No. 11-01
January 2011

WORKING PAPER

BEYOND CYBER-DOOM:
Cyberattack Scenarios and the Evidence of History

By Sean Lawson

MERCATUS CENTER
George Mason University

The ideas presented in this research are the author's and do not represent official positions of the Mercatus Center at George Mason University.

Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History

Sean Lawson, Ph.D.
Department of Communication
University of Utah

"[T]hese war games are about the real effects of a cyberwar . . . about causing chaos in our streets at home due to sudden crashes in our critical infrastructure through manipulation of our banking, transportation, utilities, communications, and other critical infrastructure industries. These are all real scenarios." (Patterson, 2010b)

"In seeking a prudent policy, the difficulty for decision-makers is to navigate the rocky shoals between hysterical doomsday scenarios and uninformed complacency." (Cavelty, 2007: 144)

Introduction

Recently, news media and policy makers in the United States have turned their attention to prospective threats to and through an ethereal and ubiquitous technological domain referred to as "cyberspace." "Cybersecurity" threats include attacks on critical infrastructures like power, water, transportation, and communication systems launched via cyberspace, but also terrorist use of the Internet, mobile phones, and other information and communication technologies (ICTs) for fundraising, recruiting, organizing, and carrying out attacks (Deibert & Rohozinski, 2010). Frustration over a perceived lack of public and policy maker attention to these threats, combined with a belief that "exaggeration" and "appeals to emotions like fear can be more compelling than a rational discussion of strategy" (Lewis, 2010: 4), a number of cybersecurity proponents have deployed what one scholar has called "cyber-doom scenarios" (Cavelty, 2007: 2). These involve hypothetical tales of cyberattacks resulting in the mass collapse of critical infrastructures, which in turn leads to serious economic losses, or even total economic, social, or civilizational collapse. These tactics seem to have paid off in recent years, with cybersecurity finding its way onto the

agendas of top civilian and military policy makers alike. The results have included the creation of a White House "cybersecurity czar," the creation of the military's U.S. Cyber Command, the drafting of a plan for Trusted Identities in Cyberspace, and the consideration of several cybersecurity-related pieces of legislation by the U.S. Congress (Gates, 2009; Olympia J. Snowe Press Releases 2009b; Rotella, 2009; Lieberman et al., 2010; Rockefeller & Snowe, 2010; Schmidt, 2010; Hathaway, 2010).

This paper examines the cyber-doom scenarios upon which so much of contemporary, U.S. cybersecurity discourse has relied. It seeks to: 1) place cyber-doom scenarios into a larger historical context; 2) assess how realistic cyber-doom scenarios are; and 3) draw out the policy implications of relying upon such tales, as well as alternative principles for the formulation of cybersecurity policy. To address these issues, this paper draws from research in the history of technology, military history, and disaster sociology. This paper argues that 1) cyber-doom scenarios are the latest manifestation of long-standing fears about "technology-out-of-control" in Western societies; 2) tales of infrastructural collapse leading to social and/or civilizational collapse are not supported by the current body of empirical research on the subject; and 3) the constant drumbeat of cyber-doom scenarios encourages the adoption of counter-productive policies focused on control, militarization, and centralization. This paper argues that cybersecurity policy should be 1) based on more realistic understandings of what is possible that are informed by empirical research rather than hypothetical scenarios and 2) guided by principles of resilience, decentralization, and self-organization.

Cybersecurity Concerns: Past and Present

Over the last three decades, cybersecurity proponents have presented a shifting and sometimes ambiguous case for what exactly is being threatened, and by whom, in and through cyberspace. During the 1980s, the main cybersecurity concern was foreign espionage via the exploitation of the United States's increasing dependence on computers and networks. Then, in the 1990s, experts began writing about the supposed threat to civilian critical infrastructures by way of cyberterrorism conducted by non-state actors. In the opening days of the Bush administration, cybersecurity proponents replaced non-state actors with state actors as the dominant threat subject.[1] But in the immediate aftermath of 9/11, the threat perception shifted back to non-state terrorists using cyberspace to attack critical infrastructure. Then, in the run-up to the Iraq war in 2003, state actors once more became the supposed threat subjects, with Saddam Hussein's Iraq making the list of states with a cyberwar capability (Weimann, 2005: 133–134; Bendrath, 2001; Bendrath, 2003; Cavelty, 2007). Recent policy documents identify a combination of state actors working directly or indirectly via non-state proxies—e.g. "patriotic hackers" or organized crime—to target information in the form of private intellectual property and government secrets (The White House, 2009a; White House Press Office, 2009; Langevin et al., 2009).

In the last three years, several high-profile "cyberattack" incidents have served to focus attention on cybersecurity even more sharply than before. These have included two large-scale cyberattacks attributed to Russia: one against the Baltic nation of Estonia in the spring of 2007 (Blank, 2008; Evron, 2008) and one against the nation of Georgia in July and August of 2008

[1] The term "threat subject" is from the work on "securitization theory" conducted by the Copenhagen School of security studies (See Buzan *et. al.* 1998). Using a grammatical analogy, securitization theory posits that the process of constructing security threats involves the identification of those actors that are the cause of the threat (e.g. threat subjects) and that which is threatened (e.g. referent objects).

that coincided with a Russian invasion of that country (The Frontrunner, 2008; Bumgarner & Borg, 2009; Korns & Kastenberg, 2008; Nichol, 2008). In January 2010, Google's accusations of Chinese cyberattacks against it garnered a great deal of press attention and were featured prominently in Secretary of State Clinton's speech on "Internet Freedom" (Clinton, 2010).[2] Most recently, some many have speculated that a computer worm called Stuxnet may have been a cyberattack by Israel on Iranian nuclear facilities (Mills, 2010).

Cyber-Doom Scenarios

Despite persistent ambiguity in cyber-threat perceptions, cyber-doom scenarios have remained an important tactic used by cybersecurity proponents. Cyber-doom scenarios are hypothetical stories about prospective impacts of a cyberattack and are meant to serve as cautionary tales that focus the attention of policy makers, media, and the public on the issue of cybersecurity. These stories typically follow a set pattern involving a cyberattack disrupting or destroying critical infrastructure. Examples include attacks against the electrical grid leading to mass blackouts, attacks against the financial system leading to economic losses or complete economic collapse, attacks against the transportation system leading to planes and trains crashing, attacks against dams leading floodgates to open, or attacks against nuclear power plants leading to meltdowns (Cavelty, 2007: 2).

Recognizing that modern infrastructures are closely interlinked and interdependent, such scenarios often involve a combination of multiple critical infrastructure systems failing simultaneously, what is sometimes referred to as a "cascading failure." This was the case in the "Cyber Shockwave" war game televised by CNN in February 2010, in which a computer worm

[2] Leaked U.S. diplomatic cables published by WikiLeaks.org seem to corroborate this accusation (Shane & Lehren, 2010).

spreading among cell phones eventually led to serious disruptions of critical infrastructures (Gaylord, 2010). Even more ominously, in their recent book, Richard Clarke and Robert Knake (2010: 64–68) present a scenario in which a cyberattack variously destroys or seriously disrupts all U.S. infrastructure in only fifteen minutes, killing thousands and wreaking unprecedented destruction on U.S. cities.

Surprisingly, some argue that we have already had attacks at this level, but that we just have not recognized that they were occurring. For example, Amit Yoran, former head of the Department of Homeland Security's National Cyber Security Division, claims that a "cyber-9/11" has already occurred, "but it's happened slowly so we don't see it." As evidence, he points to the 2007 cyberattacks on Estonia, as well as other incidents in which the computer systems of government agencies or contractors have been infiltrated and sensitive information stolen (Singel, 2009). Yoran is not alone in seeing the 2007 Estonia attacks as an example of the cyber-doom that awaits if we do not take cyber threats seriously. The speaker of the Estonian parliament, Ene Ergma, has said that "When I look at a nuclear explosion, and the explosion that happened in our country in May, I see the same thing" (Poulsen, 2007).

Cyber-doom scenarios are not new. As far back as 1994, futurist and best-selling author Alvin Toffler claimed that cyberattacks on the World Trade Center could be used to collapse the entire U.S. economy. He predicted that "They [terrorists or rogue states] won't need to blow up the World Trade Center. Instead, they'll feed signals into computers from Libya or Tehran or Pyongyang and shut down the whole banking system if they want to. We know a former senior intelligence official who says, 'Give me $1 million and 20 people and I will shut down America. I could close down all the automated teller machines, the Federal Reserve, Wall Street, and most hospital and business computer systems'" (Elias, 1994).

But we have not seen anything close to the kinds of scenarios outlined by Yoran, Ergma, Toffler, and others. Terrorists did not use cyberattack against the World Trade Center; they used hijacked aircraft. And the attack of 9/11 did not lead to the long-term collapse of the U.S. economy; we would have to wait for the impacts of years of bad mortgages for a financial meltdown. Nor did the cyberattacks on Estonia approximate what happened on 9/11 as Yoran has claimed, and certainly not nuclear warfare as Ergma has claimed. In fact, a scientist at the NATO Co-operative Cyber Defence Centre of Excellence, which was established in Tallinn, Estonia in response to the 2007 cyberattacks, has written that the immediate impacts of those attacks were "minimal" or "nonexistent," and that the "no critical services were permanently affected" (Ottis, 2010: 72).

Nonetheless, many cybersecurity proponents continue to offer up cyber-doom scenarios that not only make analogies to weapons of mass destruction (WMDs) and the terrorist attacks of 9/11, but also hold out economic, social, and even civilizational collapse as possible impacts of cyberattacks. A report from the Hoover Institution has warned of so-called "eWMDs" (Kelly & Almann, 2008); the FBI has warned that a cyberattack could have the same impact as a "well-placed bomb" (FOXNews.com, 2010b); and official DoD documents refer to "weapons of mass disruption," implying that cyberattacks might have impacts comparable to the use of WMD (Chairman of the Joint Chiefs of Staff 2004, 2006). John Arquilla, one of the first to theorize cyberwar in the 1990s (Arquilla & Ronfeldt, 1997), has spoken of "a grave and growing capacity for crippling our tech-dependent society" and has said that a "cyber 9/11" is a matter of if, not when (Arquilla, 2009). Mike McConnell, who has claimed that we are already in an ongoing cyberwar (McConnell, 2010), has even predicted that a cyberattack could surpass the impacts of 9/11 "by an order of magnitude" (*The Atlantic*, 2010). Finally, some have even compared the

impacts of prospective cyberattacks to the 2004 Indian Ocean tsunami that killed roughly a quarter million people and caused widespread physical destruction in five countries (Meyer, 2010); suggested that cyberattack could pose an "existential threat" to the United States (FOXNews.com 2010b); and offered the possibility that cyberattack threatens not only the continued existence of the United States, but all of "global civilization" (Adhikari, 2009).

In response, critics have noted that not only has the story about who threatens what, how, and with what potential impact shifted over time, but it has done so with very little evidence provided to support the claims being made (Bendrath, 2001, 2003; Walt, 2010). Others have noted that the cyber-doom scenarios offered for years by cybersecurity proponents have yet to come to pass and question whether they are possible at all (Stohl, 2007). Some have also questioned the motives of cybersecurity proponents. Various think tanks, security firms, defense contractors, and business leaders who trumpet the problem of cyber attacks are portrayed as self-interested ideologues who promote unrealistic portrayals of cyber-threats (Greenwald, 2010).

While I am sympathetic to these arguments, in this essay I would like for a moment to assume that mass disruption or destruction of critical infrastructure systems are possible entirely through the use of cyberattack. Thus, the goal in this paper will be 1) to understand the origins of such fears, 2) to assess whether the supposed second-order effects (i.e. economic, social, or civilizational collapse) of cyberattack are realistic, and 3) to assess the policy implications of relying upon such scenarios.

Cyber-Doom and Technological Pessimism

Several scholars have asked why there is such a divergence between cyber-doom scenarios and the few incidents of actual cyberattack that we have thus far witnessed (Stohl, 2007;

Weimann, 2008: 42). They have resolved the paradox, in part, by pointing to the fact that fears of cyberterrorism and cyberwar combine a number of long-standing human fears, including fear of terrorism (especially since 9/11), fear of the unknown, and fear of new technologies (Stohl, 2007; Weimann, 2008: 42; Embar-Seddon, 2002: 1034). Here I will focus on the third of these, the fear of "technology out of control" as an increasingly prominent fear held by citizens of Western, industrial societies over the last century. Concerns about cybersecurity are but the latest manifestation of this fear.

Historians of technology have written extensively about the rise of the belief in "autonomous technology" or "technological determinism" in Western societies, as well as the increasingly prominent feelings of pessimism and fear that have come along with these beliefs. While many in the nineteenth century believed that technological innovation was the key to human progress (Hughes, 2004), throughout the course of the twentieth century, many began to question both humanity's ability to control its creations, as well as the impacts of those creations. Thus, we have seen the emergence of "the belief that technology is the primary force shaping the post-modern world" (Marx, 1997: 984) but also "that somehow technology has gotten out of control and follows its own course, independent of human direction" (Winner, 1977: 13). As a result, we have also seen the emergence of an increasing sense of "technological pessimism" (Marx, 1994: 238), a sense of ambivalence towards technology in which we at once marvel at the innovations that have made modern life possible, but also "a gathering sense . . . of political impotence" and "the feeling that our collective life in society is uncontrollable" as a result of our increasing dependence upon technology (Marx, 1997: 984). Technological determinism, both optimistic and pessimistic, is found in a number of recent and influential scholarly and popular works that address the role of technological change in society. These include Manuel Castells'

mostly optimistic work, which identifies information and knowledge working on themselves in a feedback loop as being the core of the new economy (Castells, 2000), and Kevin Kelly's more recent and more pessimistic work that posits definition an emergent, self-reinforcing, technology dependent society he calls the "technium" (Kelly, 2010).

The character of the technologies that are most prominent in our lives has indeed changed over the last century, from individual mechanical devices created by individual inventors to large socio-technical systems created and managed by large, geographically dispersed organizations (Marx, 1994: 241; Marx, 1997: 972–974). In the twentieth century, we came to realize that "Man now lives *in* and *through* technical creations" (Winner, 1977: 34) and to "entertain the vision of a postmodern society dominated by immense, overlapping, quasi-autonomous technological systems," in which society itself becomes "a meta-system of systems upon whose continuing ability to function our lives depend." It is no wonder that the "inevitably diminished sense of human agency" that attends this vision should lead to pessimism and fear directed at technology (Marx, 1994: 257).

That these fears are manifest in contemporary concerns about cybersecurity should not come as a surprise. Scholars have noted that our reactions to new technologies are often "mediated by older attitudes" (Marx, 1994: 239) which often include a familiar "pattern of responses to new technologies that allure [and] threaten" (Simon, 2004: 23). Many of the concerns found in contemporary cybersecurity discourse are not unique, but rather, have strong corollaries in early 20th-century concerns about society's increasing reliance upon interdependent and seemingly fragile infrastructure systems of various types, including electronic communication networks.

Early forms of electronic communication, including the radio, telegraph, and telephone, sparked fear and anxiety by government officials and the public alike that are similar to contemporary concerns about cybersecurity. The U.S. Navy was initially reluctant to adopt the radio, in part because of concern over what today would be called "information assurance" (Douglas, 1985). The early twentieth century saw an explosion in the number of amateur radio users in the United States who could not only "listen in" on military radio traffic, but who could also broadcast on the same frequencies used by the military. Amateur broadcasts could clog the airwaves, preventing legitimate military communications, but could also be used to feed false information to ships at sea. In response, the Navy worked to have amateurs banned from the airwaves. They succeeded only in 1912 after it was reported that interference by amateur radio operators may have hampered efforts to rescue survivors of the *Titanic* disaster. After 1912, amateurs were limited to the shortwave area of the electromagnetic spectrum and during World War I, the U.S. government banned amateur radio broadcast entirely (Douglas, 2007: 214–215).

Contemporary cybersecurity concerns also echo the fears and anxieties that telephone and telegraph systems caused in the early 20th century. Along with transcontinental railroad networks, these "new networks of long-distance communication," which could not be "wholly experienced or truly seen," were the first of the kind of large, complex, nation-spanning, socio-technical systems that were at the heart of the last century's increasing technological pessimism (MacDougall, 2006: 720). The new communication networks were often portrayed in popular media as constituting a new space, a separate world dominated by crime, daring, and intrigue (MacDougall, 2006: 720–721). While the new communication network "gave new powers to its users, [it] also compounded the ability of distant people and events to affect those users' lives" (MacDougall, 2006: 718). In short, it introduced the power and danger of "action at a distance—

the ability to act in one place and affect the lives of people in another" (MacDougall, 2006: 721). Many worried that the combination of action at a distance and the relative anonymity offered by the new communication networks would allow people to more readily engage in immoral activities like gambling, that the networks would become tools of organized crime, and even that nefarious "wire devils" could use the telegraph to crash the entire U.S. economy (MacDougall, 2006: 724–726). Even if particular nefarious actors could not be identified, the mere fact of a "complex interdependence of technology, agriculture, and national finance" that was difficult if not impossible to apprehend was itself enough to cause anxiety (MacDougall, 2006: 724).

As in cybersecurity discourse, these fears were reflective of a more generalized anxiety about the supposed interdependence and fragility of modern, industrial societies. This anxiety shaped the thinking of military planners on both sides of the Atlantic. Early airpower theorists in the United States and the United Kingdom had these beliefs at the heart of their plans for the use of strategic bombardment. For example, in his influential 1925 book, *Paris, or the Future of War*, B.H. Liddell Hart (1925: 41) argued that "A modern state is such a complex and interdependent fabric that it offers a target highly sensitive to a sudden and overwhelming blow from the air." He continued, "a nation's nerve-system, no longer covered by the flesh of its troops, is now laid bare to attack, and, like the human nerves, the progress of civilization has rendered it far more sensitive than in earlier and more primitive times" (Hart, 1925: 37). In the United States, Major William C. Sherman, who co-authored the 1922 *Air Tactics* text used to train American pilots, believed industrialization to be both a blessing and a curse and his "industrial fabric" theory of aerial bombardment started from the assumption that the "very quality of modern industry renders it vulnerable" to aerial attack (Sherman, 1926: 217–218).

Like cyberwar theorists today, airpower theorists argued that the unique vulnerabilities resulting from society's new-found dependence on interlocking webs of production, transportation, and communication systems could be exploited to cause almost instantaneous chaos, panic, and paralysis in a society (Konvitz, 1990; Biddle, 2002). But just as neither telegraph "wire devils" nor nefarious Internet hackers were the cause of the economic troubles of 1929 or 2008, so too did the predictions of quick victory from the air miss their mark. In the next section, we will see that modern societies and the systems upon which they rely have proved far more resilient than many have assumed.

History & Sociology of Infrastructure Failure

Even today, planning for disasters and future military conflicts alike, including planning for future conflicts in cyberspace, often relies upon hypothetical scenarios that begin with the same assumptions about infrastructural and societal fragility found in early 20th-century theories of strategic bombardment. Some have criticized what they see as a reliance in many cases upon hypothetical scenarios over empirical data (Glenn, 2005; Dynes, 2006; Graham & Thrift, 2007: 9–10; Ranum, 2009; Stiennon, 2009). But, there exists a body of historical and sociological data upon which we can draw, which casts serious doubt upon the assumptions underlying cyber-doom scenarios. Work by scholars in various fields of research, including the history of technology, military history, and disaster sociology has shown that both infrastructures and societies are more resilient than often assumed by policy makers.

WWII Strategic Bombing

Interwar assumptions about the fragility of interdependent industrial societies and their vulnerability to aerial attack proved to be inaccurate. Both the technological infrastructures and social systems of modern cities proved to be more resilient than military planners had assumed. Historian Joseph Konvitz (1990) has noted that "More cities were destroyed during World War II than in any other conflict in history. Yet the cities didn't die." Some critical infrastructure systems like power grids even seem to have improved during the war. Historian David Nye (2010: 48) reports that the United Kingdom, Germany, and Italy all "increased electricity generation." In fact, most wartime blackouts were self-inflicted and in most cases did not fool the enemy or prevent the dropping of bombs (Nye, 2010: 65).

Similarly, social systems proved more resilient than predicted. The postwar U.S. Strategic Bombing Survey, as well as U.K. studies of the reaction of British citizens to German bombing, all concluded that though aerial bombardment led to almost unspeakable levels of pain and destruction, "antisocial and looting behaviors . . . [were] not a serious problem in and after massive air bombings" (Quarantelli, 2008: 882) and that "little chaos occurred" (Clarke, 2002: 22). Even in extreme cases, such as the the atomic bombing of Hiroshima, social systems proved remarkably resilient. A pioneering researcher in the field of disaster sociology describes that

> within minutes [of the Hiroshima blast] survivors engaged in search and rescue, helped one another in whatever ways they could, and withdrew in controlled flight from burning areas. Within a day, apart from the planning undertaken by the government and military organizations that partly survived, other groups partially restored electric power to some areas, a steel company with 20 percent of workers attending began operations again, employees of the 12 banks in Hiroshima assembled in the Hiroshima branch in the city and began making payments, and trolley lines leading into the city were completely cleared with partial traffic restored the following day (Quarantelli, 2008: 899).

Even in the most extreme cases of aerial attack, people neither panicked, nor were they paralyzed. Strategic bombardment alone was not able to exploit infrastructure vulnerability and fragility to destroy the will to resist of those that were targeted from the air (Freedman, 2005: 168; Nye, 2010: 43; Clodfelter, 2010).

In the aftermath of the war, it became clear that theories about the possible effects of aerial attack had suffered from a number of flaws, including a technological determinist mindset, a lack of empirical evidence, and even willfully ignoring evidence that should have called into question assumptions about the interdependence and fragility of both technological and social systems. In the first case, Konvitz (1990) has argued that "The strategists' fundamental error all along had been [giving] technology too much credit, and responsibility, for making cities work—and [giving] people too little." In his study of U.S. bombardment of Germany, Clodfelter (2010) concluded that the will of a nation is determined by multiple factors, both social and technical, and that it therefore takes more than targeting any one technological system or social group to break an enemy's will to resist. Similarly, Konvitz (1990) concluded that, "Immense levels of physical destruction simply did not lead to proportional or greater levels of social and economic disorganization."

Next, theories of strategic bombardment either suffered from a lack of supporting evidence or even ignored contradictory evidence. Lawrence Freedman (2005: 168) has lamented that interwar theories of strategic bombardment were implemented despite the fact that they lacked specifics about how results would be achieved or empirical evidence about whether those results were achievable at all. Military planners were not able to point to real-world examples of the kind of social or technological collapse that they claimed would result from aerial attack. But they were not deterred by this lack of empirical evidence. Instead, they maintained that "The fact

that infrastructure systems had not failed . . . is no proof that they are not susceptible to failure" and instead "emphasized how air raids *could* exploit the same kind of collapse that *might* come in peace" (Emphasis added. Konvitz, 1990). Airpower theorists were not even deterred by seemingly contradictory evidence. Instead, such evidence was either ignored or explained away. For example, during the 1930s, New York City suffered a series of blackouts that demonstrated that the social disruption caused by the sudden lack of power was not severe. In response, airpower theorists argued that the results would have been different had the blackouts been the result of intentional attack (Konvitz, 1990). But the airpower theorists missed the mark in that prediction too. Instead of leading to panic or paralysis, intentional aerial bombardment of civilians "angered them and increased their resolution" (Nye, 2010: 43; Freedman, 2005: 170).

The social reaction to strategic bombardment is just one example of how efforts both to carry out, but also to defend against, such attacks often led to results that were the opposite of what was predicted or intended. One study of the mental-health effects among victims of strategic bombing found that excessive precautionary measures taken in an attempt to prevent the panic and paralysis predicted by theorists did more to "weaken society's natural bonds and, in turn, create anxious and avoidant [sic] behavior" than did the actually bombing (Jones et al., 2006: 57). Similarly, in cases of intentional, self-inflicted blackouts, fear of what might happen to society were the power grid to fail led to a self-inflicted lack of power that not only did not have the desired military effect but may also have been an example of excessive, counter-productive precaution (Nye, 2010: 65).

The flawed assumptions and predictions of the airpower theorists had political and military impacts as well. By creating fear of a massive, German reprisal from the air, the promise of mass destruction from the air that military planners had offered civilian policy makers factored heavily

into the British decision not to enter the war sooner to stop Hitler's aggression (Biddle, 2002: 2). Once the war began, the failure of the theorists' vision did not lead them to give up on the dream of strategic bombardment, but only to "heavier, less discriminate bombing." As historian Tami Davis Biddle (2002: 9) has argued, "The result was nothing less than a form of aerial Armageddon played out over the skies of Germany and Japan."

Disaster Myths

Even though the vision of the airpower theorists had been proven false, assumptions about the fragility of modern societies did not disappear when the war ended. The first use of atomic weapons at the close of the war combined with the beginning of the Cold War nuclear stand-off with the Soviet Union kept the old assumptions alive. Surely, U.S. military planners believed, atomic weapons could achieve what strategic bombardment with conventional weapons had not. Thus, fearing "that the American civilian population might collapse in the face of atomic attack," the U.S. military began to support empirical research into the ways that people respond in disaster situations (Quarantelli, 2008: 896). Ironically, the results of that research have consistently called into question the military assumptions that were the original motivation for funding the study of disasters.

Disaster researchers have worked to define more clearly the concepts at the heart of dominant assumptions about how people respond to disaster. Official planning documents, news, and entertainment media alike often assume that in crisis situations people will either be paralyzed or panicked. On the one hand, paralysis can involve "passivity and inaction" in the face of an overwhelming situation (Quarantelli, 2008: 887). This reaction is dangerous because individuals, groups, and entire societies are not able to help themselves and others if they are

paralyzed by fear. On the opposite extreme, psychologists and sociologists have defined panic as a heightened level of fear and emotion by an individual or group leading to a degradation of rational thinking and decision-making, a breakdown of social cohesion, and ultimately to injudicious and counterproductive actions that bring more harm or threat of harm (Clarke, 2002: 21; Clarke & Chess, 2009: 998–999; Jones et al., 2006: 58). In short, both paralysis and panic are maladaptive responses to fear, one an under-reaction, the other an overreaction.

Perhaps surprisingly, empirical research has shown repeatedly that "contrary to . . . popular portrayals" by media and officials, "group panic is relatively rare" (Clarke, 2002: 21). Even specific antisocial behaviors such as looting, which is often believed to be a widespread problem in the wake of most disasters, has proven to be "unusual in the typical natural and technological disasters that afflict modern, Western-type societies" (Quarantelli, 2008: 883). Instead of panic or paralysis, "decades of disaster research shows that people behave rationally in the face of danger" (Dynes, 2006). Empirical research has shown that "survivors usually quickly moved to do what could be done in the situation," that their "behavior is adaptive" rather than maladaptive, and that such behavior usually includes "widespread altruism that leads to free and massive giving and sharing of goods and services." The survivors themselves "are truly the first responders in disasters" (Quarantelli, 2008: 885–888). Instead of panic or paralysis leading to social collapse, existing social bonds and norms of behavior are the key assets to effective response, in part because they serve to constrain tendencies towards paralysis, panic, antisocial, or other types of maladaptive behavior (Johnson, 1987: 180).

Blackouts

These results have been confirmed by studying various disasters both large and small, intentional and accidental, technological and natural, including large-scale blackouts, hurricanes, and terrorist attacks. For example, attacks upon the electrical grid are often featured prominently in cyber-doom scenarios. But historically, just what has happened when the power has gone out? As mentioned above, a series of blackouts in New York City in the 1930s indicated that people did not panic and society did not collapse at the loss of electrical power (Konvitz, 1990). That pattern continued through the remainder of the last century, where "terror, panic, death, and destruction were not the result" of power outages. Instead, as Nye (2010: 182–183) has shown, "people came together [and] helped one another," just as they do in most disaster situations.

In August 2003, many initially worried that the two-day blackout that affected 50 million people in the United States and Canada was the result of a terrorist attack. Even after it was determined that it was not, some wondered what might happen if such a blackout were to be the result of intentional attack. One commentator hypothesized that an intentional "outage would surely thwart emergency responders and health-care providers. It's a scenario with disastrous implications" (McCafferty, 2004). But the actual evidence from the actual blackout does not indicate that there was panic, chaos, or "disastrous implications." While the economic costs of the blackout were estimated between four and ten billion dollars (Minkel, 2008; Council, 2004), the human and social consequences were quite minor. Few if any deaths are attributed to the blackout.[3] A sociologist who conducted impromptu field research of New York City residents' responses to the incident reported that there was no panic or paralysis, no spike in crime or antisocial behavior, but instead, a sense of solidarity, a concern to help others and keep things

[3] One report has claimed that as many as eleven deaths can be directly attributed to the blackout (Minkel, 2008).

running as normally as possible, and even a sense of excitement and playfulness at times (Yuill, 2004). For example, though the sudden loss of traffic lights did lead to congestion, he notes that the situation was mitigated by "people spontaneously taking on traffic control responsibilities. Within minutes, most crossing points and junctions were staffed by local citizens directing and controlling traffic . . . All of this happened without the assistance of the normal control culture; the police were notably absent for long periods of the blackout" (Yuill, 2004). James Lewis (2006) of the Center for Strategic and International Studies has observed that "The widespread blackout did not degrade U.S. military capabilities, did not damage the economy, and caused neither casualties nor terror."

Despite the fact that historical and sociological evidence has shown that "People are irked but not terrified at the prospect" of power loss (Nye, 2010: 191), and, therefore, that intentional attacks on the power grid are "not likely to cause the same type of immediate fear and emotion" as a conventional attack (Stohl, 2007), scenarios in which the loss of power leads to panic, chaos, and social collapse persist because of the persistence of a technological determinist mindset among officials, the media, and the general public. Nye has observed that most reports that are written about blackouts after the fact focus on technical reasons for failures and technical or bureaucratic changes to avoid such failures in the future (Nye, 2010: 4). Not surprisingly, most of the policy response to the 2003 blackout has fit this pattern (Minkel, 2008). What gets overlooked in these accounts and the types of policy responses they encourage is the human capacity for "adaptation and improvisation in the face of crisis" (Nye, 2010: 195).

9/11 & Katrina

As mentioned above, some have argued that a so-called "cyber-9/11" could approximate or even exceed the impacts of the terrorist attacks of September 11, 2001. Others, including the sponsors of cybersecurity legislation, as well as a former White House cybersecurity czar, have spoken of a possible "cyber-Katrina" (Epstein, 2009; Olympia J. Snowe Press Releases 2009b). But, in both of those cases, people generally responded in the ways that they have in other disasters, without panic, paralysis, or social collapse. Disaster sociologist Lee Clarke has noted that on 9/11, "people did not become hysterical but instead created a successful evacuation" (Clarke, 2002: 23). That evacuation of Lower Manhattan, which involved nearly half a million people, "was a self-organized volunteer process that could probably never have been planned on a government official's clipboard" (Glenn, 2005). At the economic level, the Congressional Research Service concluded that "The loss of lives and property on 9/11 was not large enough to have had a measurable effect on the productive capacity of the United States" (Makinen, 2002). A more recent report by the Center for Risk and Economic Analysis of Terrorism Events showed that the overall economic impacts of the 9/11 attacks were even lower than initially estimated, indicating that the U.S. economy is more resilient in the face of disaster and intentional attack than commonly assumed (2010a). At the geopolitical level, if the goal of the terrorists was to drive the United States from the Middle East, then the 9/11 attacks backfired. Just as World War Two aerial bombardment often served to strengthen rather than weaken the will to resist among targeted populations, Freedman (2005: 169) has observed that "The response [to 9/11] was not to encourage the United States to abandon any involvement with the conflicts of the Muslim world but to draw them further in."

Finally, analysis of Hurricane Katrina by disaster sociologists has show that while there was some looting and antisocial behavior in the immediate aftermath of the disaster, people generally did not panic and Katrina did not result in the kind of social chaos and collapse often implied in media coverage of the event. Quarantelli (2008: 888–889) reports that "pro-social and very functional behavior dwarfed on a very large scale the antisocial behavior that also emerged. . . . [This] prevented the New Orleans area from a collapse into total social disorganization."[4] Like the attacks of 9/11, though the economic impacts of Katrina were severe, especially for those areas in the Golf Coast that were immediately affected, Katrina did not have the effect of collapsing the entire U.S. economy. And while some suggested that U.S. military operations in Iraq slowed the National Guard's response to Katrina (Gonzales, 2005), there was no indication that military response to Katrina had a negative effect upon U.S. military operations overseas or overall military readiness.

The empirical evidence provided to us from historians and sociologists about the impacts of infrastructure disruption, both intentional and accidental, as well as peoples' collective response to disasters of various types, calls into question the kinds of projections one finds in the cyber-doom scenarios. If the mass destruction of entire cities from the air via conventional and atomic weapons generally failed to deliver the panic, paralysis, technological and social collapse, and loss of will that was intended, it seems unlikely that cyberattack would be able to achieve these results. It also seems unlikely that a "cyber-9/11" or a "cyber-Katrina" would result in the loss of life and physical destruction seen in the real 9/11 and Katrina. And if the real 9/11 and Katrina did not result in social or economic collapse, nor to a degradation of military readiness or national will, then it seems unlikely that their "cyber" analogues would achieve these results.

[4] Research conducted as part of the Gulf Coast Recovery Project at the George Mason University's Mercatus Center has corroborated these findings. See http://mercatus.org/program/research/1000005.

Policy Implications

None of the discussion above should suggest, however, that we should not take cybersecurity seriously, that we should not take measures to secure our critical infrastructures, or that we should not prepare to mitigate against the effects of a large-scale cyberattack should it occur. Rather, it should suggest that taking these issues seriously requires that we re-evaluate the assumptions upon which policymaking proceeds, that we can only make effective policy if we begin with a realistic assessment of what is possible based on empirical research. Thus, in the remainder of this essay, I identify potential negative policy implications of cyber-doom scenarios and offer a set of principles that can be used to guide the formulation and evaluation of cybersecurity policy.

Negative Impacts of Flawed Assumptions

The language that we use to frame problems opens up some avenues for response while closing off others. In cyber-doom scenarios, cybersecurity is framed primarily in terms of "war" and, with the use of terms like "cyber-9/11" and "cyber-Katrina," in terms of large-scale "disaster." This war/disaster framing can lead to a militarist, command and control mindset that is ultimately counter-productive.

A war framing implies the need for military solutions to cybersecurity challenges, even though most of what gets lumped under the term "cyberwar" are really acts of crime, espionage, or political protest, and even though it is not at all clear that a military response is either appropriate or effective (Lewis, 2010). Nonetheless, the establishment of the military's U.S. Cyber Command (USCYBERCOM) has been the most significant U.S. response yet to perceived cyber-threats.

Such a response is fraught with danger. First, the very existence of USCYBERCOM, which has both an offensive and defensive mission, could undermine the U.S. policy of promoting a free and open Internet worldwide by encouraging greater Internet censorship and filtering, as well as more rapid militarization of cyberspace (Cavelty, 2007: 143). For example, some have already called for USCYBERCOM to launch strikes on WikiLeaks, which leaked hundreds of thousands of classified U.S. documents about the wars in Iraq and Afghanistan (McCullagh, 2010b; Whitton, 2010; Thiessen, 2010). Such a response would only serve to create a "say-do gap" (Mullen, 2009) that potential adversaries could use to justify their own development and use of offensive cyber weapons and efforts to thwart whatever possibility there is for international cooperation on cybersecurity.

Second, there is the danger of "blow back." In a highly interconnected world, there is no guarantee that an offensive cyberattack launched by the United States against another country would not result in serious collateral damage to noncombatants or even end up causing harm to the United States (Cavelty, 2007: 143). Such "blow back" may have occurred in a recent case where the United States military took down a Jihadist discussion forum, causing collateral damage to noncombatant computers and websites, as well as undermining an ongoing U.S. intelligence gathering operation (Nakashima, 2010).

Third, there is the risk of conflict escalation from cyberattack to physical attack. If the United States launched a cyberattack against a state or non-state actor lacking the capability to respond in kind, that actor might chose to respond with physical attacks (Clarke, 2009). There have even been calls for the United States to respond with conventional military force to cyberattacks that amounted to little more than vandalism (Zetter, 2009; Dunn, 2010). Finally, a 2009 review of U.S. military strategy documents, combined with statements from officials,

further adds to the confusion and potential for escalation by indicating that nuclear response remains on the table as a possible U.S. response to cyberattack (Markoff & Shanker, 2009; Owens et al., 2009).

Next, a disaster framing portends cybersecurity planning dominated by the same "command and control [C2] model" rooted in flawed assumptions of inevitable "panic" and "social collapse" that has increasingly dominated official U.S. disaster planning (Quarantelli, 2008: 897). The result has been ever more centralized, hierarchical, and bureaucratic disaster responses that increasingly rely upon the military to restore order and official control first and foremost (Quarantelli, 2008: 895–896; Alexander, 2006; Lakoff, 2006). The result can be a form of "government paternalism" in which officials panic about the possibility of panic and then take actions that exacerbate the situation by not only failing to provide victims with the help they need, but also preventing them from effectively helping themselves (Dynes, 2006; Clarke & Chess, 2009: 999–1001). This phenomenon was on display in the official response to Hurricane Katrina (Clarke & Chess, 2009: 1003–1004). In the realm of cybersecurity, there are already provisions for the military's USCYBERCOM to provide assistance to the Department of Homeland Security in the event of a domestic cyber emergency (Ackerman, 2010). Reminiscent of self-imposed blackouts during WWII, Senator Joseph Lieberman's proposal for a so-called "Internet kill switch," which would give the president the authority to cut U.S. Internet connections to the rest of the world in the event of a large-scale cyberattack,[5] is the ultimate

[5] Lieberman has said, "We need the capacity for the president to say, Internet service provider, we've got to disconnect the American Internet from all traffic coming in from another foreign country… A cyber attack on America can do as much or more damage today by incapacitating our banks, our communications, our finance, our transportation, as a conventional war attack. And the president, in catastrophic cases—not going to do it every day, not going to take it over. …Right now, China, the government, can disconnect parts of its Internet in a case of war. We need to have that here, too." See http://edition.cnn.com/TRANSCRIPTS/1006/20/sotu.01.html. See also McCullagh, 2010a.

expression of the desire to regain control by developing the means to destroy that which we fear to lose.

The war/disaster framing at the heart of cyber-doom scenarios and much of contemporary U.S. cybersecurity discourse risks focusing policy on the narrowest and least likely portion of the overall cybersecurity challenge—i.e. acts of "cyberwar" leading to economic, social, or civilizational collapse—while potentially diverting attention and resources away from making preparations to prevent or mitigate the effects of more realistic but perhaps less dramatic scenarios. But, there are a number of principles that can guide the formulation and evaluation of cybersecurity policy that can help us to avoid these pitfalls.

Strive for Clear Problem Definition First and Foremost

The first step to formulating and evaluating prospective cybersecurity policies more effectively is to strive for clearer definitions of the problems to be addressed. James Lewis (2010: 1) has argued that "Pronouncements that we are in a cyber war or face cyber terror conflate problems and make effective response more difficult." Instead, he advocates that we disaggregate the different types of cyber-threats—including cyberspace-enabled economic espionage, political and military espionage, crime, and cyberwar or cyberterror—so that each particular threat can be addressed in the most appropriate and effective manner. There is no one-size-fits-all solution. Myriam Dunn Cavelty (2007: 144), who has written the most comprehensive history of U.S. cybersecurity policy, goes even further. She urges us to take the complexity of contemporary cybersecurity problems seriously, not by reducing all challenges to "cyberwar" and thinking in terms of "hysterical doomsday scenarios," but instead by focusing "on a far broader range of potentially dangerous occurrences involving cyber-means and targets,

including failure due to human error, technical problems, and market failure apart from malicious attacks." For effective response, complex problems like contemporary cybersecurity challenges require us first and foremost to acknowledge their complexity and to work towards the clearest, most precise definitions possible, even when absolute clarity and precision are unattainable.

Seek Guidance from Empirical Research

The formulation and evaluation of cybersecurity policy needs to be guided whenever possible by empirical research and rely less on hypothetical scenarios. In the case of early airpower theory, reliance upon unchallenged assumptions and hypothetical scenarios in the face of contradictory empirical evidence had disastrous results. By relying too heavily on hypothetical, cyber-doom scenarios, current cybersecurity planning is open to the same criticism that has been leveled against contemporary disaster planning, which is that it is "organized to deal with predicted vulnerabilities rather than to mobilize social capital to deal with actual threats" (Dynes, 2006). Additionally, we should follow the recommendations of both James Lewis and Jeffrey Carr, who note that while empirical research of a technical nature is crucial, the formulation and evaluation of cybersecurity policy requires knowledge of relevant "non-technical" matters like the geopolitical, economic, legal, and other aspects of cybersecurity (Carr, 2009; Lewis, 2009). One goal of this essay has been to demonstrate the value of research conducted in the humanities and social sciences, in particular the history of technology, military history, and disaster sociology, to the analysis of cyber-threats. Finally, experts and policy makers alike need to be critical and reflexive about cybersecurity claims, constantly asking if what they are saying or hearing is based on empirical evidence or merely the reflection of long-

held anxieties about technology and recycled assumptions about infrastructural and social fragility.

Promote Resilience in Technological and Social Systems

While we should seek to prevent cyberattack when it is possible and prudent to do so, we should also promote resilience in technological and social systems. While it is unclear whether the possession of an offensive cyberwar capability will deter potential attackers, it is clear that more resilient technological and social systems are a benefit in any case, can help to mitigate the effects of a cyberattack should it occur, and can even help to deter cyberattacks by providing a would-be attacker with fewer valuable and vulnerable targets (Lewis, 2006; Nye, 2010: 189, 191).

Promote Repair, Maintenance, and Modernization of Infrastructure Systems

Promoting resilience in critical infrastructures hinges upon supporting ongoing repair, maintenance, and modernization of those systems. Recent events, such as the 2003 blackout and the 2007 collapse of the I-35 Mississippi River bridge in Minnesota, illustrate that U.S. infrastructure systems are aging and, as they do, becoming more fragile and prone to failures. In each case, it was a lack of repair and maintenance that was the cause of failure, not intentional attack (Nye, 2010: 180; Patterson, 2010a). Some have even argued that increased attention to infrastructure security has led to a reduction in funding for basic repair and maintenance activities (Liles, 2008). But repair and maintenance are the key to resilient systems, not only because they reduce the fragility of those systems and thus help to prevent failures in the first place, but also because they promote learning and adaptation among the human repair crews that

will be the first responders when failures do occur (Graham & Thrift, 2007: 5, 14; Nye, 2010: 189). Thus, instead of "think[ing] of the grid as a fortress to be protected at every point" (Nye, 2010: 197) by a central authority against total collapse caused by a hypothetical cyberattack, we should invest in the more mundane, ongoing, and essentially decentralized work of repair and maintenance that are the true source of resilient infrastructures (Graham & Thrift, 2007: 9–10). This warning against a fortress mentality and centralization of authority should apply to cyberspace itself and call into question recent calls to "re-engineer the Internet" largely under the direction of the National Security Agency (McConnell, 2010).

Promote Decentralization and Self-Organization in Social Systems

Cybersecurity policy should promote decentralization and self-organization in efforts to prevent, defend against, and respond to cyberattacks. Disaster researchers have shown that victims are often themselves the first responders and that centralized, hierarchical, bureaucratic responses can hamper their ability to respond in the decentralized, self-organized manner that has often proved to be more effective (Quarantelli, 2008: 895–896). One way that officials often stand in the way of decentralized self-organization is by hoarding information (Clarke & Chess, 2009: 1000–1001). Similarly, over the last 50 years, U.S. military doctrine increasingly has identified decentralization, self-organization, and information sharing as the keys to effectively operating in ever-more complex conflicts that move at an ever-faster pace and over ever-greater geographical distances (LeMay & Smith, 1968; Romjue, 1984; Cebrowski & Garstka, 1998; Hammond, 2001). In the case of preventing or defending against cyberattacks on critical infrastructure, we must recognize that most cyber and physical infrastructures are owned by private actors. Thus, a centralized, military-led effort to protect the fortress at every point will

not work. A combination of incentives, regulations, and public-private partnerships will be necessary. This will be complex, messy, and difficult. But a cyberattack, should it occur, will be equally complex, messy, and difficult, occurring instantaneously over global distances via a medium that is almost incomprehensible in its complex interconnections and interdependencies. The owners and operators of our critical infrastructures are on the front lines and will be the first responders. They must be empowered to act. Similarly, if the worst should occur, average citizens must be empowered to act in a decentralized, self-organized way to help themselves and others. In the case of critical infrastructures like the electrical grid, this could include the promotion of alternative energy generation and distribution methods. In this way, "Instead of being passive consumers, [citizens] can become actors in the energy network. Instead of waiting for blackouts, they can organize alternatives and become less vulnerable to either terror or natural catastrophe" (Nye, 2010: 203).

Promote Strong Local Communities, Economies, and Good Local Governance

Finally, preparation for responding to a large-scale cyberattack, or any other disaster, requires the promotion of strong local communities, economies, and good local governance. Just as more resilient technological systems can better respond in the event of failure, so too are strong social systems better able to respond in the event of disaster of any type. Historians and disaster researchers alike have documented that the response of individuals and groups in disaster situations largely depends on larger structural conditions in existence before the disaster itself. Communities that have weaker social ties among members, have corrupt or ineffective local government and law enforcement, and that suffer from economic hardship prior to a

disaster will find it more difficult if not impossible to respond effectively in a time of crisis (Nye, 2010: 185; Alexander, 2006; Lakoff, 2006).

In part, this requires policies and planning by local governments during normal, pre-disaster periods that not only promotes the growth of strong local civil-society organizations like businesses, churches, nonprofits, and neighborhood associations, but also plans to involve those organizations in post-disaster response and recovery efforts. Local governments should plan in advance to allow these organizations to be social entrepreneurs who act in a decentralized and self-organizing manner to aide in response and recovery. This could include not only planning for what government institutions can and will do in a disaster, but also what will be left to civil-society organizations, as well as which regulations from normal, non-disaster contexts might be relaxed during an emergency to allow civil-society organizations to aide in response and recovery. Finally, pre-disaster efforts by local government institutions to encourage the formation of informal network ties among the various civil-society organizations within the community can facilitate the kind of horizontal and bottom-up information sharing that is necessary to effective disaster response and recovery (Chamlee-Wright & Storr, 2008, 2009; Storr & Haeffele-Balch, 2010; Brito & Rothschild, 2009).

Conclusion

In the last three years, cybersecurity has received perhaps more attention than at any time during the last three decades. Proponents of greater cybersecurity have deployed cyber-doom scenarios that frame prospective cyber-threats in terms of "war" and "disaster" and offer the possibility of total economic, social, or even civilizational collapse. In this paper, I have argued that cyber-doom scenarios are more a reflection of long-held, but ultimately incorrect,

assumptions and fears about the fragility of modern societies and infrastructure systems than they are a realistic portrayal of what is possible as a result of cyberattack. Research by historians of technology, military historians, and disaster sociologists has shown consistently that modern technological and social systems are more resilient than military and disaster planners often assume. What's more, they have shown that fears and assumptions to the contrary often lead to a centralized, militarized quest for top-down control that is ultimately counterproductive to achieving stated policy objectives. Influenced by cyber-doom scenarios, current U.S. cybersecurity policy, with its creation of a military Cyber Command and suggestions for an "Internet kill switch," is tending towards the centralized, militarized, control-oriented, fortress mentality that research suggests is neither prudent nor effective. Instead, research suggests that effective prevention of, defense against, and mitigation in response to cyberattack requires the promotion of resilience by way of repair, maintenance, and modernization of our technological systems and decentralization, self-organization, economic strength, and good governance in our social systems.

References

Chairman of the Joint Chiefs of Staff (2004) *The National Military Strategy of the United States of America: A Strategy for Today; a Vision for Tomorrow.* Washington, D.C.: Chairman of the Joint Chiefs of Staff.

Chairman of the Joint Chiefs of Staff (2006) *The National Military Strategy for Cyberspace Operations.* Washington, D.C.: Chairman of the Joint Chiefs of Staff.

The Frontrunner, (2008) Georgia Cyberattacks Spark Debate in Washington. *The Frontrunner,* August 14, Available at: Lexis-Nexis.

The White House (2009a) *Cybersapce Policy Review: Assuring a Resilient Information and Communications Infrastructure.* Washington, D.C.: The White House.

Olympia J. Snowe Press Releases (2009b), Senator Snowe and Chairman Rockefeller Introduce Comprehensive Cybersecurity Legislation. *Olympia J. Snowe Press Releases,* 1 April, Available at: http://snowe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord_id=6306ecb2-802a-23ad-4a08-163f03f287da.

White House Press Office, (2009) Remarks By the President on Securing Our Nation's Cyber Infrastructure. *White House Press Office,* 29 May, Available at: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

NBC Los Angeles, (2010a) Study: Economic Impact of 9/11 Was "Short-Lived". *NBC Los Angeles,* 7 January, Available at: http://www.nbclosangeles.com/news/business/Study-bin-Ladens-Strategy-Was-Short-Lived.html.

FOXNews.com, (2010b) FBI Warns Brewing Cyberwar May Have Same Impact as 'Well-Placed Bomb'. *FOXNews.com,* Available at: http://.

The Atlantic, (2010) Fmr. Intelligence Director: New Cyberattack May be Worse Than 9/11. *The Atlantic,* 30 September, Available at: http://www.theatlantic.com/politics/archive/2010/09/fmr-intelligence-director-new-cyberattack-may-be-worse-than-9-11/63849/.

Ackerman S (2010), Doc of the Day: Nsa, Dhs Trade Players for Net Defense. *Danger Room,* 13 October, Available at: http://www.wired.com/dangerroom/2010/10/doc-of-the-day-nsa-dhs-trade-players-for-net-defense/.

Adhikari R, (2009) Civilization's High Stakes Cyber-Struggle: Q&A With Gen. Wesley Clark (Ret.). *TechNewsWorld,* 2 December, Available at: http://www.technewsworld.com/story/Civilizations-High-Stakes-Cyber-Struggle-QA-With-Gen-Wesley-Clark-ret-68787.html?wlc=1259861126&wlc=1259938168&wlc=1290975140.

Alexander D, 2006. *Symbolic and Practical Interpretations of the Hurricane Katrina Disaster in New Orleans.* Presentation. Understanding Katrina: Perspectives from the Social Sciences, the Forum of the Social Science Research Council (http://understandingkatrina.ssrc.org/Alexander/).

Arquilla J, (2009) Click, Click.Counting Down to Cyber 9/11. *San Francisco Chronicle,* 26 July, p. E2.

Arquilla J, Ronfeldt D (1997) Cyberwar is Coming! In Arquilla J, Ronfeldt D (eds) *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, CA: RAND, 24-60.

Bendrath R (2001) The Cyberwar Debate: Perception and Politics in Us Critical Infrastructure Protection. *Information & Security: An International Journal* 7: 80-103.

Bendrath R (2003) The American Cyber-Angst and the Real World–Any Link. In Latham R (ed) *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security.* New York: The Free Press, 49-73.

Biddle TD (2002) *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945.* Princeton, N.J: Princeton University Press.

Blank S (2008) Web War I: Is Europe's First Information War a New Kind of War? *Comparative Strategy* 27(3): 227-247.

Brito J, Rothschild DM (2009) Information Trickles Up. *Local Knowledge* 2 (August).

Bumgarner J, Borg S (2009) Overview By the Us-Ccu of the Cyber Campaign Against Georgia in August of 2008. *US-CCU Special Report* August.

Buzan B, Wæver O, Wilde Jd (1998) *Security : A New Framework for Analysis*. Boulder, Colo: Lynne Rienner Pub.

Carr J (2009) *Inside Cyber Warfare: Mapping the Cyber Underworld.* Sebastopol, CA: O'Reilly Media.

Castells M (2000) *The Rise of the Network Society*. Oxford: Blackwell Publishers.

Cavelty M (2007) *Cyber-Security and Threat Politics : U.S Efforts to Secure the Information Age.* New York: Routledge.

Cebrowski AK, Garstka JJ (1998) Network-Centric Warfare: Its Origin and Future. *Proceedings of the U.S. Naval Institute* 124(1): 28-35.

Chamlee-Wright E, Storr V, (2008) The Role of Social Entrereneurship in Post-Disaster Recovery. Working Paper, Mercatus Center at George Mason University, July, Available at: http://mercatus.org/publication/role-social-entrepreneurship-post-disaster-recovery.

Chamlee-Wright E, Storr V, (2009) Filling the Civil-Society Vacuum: Post-Disaster Policy and Community Response. Mercatus Policy Series, Policy Comment No. 22, February, Available at: http://mercatus.org/publication/filling-civil-society-vacuum-post-disaster-policy-and-community-response.

Clarke L (2002) Panic: Myth Or Reality? *Contexts* 1(3): 21-26.

Clarke L, Chess C (2009) Elites and Panic: More to Fear Than Fear Itself. *Social Forces* 87(2): 993-1014.

Clarke R (2009) War From Cybersapce. *The National Interest* October/November.

Clarke RA, Knake R (2010) *Cyber War: The Next Threat to National Security and What to Do About it.* New York: HarperCollins.

Clinton HR (2010) Remarks on Internet Freedom. Presentation to The Newseum, Washington D.C. 21 January.

Clodfelter M (2010) Aiming to Break Will: America's World War Ii Bombing of German Morale and Its Ramifications. *Journal of Strategic Studies* 33(3): 401-435.

Deibert R, Rohozinski R (2010) Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology* 4: 15-32.

Douglas SJ (1985) Technological Innovation and Organizational Change: The Navy's Adoption of Radio, 1899-1919. In (ed) *Military Enterprise and Technological Change: Perspectives on the American Experience.* Cambridge, Mass: MIT Press, 117-174.

Douglas SJ (2007) Early Radio. In Crowley D, Heyer P (eds) *Communication in History: Technology, Culture, Society.* Boston: Pearson, 210-216.

Dunn JE, (2010) North Korea 'Not Responsible' for 4 July Cyberattacks. *Network World,* 6 July, Available at: http://www.networkworld.com/news/2010/070610-north-korea-not-responsible-for.html.

Dynes R (2006) Panic and the Vision of Collective Incompetence. *Natural Hazards Observer* 31(2).

ECR Council (2004) *The Economic Impacts of the August 2003 Blackout.* Washington, DC: Electricity Consumers Resource Council.

Elias TD, (1994) Toffler: Computer Attacks Wave of Future. *South Bend Tribune (Indiana),* 2 January.

Embar-Seddon A (2002) Cyberterrorism: Are We Under Siege? *American Behavioral Scientist* 45(6): 1033-1043.

Epstein K, (2009) Fearing "Cyber Katrina," Obama Candidate for Cyber Czar Urges a "Fema for the Internet". *Business Week,* 18 February, Available at: http://www.businessweek.com/the_thread/techbeat/archives/2009/02/fearing_cyber_katrina_obama_candidate_for_cyber_czar_urges_a_fema_for_the_internet.html.

Evron G (2008) Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War. *Georgetown Journal of International Affairs* 9(Winter/Spring): 121-126.

Freedman L (2005) Strategic Terror and Amateur Psychology. *The Political Quarterly* 76(2): 161-170.

Gates RM (2009) Memorandum for Secretaries of the Military Departments, Subject: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations.

Gaylord C, (2010) Cyber Shockwave Cripples Computers Nationwide (Sorta). *Christian Science Monitor,* 16 February, Available at: http://www.csmonitor.com/Innovation/Horizons/2010/0216/Cyber-ShockWave-cripples-computers-nationwide-sorta.

Glenn D, (2005) Disaster Sociologists Study What Went Wrong in the Response to the Hurricanes, But Will Policy Makers Listen? *The Chronicle of Higher Education,* 29 September, Available at: http://chronicle.com/article/Disaster-Sociologists-Study/120178/.

Gonzales J, (2005) Iraq Mess Adds to the Problem. *New York Daily News,* Available at: http://www.commondreams.org/views05/0901-25.htm.

Graham S, Thrift N (2007) Out of Order: Understanding Repair and Maintenance. *Theory, Culture & Society* 24(3): 1-25.

Greenwald G, (2010) Mike Mcconnell, the Washpost & the Dangers of Sleazy Corporatism. *Salon.com,* 29 March, Available at: http://www.salon.com/news/opinion/glenn_greenwald/2010/03/29/mcconnell.

Hathaway M (2010) Cybersecurity: The U.S. Legislative Agenda. Presentation to Belfer Center for Science and International Affairs. 17 May.

Hammond GT (2001) *The Mind of War: John Boyd and American Security.* Washington: Smithsonian Institution Press.

Hart BHL (1925) *Paris; Or the Future of War.* New York: E.P. Dutton & Company.

Hughes TP (2004) *Human-Built World : How to Think About Technology and Culture.* Chicago: University of Chicago Press.

Johnson NR (1987) Panic and the Breakdown of Social Order: Popular Myth, Social Theory, Empirical Evidence. *Sociological Focus* 20: 171-183.

Jones E et al. (2006) Public Panic and Morale: Second World War Civilian Responses Re-Examined in the Light of the Current Anti-Terrorist Campaign. *J. of Risk Res.* 9(1): 57-73.
Kelly JJ, Almann L (2008) Ewmds: The Botnet Peril. *Policy Review* 152: http://www.hoover.org/publications/policy-review/article/5662.
Kelly K (2010) *What Technology Wants*. New York: Viking.
Konvitz JW (1990) Why Cities Don't Die: The Surprising Lessons of Precision Bombing in World War Ii and Vietnam. *American Heritage Invention & Technology Magazine* 5(3): 58-63.
Korns SW, Kastenberg JE (2008) Georgia's Cyber Left Hook. *Parameters* Winter: 60-76.
Lakoff A, 2006. *From Disaster to Catastrophe: The Limits of Preparedness.* Presentation. Understanding Katrina: Perspectives from the Social Sciences, the Forum of the Social Science Research Council (http://understandingkatrina.ssrc.org/Lakoff/).
Langevin RJR et al. (2009) *Securing Cyberspace for the 44th Presidency.* Washington, D.C.: Center for Strategic and International Studies.
LeMay GCE, Smith MGDO (1968) *America is in Danger.* New York: Funk and Wagnalls.
Lewis JA, (2006) The War on Hype. *San Francisco Chronicle,* 19 February, Available at: http://articles.sfgate.com/2006-02-19/opinion/17283144_1_cyber-attack-pandemic-avian-flu.
Lewis JA (2010) The Cyber War Has Not Begun. Unpublished manuscript, Available at: http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf.
Lewis JA (2009) The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict. Unpublished manuscript, Available at: http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf.
Lieberman SJ, Collins SS, Carper ST (2010), We Must 'Arm' Cyberspace Battlefront. *Politico,* 10 June, Available at: http://dyn.politico.com/printstory.cfm?uuid=1ECC7CEE-18FE-70B2-A8F3B8F613F995E9.
Liles S (2008), Or Crumbling Infrastructure: How the Aging of America's Infrastructure is a Homeland Security Concern. *Selil,* 29 July, Available at: http://selil.com/?p=260.
MacDougall R (2006) The Wire Devils: Pulp Thrillers, the Telephone, and Action At a Distance in the Wiring of a Nation. *American Quarterly* 58: 715-741.
Makinen G (2002) *The Economic Effects of 9/11: A Retrospective Assessment.* Washington, D.C.: Congressional Research Service.
Markoff J, Shanker T, (2009) Panel Advises Clarifying U.S. Plans on Cyberwar. *New York Times,* 30 April, Available at: http://www.nytimes.com/2009/04/30/science/30cyber.html?_r=1.
Marx L (1994) The Idea of 'Technology' and Postmodern Pessimism. In Smith MR, Marx L (eds) *Does Technology Drive History? The Dilemma of Technological Determinism.* Cambridge: MIT Press, 237-258.
Marx L (1997) Technology: The Emergence of a Dangerous Concept. *Social Research* 64(3): 965-988.
McCafferty D, (2004) Dark Lessons: Learning From the Blackout of August '03. *Homeland Security Today,* 1 August, Available at: http://www.hstoday.us/content/view/1177/60/.
McConnell M, (2010) Mike Mcconnell on How to Win the Cyber-War We'Re Losing. *Washington Post,* 28 February, p. B01.

McCullagh D, (2010a) Senators Propose Granting President Emergency Internet Power. *CNET news,* 10 June, Available at: http://news.cnet.com/8301-13578_3-20007418-38.html.

McCullagh D, (2010b) Wikileaks Draws Criticism, Censorship Threats. *CNEt News,* 2 August, Available at: http://news.cnet.com/8301-31921_3-20012430-281.html.

Meyer D (2010), Cyberwar Could be Worse Than a Tsunami. *ZDNet,* 3 September, Available at: http://www.zdnet.com/news/cyberwar-could-be-worse-than-a-tsunami/462576.

Mills E, (2010) Symantec: Stuxnet Clues Point to Uranium Enrichment Target. *CNET News,* 15 November, Available at: http://news.cnet.com/8301-27080_3-20022845-245.html.

Minkel JR, (2008) The 2003 Northeast Blackout--Five Years Later. *Scientific American,* 13 August, Available at: http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

Mullen ADMM (2009) Strategic Communication: Getting Back to Basics. *Joint Forces Quarterly* 55(4): 2-4.

Nakashima E, (2010) Dismantling of Saudi-Cia Web Site Illustrates Need for Clearer Cyberwar Policies. *Washington Post,* 19 March, Available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464_pf.html.

Nichol J (2008) *Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests.* Washington, D.C.: Congressional Research Service.

Nye DE (2010) *When the Lights Went Out: A History of Blackouts in America.* Cambridge, MA: MIT Press.

Ottis R, (2010) The Vulnerability of the Information Society. *futureGOV Asia Pacific,* August-September, p. 70.

Owens WA, Dam KW, Lin HS (2009) *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, D.C.: National Academies Press.

Patterson T, (2010a) U.S. Electricity Blackouts Skyrocketing. *CNN.com,* 15 October, Available at: http://www.cnn.com/2010/TECH/innovation/08/09/smart.grid/index.html?hpt=Sbin.

Patterson T, (2010b) The Pentagon's Latest Cyber War Games, Told From the Inside. *Federal Computer Week,* Available at: http://fcw.com/Articles/2010/10/12/Inside-Pentagon-cyber-war-game.aspx.

Poulsen K (2007), 'Cyberwar' and Estonia's Panic Attack. *Threat Level,* 22 August, Available at: http://www.wired.com/threatlevel/2007/08/cyber-war-and-e.

Quarantelli EL (2008) Conventional Beliefs and Counterintuitive Realities. *Social Research: An International Quarterly* 75(3): 873-904.

Ranum M (2009) The Problem With Cyberwar. Presentation to DojoSec Monthly Briefings. March.

Rockefeller J, Snowe O, (2010) Now is the Time to Prepare for Cyberwar. *Wall Street Journal,* 2 April, Available at: http://online.wsj.com/article/SB10001424052702303960604575157703702712526.html.

Romjue JL (1984) The Evolution of the Airland Battle Concept. *Air University Review* May-June.

Rotella S, (2009) Howard Schmidt Naned Cyber-Security Czar. *Los Angeles Times,* 23 December, Available at: http://articles.latimes.com/2009/dec/23/nation/la-na-cyber-czar23-2009dec23.

Schmidt HA (2010), The National Strategy for Trusted Identities in Cyberspace. *The White House Blog,* 25 June, Available at: http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace#.

Shane S, Lehren AW, (2010) Leaked Cables Offer Raw Look At U.S. Diplomacy. *New York Times*, 28 November, Available at: http://www.nytimes.com/2010/11/29/world/29cables.html?_r=4.

Sherman WC (1926) *Air Warfare.* New York: The Ronald Press Company.

Simon L (2004) *Dark Light: Electricity and Anxiety From the Telegraph to the X-Ray.* Orlando: Harcourt.

Singel R (2009), Is the Hacking Threat to National Security Overblown? *Threat Level,* 3 June, Available at: http://www.wired.com/threatlevel/2009/06/cyberthreat.

Stiennon R (2009), Scenarios Are Silly Syllogisms. *ThreatChaos,* 19 October, Available at: http://threatchaos.com/2009/10/scenarios-are-silly-syllogisms/.

Stohl M (2007) Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point Or Patriot Games? *Crime, Law and Social Change* X(X): XX-XX.

Storr V, Haeffele-Balch S, (2010) Can Decentralized Bottom-Up Post-Disaster Recovery Be Effective? Working Paper, Mercatus Center at George Mason University, 5 April, Available at: http://mercatus.org/publication/can-decentralized-bottom-post-disaster-recovery-be-effective.

Thiessen MA, (2010) Wikileaks Must be Stopped. *Washington Post,* 3 August, Available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080202627_pf.html.

Walt SM (2010), Is the Cyber Threat Overblown? *Foreign Policy,* 30 March, Available at: http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.

Weimann G (2005) Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism* 28(2): 129-149.

Weimann G (2008) Cyber-Terrorism: Are We Barking At the Wrong Tree? *Harvard Asia Pacific Review* 9(2): 41-46.

Whitton C, (2010) Why Do We Keep Ignoring the Wikileaks Threat? *FOXNews.com,* 25 October, Available at: http://www.foxnews.com/opinion/2010/10/25/christian-whiton-wiki-leaks-ignore-threat-obama-democrats-congress-iraq-war/.

Winner L (1977) *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought.* Cambridge, MA: MIT Press.

Yuill C (2004) Emotions After Dark: A Sociological Impression of the 2003 New York Blackout. *Sociological Research Online* 9(3): http://www.socresonline.org.uk/9/3/yuill.html.

Zetter K, (2009) Lawmaker Wants 'Show of Force' Against North Korea for Website Attacks. *Wired Threat Level,* 10 July, Available at: http://www.wired.com/threatlevel/2009/07/show-of-force/.