson, *supra* note 3, at 6–7, 20–22 (arguing that comparisons of cyber threats to 9/11 are not apt and that the U.S. proved resilient to those attacks and would likely be resilient to a large cyber attack).
[229] 156 Cong. Rec. S4852–S4855 (daily ed. June 10, 2010) (statement of Sens. Lieberman & Collins).

> that could be activated later to disrupt the grid during a war or other national crisis.
>
> At about the same time, we learned that, beginning in 2007 and continuing well into 2008, hackers repeatedly broke into the computer systems of the Pentagon's $300-billion Joint Strike Fighter project. They stole crucial information about the Defense Department's costliest weapons program ever.[230]

Senator Collins was not providing any verifiable evidence of a threat, but was instead simply quoting the front-page *Wall Street Journal* stories that, as we have seen, relied exclusively on information from anonymous government officials.[231] Representative Yvette Clarke has also cited the *Wall Street Journal*'s reporting about the electrical grid during a hearing in support of legislation.[232] The fact that members of Congress are citing anonymously sourced press accounts of a government leak, rather than hard evidence, as a rationale for legislation is disheartening. It is also reminiscent of Vice President Cheney citing Judith Miller and Michael Gordon's *New York Times* reporting as evidence of an Iraqi nuclear threat.

B. Conducting a Proper Analysis

Perhaps the most frustrating aspect of the calls for cybersecurity regulations is that they have not been accompanied by economic analysis to determine their need or effectiveness. This final section, therefore, seeks to offer a simple framework for assessing whether in fact federal intervention in cybersecurity is warranted. Let us be very clear: although we are skeptical of the scope of the threat as presented by the proponents of regulation, we do not doubt that cyber threats do exist, nor would we suggest that regulation can never be appropriate. What we do propose is that before we rush to regulate cyberspace we should first demand verifiable evidence of the threat and its scope and, second, we should use any such evidence to conduct a proper analysis to determine whether regulation is necessary and whether it will do more good than harm.

---

[230] *Id.* at S4853.
[231] *See supra* notes 105–107 and accompanying text.
[232] *Reviewing the Federal Cybersecurity Mission*, *supra* note 126.

Regulatory analysis is the generally accepted toolkit used to evaluate proposed government interventions in the market.[233] The Office of Management and Budget has set forth the key elements of regulatory analysis in its Circular A-4, which guides all executive agency rulemaking.[234] The steps to a proper analysis include:

- Determining the need for regulation in terms of market failure or other systemic problems[235]
- Considering alternatives to federal regulation and alternative forms of regulation[236]
- Determining the costs and benefits of proposed regulations[237]

We do not attempt to conduct an analysis of any proposed regulations here. Instead we simply use the framework to evaluate the evidence as it stands now and suggest that a similar analysis be conducted before cybersecurity regulation or legislation is adopted.

The first step of any analysis is to clearly state the problem one is trying to solve.[238] It seems obvious, but without a clear sense of the problem, and one's desired outcome, one cannot properly assess the problem or possible solutions.

One view of the cybersecurity problem is cyber war. That is, the threat that foreign states or organizations could employ cyber attacks to strike at our critical infrastructure. What evidence do we have to corroborate these massive threats? Mike McConnell has cited the hacking of Google's Gmail service—a case of espionage that has been attributed to China—as well as other instances of espionage and IP theft.[239] Similarly, the

---

[233] *See* Jerry Ellig & Jerry Brito, *Toward a More Perfect Union: Regulatory Analysis and Performance Management*, 8 FLA. ST. BUS. L. REV. 1, 1 (2009).
[234] OFFICE OF MANAGEMENT AND BUDGET, CIRCULAR A-4: REGULATORY ANALYSIS (Sept. 17, 2003), *available at* http://www.whitehouse.gov/omb/circulars_a004_a-4 [hereinafter CIRCULAR A-4]. President Obama recently endorsed Circular A-4 and its decision making process in his executive order on regulatory review. Exec. Order No. 13563 of Jan. 18, 2011, *available at* http://www.whitehouse.gov/the-press-office/2011/01/18/improving-regulation-and-regulatory-review-executive-order.
[235] CIRCULAR A-4, *supra* note 234, at 3–4.
[236] *Id.* at 6–7.
[237] *Id.* at 9–11.
[238] Ellig & Brito, *supra* note 233, at 29.
[239] McConnell, *supra* note 115.

only verifiable evidence that Clarke and Knake present is of denial of service attacks or cyber espionage. They also cite anonymous sources suggesting that the power grid has been compromised and is riddled with "logic bombs."[240]

Two things stand out here. First, as we have seen, there is lack of verifiable evidence of a cyber war threat. The implication is that the hard evidence is classified and the public is not privy to it. However, before the American people can be expected to support far-reaching regulation, we must have some evidence of the threat and its probability. Fear is not a basis for policy making. If this means declassifying embarrassing information to some extent, it might be necessary.[241] It is the only way we can be sure that we are not simply seeing threat inflation at work.

The CSIS Report and Clarke and Knake all bemoan the overclassification of information related to cyber threats.[242] Former NSA and CIA chief General Michael Hayden gets to the core of the issue writing in Strategic Studies Quarterly:

> Let me be clear: This stuff is overprotected. It is far easier to learn about physical threats from US government agencies than to learn about cyber threats. . . . [I]f we want to shift the popular culture, we need a broader flow of information to corporations and individuals to educate them on the threat. To do that we need to recalibrate what is truly secret. Our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a common body of knowledge. With no common knowledge, no meaningful discussion, and no consensus . . . the policy vacuum continues. This will not be easy, and in the wake of

---

[240] CLARKE & KNAKE, *supra* note 58, at 54, 59, & 62.

[241] As President Obama has stated, "The Government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears. Nondisclosure should never be based on an effort to protect the personal interests of Government officials at the expense of those they are supposed to serve." Memorandum from President Obama to the Heads of Executive Departments and Agencies regarding the Freedom of Information Act (Jan. 21, 2009), *available at* http://www.fas.org/sgp/obama/foia012109.html.

[242] CLARKE & KNAKE, *supra* note 58, at 262; Commission Report, *supra* note 41, at 27–28.

> WikiLeaks it will require courage; but, it is essential and should itself be the subject of intense discussion.[243]

Second, there is the danger of conflating threats. Physical threats to critical infrastructure, cyber espionage, and denial of service attacks are all different beasts.[244] Evidence for each of them is no more interchangeable than evidence of a chemical or biological weapons capability is evidence of a nuclear capability.

As the CSIS Commission report has pointed out, the real threat of cyber attack is not a physical threat, but an informational one.[245] So let us set aside the more alarmist visions of cyber war and focus on the cybersecurity problems for which there is evidence: cyber espionage and denial of service attacks. The policy question being asked is whether private businesses, when left to their own devices, provide enough cybersecurity to address these problems, or if some government involvement is justified.[246]

The next step in regulatory analysis is to determine whether there is a market failure or some other systemic problem.[247]

Let us first look at cyber espionage. The CSIS Commission, Clarke, McConnell, and others identify a massive loss of intellectual property from American companies as a major component of the national security threat that they see.[248] To the extent that this is the case, it would seem that private industry should have the best incentive to protect itself from that threat.[249]

---

[243] Michael V. Hayden, *The Future of Things "Cyber",* 5 STRATEGIC STUD. Q. 3, 5 (2011), *available at* http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.
[244] James Lewis, *Thresholds for Cyberwarfare,* IEEE SECURITY AND PRIVACY (Feb. 17, 2011), http://doi.ieeecomputersociety.org/10.1109/MSP.2011.25.
[245] Commission Report, *supra* note 41, at 12.
[246] Benjamin Powell, *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry*, Independent Institute Working Paper No. 57, March 14, 2005, at 1, *available at* http://www.independent.org/pdf/working_papers/57_cyber.pdf.
[247] For an analysis of the various market failure rationales for regulation in cybersecurity, see Eli Dourado, *Is there a Cybersecurity Market Failure*?, Mercatus Center Working Paper No. 11-XX, October 2011.
[248] S.773 at § 2; CLARKE & KNAKE, *supra* note 58, at 126; Commission Report, *supra* note 41, at 11.
[249] Wolf, *supra* note 170 ("Greg Neichin of San Francisco-based Cleantech Group LLC, a research firm, says utility companies already are well aware of the need to guard their infrastructure, which can represent billions of dollars of investment. 'Private industry is throwing huge sums at this already,' he says. 'What is the gain from government involvement?'"); Doug Raymond, head of monetization at Google Asia-Pacific, notes,

After all, it internalizes the cost of IP theft and loss of reputation. It is therefore difficult to see the market failure here, but it is an empirical question and the burden of proof is on those who favor regulation to provide evidence to the contrary.

Next, let us turn to denial of service attacks and other threats that stem from compromised computers. Here we can put forth an arguable case that there can be a market failure. Because computers can be part of a botnet without the user's knowledge, the user does not always internalize the harm from poor security, but imposes a negative externality on others.[250] But before we conclude that there is a market failure, and that regulation is the only answer, we should look at the issue more closely.

First, it is not true that a user will not internalize any of the cost of an infected computer.[251] In reality, good security practices create both public and private benefits.[252] While a user may not have an incentive to protect others, he should be concerned about viruses, spyware, and other threats to the integrity of his own data. As a result, the relevant policy question is, are the private benefits sufficient to cause firms and consumers to provide enough security?[253]

"Companies like Google are the ones who are hurt the most when our users' trust is put in question or material of economic value is stolen. . . . [technology] has been so rapidly changing that, in my observation, the best people to stay ahead of the curve and come up with solutions are those who are on the ground managing those products day to day." The Center for National Policy, transcript of "The Private Sector's Role in Cyber Security," Apr. 14, 2010, *available at* http://www.centerfornationalpolicy.org/ht/a/GetDocumentAction/i/18044.

[250] Van Eeten & Bauer, *supra* note 66.

[251] Powell, *supra* note 246, at 4.

[252] *Id*.

[253] *Id*. Some initial evidence may suggest that ISPs are indeed taking steps to grapple with the malware and botnet problems. For example, Comcast has begun warning customers that their computers are likely compromised. Brian Krebs, *Comcast Pushes Bot Alert Program Nationwide*, KREBS ON SECURITY (Oct. 4, 2010), http://krebsonsecurity.com/2010/10/comcast-pushes-bot-alert-program-nationwide. Also, a private cyber insurance market seems to be forming. *See* Jay P. Kesan et al., The Economic Case for Cyberinsurance, University of Illinois College of Law, Law and Economics Working Paper No. 2004-2, *available at* http://www.heartland.org/custom/semod_policybot/pdf/28828.pdf; Internet Security Alliance, White Paper: Cyber-Insurance Metrics and Impact on Cyber-Security, *available at* http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf.

As mentioned above, the CSIS Commission feels it knows the answer to this question: "An *appropriate level* of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives."[254] Again, the burden is on proponents of regulation to explain how they determine what is the appropriate level of cybersecurity and how they determine that the private sector is under-providing it. Those are empirical questions that, as we have seen, have so far only been answered with assertions.

Finally, it should be pointed out that even if one were to determine that cybersecurity is under-provided by the private sector, one would then have to proceed to the next questions in an economic analysis: consider different alternatives to regulation, as well as alternative forms of regulation, and determine whether the benefits of the chosen alternative outweigh its costs. Indeed, although cyber-doom scenarios are often presented as existential threats to our fragile interconnected society, the evidence from history—from WWII to 9/11 to Katrina—is that people and institutions are incredibly resilient and would likely bounce back from any probable cyber attack.[255] As Aaron Wildavsky puts it when addressing how best to respond to dangers that cannot be understood in advance: "[m]y vote goes to the resilience that comes from passing many trials and learning from errors so that the defects of society's limited imagination are made up by larger amounts of global resources that can be converted into meeting the dangers that its members never thought would arise."[256]

Both Mr. Clarke and the CSIS Commission explain that command and control regulation has failed in the past, and that government has abused the surveillance powers that it has been granted. But this time, they say, things will be different. New technologies will allow us to employ "smart regulation" that will be immune to human incentives. There is little reason not to be skeptical of these suggestions.

Conclusion

Cybersecurity is an important policy issue, but the alarmist rhetoric coming out of Washington that focuses on worst-case scenarios is unhelpful

---

[254] Commission Report, *supra* note 41, at 50 (emphasis added).
[255] *See* Lawson, *supra* note 3, at 20–21.
[256] Aaron Wildavsky, *Playing It Safe Is Dangerous*, 8 REG. TOXICOLOGY AND PHARMACOLOGY 283, 287 (1988).

and dangerous. Aspects of current cyber policy discourse parallel the run-up to the Iraq War and pose the same dangers. Pre-war threat inflation and conflation of threats led us into war on shaky evidence. By focusing on doomsday scenarios and conflating cyber threats, government officials threaten to legislate, regulate, or spend in the name of cybersecurity based largely on fear, misplaced rhetoric, conflated threats, and credulous reporting. The public should have access to classified evidence of cyber threats, and further examination of the risks posed by those threats, before sound policies can be proposed, let alone enacted.

Furthermore, we cannot ignore parallels between the military-industrial complex and the burgeoning cybersecurity industry. As President Eisenhower noted, we must have checks and balances on the close relationships between parties in government, defense, and industry. Relationships between these parties and their potential conflicts of interest must be considered when weighing cybersecurity policy recommendations and proposals.

Before enacting policy in response to cyber threats, policymakers should consider a few things. First, they should end the cyber rhetoric. The alarmist rhetoric currently dominating the policy discourse is unhelpful and potentially dangerous. Next, they should declassify evidence relating to cyber threats. Overclassification is a widely acknowledged problem, and declassification would allow the public to verify before trusting blindly. They must also disentangle the disparate cyber threats so that they can determine who is best suited to address which threats. In cases of cyber crime and cyber espionage, for instance, private network owners may be best suited and may have the best incentive to protect their own valuable data, information, and reputations. After disentangling threats, policymakers can then assess whether a market failure or systemic problem exists when it comes to addressing each threat. Finally, they can estimate the costs and benefits of regulation and its alternatives and determine the most effective and efficient way to address disparate cyber threats.

No one wants a "cyber Katrina" or a "digital Pearl Harbor." But honestly assessing cyber threats and appropriate responses does not mean that we have to learn to stop worrying and love the cyber bomb.