DRAFT

Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016

Sean Lawson, Ph.D. | Associate Professor | Department of Communication | University of Utah
Michael K. Middleton, Ph.D. | Assistant Professor | Department of Communication | University of Utah

Presented at "Legal and Policy Dimensions of Cybersecurity," George Washington University, Washington, DC, September 27-29, 2016.

Introduction

For twenty-five years, Americans have been warned that the United States faces an imminent "cyber Pearl Harbor." Such a scenario is depicted as involving cyber attacks against critical infrastructure leading to mass destruction and disruption, followed by social and economic chaos. To date, however, no such attacks have transpired. It is perhaps unsurprising, therefore, that such scenarios have come under increased scrutiny over the last year. For example, some prominent intelligence officials have rejected the use of "cyber Armageddon" or "cyber Pearl Harbor" descriptions of cyber threats facing the United States (Clapper 2015; Bussey 2016). Nonetheless, one former defense official, John Hamre, has gone on record claiming (incorrectly) to have been the first person to use "electronic Pearl Harbor" publicly, worrying that it may have "backfired" in terms of motivating a response to cyber threats because it was the wrong analogy in 1991. However, in the same article, Hamre was quick to assert that it really is the correct analogy for the cyber threats we face now (Hamre 2015). Finally, at NATO's 2016 International Conference on Cyber Conflict, the Atlantic Council's Jason Healey sided with those intelligence officials mentioned above when he argued that the persistence of this analogy is an indicator that we have failed to understand the true nature of national security threats and capabilities in cyberspace.[1]

Together, these developments raise a number of important questions. Where does the "cyber Pearl Harbor" analogy come from? What is such an attack supposed to entail? How has the analogy evolved during its twenty-five years of use by cyber security stakeholders? And, is it possible that use of this analogy can have negative implications for cyber security policy making?

Addressing these questions is important because our perceptions of threats and vulnerabilities, fear of an uncertain future, and imagined scenarios all help to shape the cyber security policies that we adopt. "Cyber Pearl Harbor" is one of the most prominent analogies used to frame our understanding of cyber security threats, vulnerabilities, and possible futures in the United States (Stevens 2015: 131; Wirtz 2014: 7; Singer 2015: 37). It is exemplary of a history of debate about cyber security policy and governance prone to the use of hyperbole and appeals to fear. As such, the emergence, use, and spread of this analogy warrant further investigation.

[1] Jason Healey, quoted in "CyCon 2017 to Focus on 'Defending the Core," 3 June 2016, https://ccdcoe.org/cycon/content/cycon-2017-focus-defending-core.html.

This paper reports on the findings of a project that deploys a combination of content analysis and rhetorical analysis to examine the use of the “cyber Pearl Harbor” analogy in major U.S. newspapers, government documents, and policy maker speeches over the last twenty-five years. The results demonstrate that concern with the possibility of a “cyber Pearl Harbor” scenario have remained constant, despite a distinct lack of cyber attacks rising to the level of those contemplated in such a scenario. Overwhelmingly, our results indicate that it is government officials who promote fear of “cyber Pearl Harbor” in public policy debates. However, they do so with a great deal of help from news media, which regularly reports such warnings uncritically, without questioning the scenario’s purported likelihood or impacts. This is despite the fact that the supposed sources and targets of such an attack often remain uncertain or ambiguous. That is, those who deploy this analogy are often unclear about which adversary or adversaries (e.g. state or non-state actors) are most likely to carry out such an attack and just what it is they are most likely to target (e.g. civilian or military assets). In short, the “cyber Pearl Harbor” analogy functions primarily to maintain fear of an ever-impending doom scenario from an uncertain adversary, and the social and economic chaos depicted in these scenarios serve to raise doubt about society’s ability to respond. Thus, we argue that we must rethink the way we frame and communicate our understandings of cyber threats and vulnerabilities if we are to make progress in cyber security policy and governance.

Cyber Pearl Harbor and the Reality of Cyber Conflict

Perhaps the most concise definition of what a “cyber Pearl Harbor” might entail can be found in a 1999 article by *New York Times* reporter, John Markoff, who wrote, "The specter of simultaneous computer network attacks against banking, transportation, commerce and utility targets--as well as against the military--conjures up the fear of an electronic Pearl Harbor in which the nation is paralyzed without a single bullet ever being fired” (Markoff 1999). Markoff was by no means the first to use the Pearl Harbor analogy to describe the potential impacts of large-scale cyber attacks. Computer security entrepreneur Winn Schwartau, in an op-ed for *Computerworld* magazine, first used the analogy in 1991 and then again in his testimony before Congress that same year about the nature of cyber threats facing the United States. Schwartau described the impacts of an “electronic Pearl Harbor” as “truly crippling,” “devastating,” and “inflicting massive damage” on a scale that would undermine “the continuation of well-ordered society” and the ability for “society [to] function as we know it” (Schwartau, 1991).

For the last twenty-five years, this has been the dominant vision of what such a scenario would entail. One of the most influential recent examples comes from former Defense Secretary Leon Panetta who, in his June 2011 confirmation hearing, warned Congress, “I've often said that there's a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems. This is a real possibility in today's world” (Senate Armed Services Committee 2011). The following year, Secretary Panetta expounded further on the potential impacts of a “cyber Pearl Harbor,” which he said “could be as destructive as the terrorist attack

of 9/11," "cause panic, destruction, and even the loss of life," "paralyze and shock the nation, and create a profound new sense of vulnerability" (Panetta 2012).

The use of the Pearl Harbor analogy to raise fear of, and motivate a response to, impending catastrophic cyber attacks is exemplary of broader doom rhetoric that is common in U.S. public policy debates about cyber security. Scholars have noted the widespread use of "cyber-doom," "shut down the power grid," and "worst-case" scenarios by the full range of participants in these debates (Debrix, 2001; Weimann, 2005; 2008; Stohl, 2007; Conway, 2008; Dunn Cavelty, 2008, p. 2; Lawson, 2013a; Valeriano & Maness, 2015). In particular, "cyber Pearl Harbor" is exemplary of the tendency to deploy hypothetical scenarios, but also to appropriate the fear and anxiety elicited by non-cyber events such as natural disasters, conventional military attacks, or terrorist attacks to promote fear of cyber-doom (Hasian et. al. 2015, 136-146).

The use of hypotheticals and appropriated fears abounds in U.S. cyber security discourse. In the wake of the first Word Trade Center bombing in 1993, the influential futurist and theorist of the Information Age, Alvin Toffler, warned that next time terrorists could cyber attack the World Trade Centre and crash the US economy (Elias, 1994). In 1999, Fox News ran a documentary, *Dangers on the Internet Highway: Cyberterror*, warning of the possibility of catastrophic cyber attacks (Debrix, 2001; Conway, 2008). Eleven years later, CNN ran a televised war game called *Cyber.Shockwave*, which contemplated the implications of a massive cyber attack. That same year, Richard Clarke and Robert Knake included in their book, *Cyber War*, a tale of cyber attack crippling all US critical infrastructure and killing thousands in only a matter of minutes (Clarke & Knake, 2010). Others have speculated that cyber attacks could be as devastating as the 9/11 terrorist attacks (Martinez, 2012), the 2004 Indian Ocean tsunami (The Atlantic, 2010), Superstorm Sandy (Meyer, 2010), or the Fukushima nuclear disaster (Rothkopf, 2011). One former policy maker even warned that cyber attacks could pose a threat to global civilization (Adhikari, 2009).

On the other hand, some influential voices in the U.S. cyber security debate have rejected these framings of cyber threats facing the United States. In doing so, they join scores of academics, journalists, policy makers, industry experts, and others who have criticized the use of hyperbolic rhetoric and doom scenarios in the debate over cyber threats. Many of those critics agree with Hamre that the use of such rhetoric can backfire and be counterproductive for motivating appropriate responses to the cyber threats we actually face (Debrix 2001; Weimann 2005; 2008; Stohl 2007; Conway 2008; Dunn Cavelty 2008: 2; Lawson 2013; Valeriano & Maness 2015: 1, 196; Lewis 2010; Dunn Cavelty & Van Der Vlugt 2015). Nonetheless, policy maker's reliance on cyber-doom rhetoric, "cyber Pearl Harbor," and associated analogies and metaphors (e.g. "cyber 9/11") persists. In a February 2015 speech on cyber security, President Barack Obama urged listeners "to imagine" cyber attacks that "plunge cities into darkness" (Obama, 2015). In August 2015, Senator Susan Collins (R-ME) effectively urged the passage of the Cybersecurity Information Sharing Act of 2015 by insisting it was necessary "to reduce the likelihood of a cyber 9/11" (Collins, 2015; Pagliery, 2015). Finally, veteran journalist and television news personality Ted Koppel made headlines with his October 2015 book warning of the possibility of catastrophic cyber attacks on the power grid (Koppel, 2015).

Thus, despite some critics, the cyber Pearl Harbor analogy has become a consistent and sedimented trope in cyber security discourse and in the logics that inform efforts to develop cyber security policy. But, if critics and users of the cyber Pearl Harbor analogy and doom scenarios are correct that such rhetoric is potentially counterproductive--a point which we will argue below is correct--then we need to understand better the origins and emergence of the ever-imminent "cyber Pearl Harbor." This includes investigating who has used and perpetuated this analogy, what such an event is said to entail in terms of impacts and necessary responses, for what reasons, and with what evidence. As we suggest below, doing so both reveals the contours of the discursive terrain shaped by the use of the cyber Pearl Harbor scenario and, potentially, illustrates ways that our framing of cyber security threats could have been otherwise.

Sources and Methods

This study employs a combination of rhetorical analysis of key texts that have deployed the cyber Pearl Harbor analogy over the past 25 years with a quantitative content analysis of U.S. newspaper articles in which the analogy appears during the same time period. In each case, analysis was informed by theoretical insights from the critical constructivist tradition of scholarship in security studies (Peoples & Vaughan-Williams 2010), including other scholarship that has explored the role of language and rhetoric in U.S. cyber security discourse (Bendrath 2001, 2003, 2007; Dunn Cavelty 2008; Eriksson 2002; Hansen & Nissenbaum 2009; Lawson 2012; Betz & Stevens 2013).

Much of this work has been informed by securitization theory, which posits that it is not predetermined which security threats will make it onto the political agenda. Instead, security threats are said to be "constructed" because the process of identifying, understanding, and responding to them is the result of political discourse. That process involves a "securitizing actor" (usually a political leader or decision maker) identifying "threat subjects" (the source of the threat), "referent objects" (that which is threatened), and the prospective impacts of a threat (Buzan et. al. 1998). Additionally, Dunn Cavelty notes that in the case of cyber securitization, specific and sometimes dramatic events or conditions often serve to focus securitizing actors' attention on cyber security matters (Dunn Cavelty 2008).

Critical security scholars have been particularly interested in the construction of cyber threats because they have been seen as exemplary of concern with myriad so-called "new threats" in the post-Cold War period (Wall 2008: 866; Dunn Cavelty, 2008: 5; Füredi 2009: 25-26). These have included a host of seemingly ambiguous, uncertain, but dangerous threats related to environmental degradation, poverty, health, immigration, and technology (Füredi, 2009: 25-26; Bigo 2000, 2006; Buzan et al. 1998; Hardt and Negri 2004). Cyber threat perceptions have mirrored the ambiguity and uncertainty found in perceptions of other "new threats." Though cyber security concerns arose as far back as the 1970s, dominant perceptions of the potential threats have shifted over time. Cyber security proponents have found it difficult to identify and then communicate clearly and precisely what it is that is threatened, by whom, and with what potential impacts, in and through cyberspace. As threat perceptions have shifted, so have

claims about the primary subjects (e.g. foreign spies, criminals, terrorists, insiders), objects (e.g. business data, state secrets, critical infrastructure), and impacts (e.g. monetary loss, diminished competitiveness, catastrophe) of those threats (Dunn Cavelty 2008; Bendrath 2001, 2003, 2007).

To place the use of the cyber Pearl Harbor analogy and metaphor into this larger context of a shifting U.S. cyber security discourse, we used a combination of rhetorical and content analysis to examine a number of "key texts" and U.S. newspaper articles. We identified ten key texts that we examined through close reading and rhetorical analysis (See the list of texts in Appendix C). These texts were chosen because they were exemplary of the use of the cyber Pearl Harbor analogy by critical stakeholders, including industry experts, government officials, large media outlets, or others with the ability to shape and influence U.S. cyber security discourse. The kinds of texts chosen included op-eds, Congressional testimony, speeches, a documentary, and an internal government document. Finally, to collect examples of the cyber Pearl Harbor analogy in U.S. news media, we searched the "U.S. Newspapers" category in LexisNexis Academic Universe using the search string *"electronic pearl harbor" OR "digital pearl harbor" OR "cyber pearl harbor."*[2] This produced 214 results. After removal of duplicates and irrelevant results (e.g. letters to the editor), the final coded set included 203 articles.

On the one hand, rhetorical analysis provides a means both to develop fine-grained insights into particular texts and to understand how those texts are deployed to accomplish strategic outcomes within the context of cyber security debates. On the other hand, content analysis of a broad collection of texts, like those we examine in this study, both helps scholars identify how cyber security discourse circulates (and evolves) among broader communities of stakeholders, as well as how those circulating discourses both enable and constrain the rhetorical interventions observed in texts created by key figures in the cyber security debate. As a consequence, it is worthwhile to briefly develop the assumptions and contributions each of these methodological approaches offer to our study.

Rhetorical Analysis

Rhetorical analysis provides a tool for explaining "the relationship of persons and ideas within a situation" (Brockriede 1974: 166). To arrive at these explanations, rhetoricians cast their net broadly, asking how "written as well as spoken discourse, nonverbal [e.g., images] as well as verbal symbols, movements as well as individual events, and functions other than those implied by a narrow conception of persuasion" and overtly persuasive texts provide a lens through which to understand how ideas and their relationship to both their producers and audiences are shaped and defined (Brockriede 1974). Put differently, rhetoricians focus their critical attention on "apparently finished discourse[s] that present [themselves] as transparent," including, in this instance, discourses that shape our understanding of cyber Pearl Harbor, and seek to demystify how those discourses are constructed (McGee 1990: 279; McKerrow 1989). Drawing together fragments of discourse (congressional testimony, key speeches, documentaries, and other texts

[2] The search was conducted and articles collected on February 15, 2016.

broadly conceived) can, rhetorical analysis argues, help reveal how particular meanings and relationships to ideas become sedimented, as well as how competing interpretations become marginalized. Concretely, rhetorical analysis asks how the range of participants in debates over cyber security shape a particular understanding of and relationship to that threat. At the same time, rhetorical analysis reveals that these meanings are contingent, that it could be otherwise, by exposing how alternative understandings of cyber Pearl Harbor are minimized across texts and through media representations.

In this study, rhetorical analysis drives our engagement with key texts that have shaped and have been shaped by twenty-five years of cyber Pearl Harbor discourse constructed by policy makers, industry experts, commentators, and the media. These include congressional testimony by military and cabinet-level officials, declassified military documents, speeches by government officials, and a documentary (See the list of texts in Appendix C). Rhetorical analysis' focus on textual features (metaphor, analogy, etc.) and argumentative strategies provides a means to deconstruct these texts, identifying how cyber Pearl Harbor comes to be defined and operationalized in political debates over its importance. In this regard, rhetorical analysis provides a technique for identifying an "unfolding sequence of arguments, ideas, and figures which interact through the text and gradually build a structure of meaning" (Leff 1990: 256). For example, rhetorical analysis helps identify how threat subjects, referent objects, and focusing events that constitute cyber Pearl Harbor are discursively constructed through these key texts. However, beyond helping illuminate how these texts function to define cyber Pearl Harbor as a real and viable threat, a rhetorically-driven close reading also helps inform our analysis of 25 years of media discourse about cyber Pearl Harbor because "the close reading of specific texts often provides both data and methods for comprehending larger discursive formations," which constitutes the focus of our content analysis of major U.S. newspapers (Leff 1990: 257).

Content Analysis

Content analysis complements a rhetorical analysis focused on key texts that participated in and constructed the cyber Pearl Harbor analogy in two ways. First, whereas rhetorical analysis focuses on a small number of key texts to identify the specific, and often complex, rhetorical strategies through which the cyber Pearl Harbor analogy is crafted and reinforced by key stakeholders, content analysis provides a means to identify and draw inferences about how those texts circulate in media discourse and to broader audiences, as well as how that circulation reinforces and shapes key texts over the span of time that our study examines (1991-2016). Second, content analysis complements the interpretive and qualitative conclusions of rhetorical analysis with systematic and more objective accounts of how the cyber Pearl Harbor analogy has evolved over twenty-five years of use in cyber security discourse.

While content analysis operates as a method across a variety of disciplines and includes many variations, its essential characteristic is that it offers a methodology for "a summarizing, quantitative analysis of messages that relies on the scientific method, including attention to objectivity, a priori design, reliability, validity, generalizability, and replicability" (Neuendorf 2011: 277; Krippendorff 2004). Because content analysis provides a tool for analyzing an expansive

corpus of messages, it has been widely used to describe political communication and informed germinal scholarship in the agenda-setting research that explored the interaction between media discourse and the discourse of policy makers about topics of critical public concern (Benoit 2011: 268).

By quantifying dimensions of content in specific texts and across a large body of texts, content analysis offers an ability to "'mak[e] inferences by objectively and systematically identifying specified characteristics of messages" (Benoit 2011: 268; Krippendorff 2004). When practicing content analysis, the dimensions of texts that are quantified can be identified and defined inductively or deductively (Benoit 2011: 271). In the case of the former, researchers derive variables to be quantified by developing familiarity with a body of texts to the extent that a set of exhaustive, mutually exclusive categories emerge. Deductive variables, on the other hand, are derived from a theoretical framework that informs the content analysis and which are relevant to the texts under examination based on related scholarship (Neuendorf 2011: 277).

For example, in the present study, coding categories were informed by the main concepts of securitization theory, including securitizing actor and referent object, as well as the sentiment of the article and the focusing events or conditions identified as reason for taking such a threat seriously (See Appendix A). When coding sentiment, we sought to identify whether each article included an articulation of the threat that was positive (suggested that cyber Pearl Harbor was a real and viable threat), negative (dismissed the viability of a cyber Pearl Harbor), or neutral (equivocated or took no firm position on the possibility of cyber Pearl Harbor). When coding securitizing actor, we bifurcated this concept into official (governmental) actors and private (academia, industry, media) actors. Similarly, threat subject was bifurcated between State and non-State actors. In both instances, we further refined these codes with sub-categories, including specific state threat subjects (e.g., Russia, China, etc.) and securitizing actors (e.g., bureaucrats, elected officials, military officers, professors, journalists, etc.). We operationalized referent object by utilizing three foci of cyber attack: civilian critical infrastructure, military infrastructure and assets, and informational assets. Finally, focusing events were bifurcated into cyber and non-cyber events that provided the impetus for a discussion of cyber Pearl Harbor, and were sub-divided into actualized events and imagined events. For each category, we collaboratively coded random samples from our overall pool of articles until intercoder reliability was established (See Appendix B for a table of intercoder reliability scores calculated using Krippendorff's alpha). Once we achieved an acceptable level of reliability, we divided and independently coded the remainder of the articles. While this practice of quantification of the content of texts can offer a variety of measurement possibilities, most content analysis, like the present study, relies on frequency data to support its inferences about texts, the circumstances of their emergence, and the contexts and consequence of their circulation and/or reception (Benoit 2011: 271).

By combining these two methodological approaches, we are able to make complementary claims about the development of the cyber Pearl Harbor analogy within cyber security discourses. On the one hand, rhetorical analysis offers a "close-up" view of specific exemplars, or key texts, crafted by primary stakeholders in the evolution of cyber security policy and

political discourse. By examining these texts closely, we are able, as argued by rhetorical scholars, to identify how structures of meaning are gradually built (Leff 1990; Darsey 1994). On the other hand, the "satellite view" offered by content analysis of a broad swath of texts across a period of time enables us to identify variations in the intensity of discussion of cyber security via the cyber Pearl Harbor analogy, as well as who is participating in that discourse, based on what concerns, and with what aims (Hart 1990; Hoffman & Waisanen 2015). By working between these two levels of abstraction and critical insight, our approach to the use of the cyber Pearl Harbor analogy allows us to make inferences about how these two sources of discourse on the subject influence one another, how they are impacted by contextual factors, e.g., terror attacks, cyber security breaches, etc., and how certain dimensions of the cyber Pearl Harbor analogy are strategically given greater presence (or marginalized) to shape broader cyber security discussions toward specific outcomes.

The Emergence and Evolution of Cyber Pearl Harbor

As mentioned above, there has been confusion over the origins of the Pearl Harbor analogy in U.S. cyber security discourse. In December 2015, former defense official, John Hamre, claimed to have been the first person to use the term publicly in his November 1997 testimony before Congress. He further claimed that General Tom Marsh had been "the author of that phrase" as a result of having led the President's Commission on Critical Infrastructure Protection, the final report from which was published in 1997 (Hamre 2015). Others have claimed that president of the RSA computer security company, D. James Bidzos, was the first to use the term in 1991. However, as Tim Stevens notes, the weight of the available evidence supports the contention that it was the computer security entrepreneur and novelist, Winn Schwartau, who first used the term "electronic Pearl Harbor" in 1991 in an op-ed, Congressional testimony, and a self-published novel (Stevens 2015: 131).

Regardless of its likely emergence in the early 1990s from computer security industry experts, the Pearl Harbor analogy did not become widespread until the mid to late 1990s when it was mentioned in a string of Congressional testimonies by government officials, most notably Director of the C.I.A. John Deutch in 1996 and Deputy Secretary of Defense John Hamre in 1997 and 1998. A close reading of these early sources of cyber Pearl Harbor from the 1990s demonstrates that the seeds of the currently dominant use of that analogy and related themes emerged very early in the discourse. However, it also reveals the existence of subtle differences in early meanings of cyber Pearl Harbor, which were in turn associated in some cases with differing views of how one should respond to such a threat.

In June 1996, Senator Sam Nunn (D-GA) opened a hearing of the Senate Governmental Affairs Committee on cyber threats by informing listeners and participants that the proceeding would

> "focus on the possibility that cyber-attacks on our national infrastructure could be used as a part of a coordinated strategic attack on the United States. How likely is such a scenario? Who has the capacity to launch such an attack? How do we defend against

> such an attack? Perhaps most important, would we even recognize the fact that such an attack was being carried and be able to determine who was behind the attack in a very timely manner?" (Deutch 1996)

That is, the hearing would focus on the primary issues of concern for the construction of any threat narrative, including the identification of potential threat subjects and referent objects: Who might attack? What might they target? The answer to the referent object question was already assumed: "national infrastructure." But, just which infrastructure would be targeted was less certain. What is more, Sen. Nunn raised questions related to evidence and uncertainty, as well as possible responses. How do we know, in the realm of cyber threats, where the real concerns exist and, in the end, what do we do? Beyond the hearing that day, all of the key texts that address the possibility of cyber Pearl Harbor provide answers to most of these questions.

Where threat subjects are concerned, the key texts that we analyzed from the 1990s and early 2000s were focused almost exclusively on non-state actors. Of course, Schwartau's piece was titled "Fighting Terminal Terrorism" and contemplated that "a motivated individual or organization" could carry out "an electronic Pearl Harbor" (Schwartau 1991). In his 1996 testimony, DCI Deutch and his questioner, Sen. Sam Nunn, both worried about the possibility that not just states, but also "sub-national groups" and "terrorist groups" could obtain the capability to carry out cyber attacks against the United States' vulnerable networks. DCI Deutch also mentioned the potential, but uncertain, threat from "individual criminal elements or individual hacker activities" (Deutch 1996). Finally, the 2003 PBS Frontline documentary, *Cyber War!*, which included interviews with prominent cyber security experts, focused entirely on non-state cyber threats, particularly the threat of from terrorists (Kirk 2003).

Though they continue to mention possible non-state attackers, we see an increased concern with state actors over time in the later texts that we analyzed. Gen. Alexander's 2012 memo about preventing a cyber Pearl Harbor mentions non-state actors, but is primarily focused on "nation states" (Alexander 2012). Similarly, Secretary Panetta's 2012 speech noted the threats from cyber criminals, but said "the even greater danger facing us in cyberspace goes beyond crime and harassment. A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11" (Panetta 2012). Finally, Hamre's December 2015 op-ed warned, "Hostile intelligence and military establishments are prepared to wage war now, using cyber tools" (Hamre 2015).

In both cases, however, specific actors are rarely mentioned, with a few exceptions. In the non-state category, al-Qa'ida is sometimes identified as a potential attacker in the wake of the September 11, 2001 terrorist attacks (Kirk 2003). Later, when officials like Secretary Panetta begin to focus more on the threat from state actors, we see occasional mentions of China, Russia, and Iran as potential perpetrators of a cyber Pearl Harbor attack (Alexander 2012; Panetta 2012). However, the texts we analyzed far more often identified generic, unspecified state or non-state actors (or both) as the would-be authors of a cyber Pearl Harbor (Schwartau 1991; Deutch 1996; Hamre 1997, 1998; Panetta 2011). In short, those officials and experts

raising the alarm about the threat of a cyber Pearl Harbor were often unclear about exactly who might carry out such an attack.

Far from being a rhetorical weakness, this inability or unwillingness to identify specific threat subjects may serve to heighten fear of a possible cyber Pearl Harbor. One might expect that inability or unwillingness to specify who is willing and able to carry out such an attack would weaken the case that such a threat is indeed real. Instead, the so-called “attribution problem”--the idea that one could be cyber attacked without knowing who had carried out the attack--emerged as a consistent theme in the cyber Pearl Harbor discourse that only seemed to heighten the fear. This possibility was first raised by Schwartau, who cautioned that “such an attack can also be launched...with little or no ability to identify...the perpetrators” and that “the source of the attack is completely disguised” (Schwartau 1991). In 1996, the difficulty in determining the source of cyber attack was a concern raised multiple times in Sen. Nunn’s questioning of DCI Deutch (Deutch 1996). In his 1997 testimony, John Hamre noted, “Our knowledge of the origin of such attacks, and their sponsorship, is likely to be imprecise” (Hamre 1997). The 2003 PBS documentary used the examples of the Slammer, Code Red, and Nimda malware attacks as evidence of the danger of the attribution problem (Kirk 2003). By 2012, however, Secretary Panetta was warning would-be cyber attackers that the U.S. had “made made significant investments in forensics to address this problem of attribution, and we are seeing returns on those investments” (Panetta 2012).

The documents we analyzed were also, in the aggregate, ambiguous about which “national infrastructures” would be the target of such an attack. Civilian critical infrastructures like power, water, communications, and transportation were identified most often as likely targets for a cyber Pearl Harbor attack, followed closely by military command, control, and logistics systems. Some authors also worried that attacks against informational assets such as financial information, intellectual property, or government secrets could result in a cyber Pearl Harbor (Schwartau 1991; Alexander 2012). Most common, however, was to merely present a laundry list of potential civilian, military, and informational targets that may, if struck in some combination, result in a catastrophic and crippling cyber Pearl Harbor situation. Little distinction is made in these texts between different civilian infrastructure systems. What’s more, the line between civilian and military systems becomes blurry when some authors note the military’s reliance on civilian infrastructure systems. In the end, the effect is to leave largely unanswered the question of exactly what the target of a cyber Pearl Harbor might be.

Though they are often unclear about who or what is threatening/threatened in a would-be cyber Pearl Harbor, proponents of this threat point to various events and conditions that they believe warrant sensitizing us to, and focusing our attention on, the possibility of a cyber Pearl Harbor. First, and most obvious, is to point to actual cyber incidents as a warning of what might happen if we do not take cyber security more seriously. These include specific hacking incidents against government or private targets, reports of mass numbers of unspecified “intrusions” of networks each day, and reports of system vulnerabilities that create the possibility for cyber attack.

Second, those who warn of a coming cyber Pearl Harbor point to general, structural conditions of society and technology in the Information Age as reason for concern. In 1996, DCI Deutch mentioned twice during his testimony the dangers that come with "growing dependency" on information technology and networks (Deutch 1996). In 1997 and again in 1998, John Hamre cited "dependence" or "reliance" on networks as a source of vulnerability (Hamre 1997, 1998). In 2003, Richard Clarke told PBS flatly, "we depend upon the Internet for our national security and our national economy" (Kirk 2003). In 2011, Senators Lieberman, Collins, and Carper called the Internet "a nearly indispensable tool of modern life" (Lieberman et. al. 2011). Finally, in 2012, Gen. Alexander warned, "The U.S. as a society is extraordinarily vulnerable because we rely on highly interdependent networks" (Alexander 2012). In 1997, Hamre explained that concern about such vulnerability-inducing dependence on networked systems was due to the complexity of such systems and the possibility "that the fixes put in place to solve familiar problems may not be adequate for the more 'closely coupled' world in which we now find ourselves" (Hamre 1997).[3]

Finally, there are other, more problematic events used to focus attention on the prospect of a cyber Pearl Harbor. These include other, non-cyber events appropriated in an effort to raise fear of a potential cyber Pearl Harbor. These included a 1996 power outage (Hamre 1997, 2015), a 1998 failure of a communications satellite (Hamre 1998), and the terrorist attacks of September 11, 2001 (Kirk 2003; Panetta 2012). They also include fictional scenarios such as simulations and war games. For example, at the same hearing at which DCI Deutch testified, Senator Nunn cited in his opening comments, "an actual war game scenario presented by our witnesses from the Rand Corporation" that he believed "will hopefully provide the subcommittee and the public at large with a better appreciation for the difficult issues which must be wrestled with when it comes to information warfare" (Deutch 1996). Similarly, experts interviewed in PBS's 2003 documentary pointed to prior war games as evidence of cyber threat. The documentary itself included a segment showing military personnel participating in a cyber war game exercise (Kirk 2003). Hamre points to the importance of one war game in particular, Eligible Receiver, that served to "trigger" the "cyber worries" of many in government in the 1990s (Hamre 2015). Finally, Secretary Panetta's 2012 speech included a detailed but entirely fictional scenario meant to depict what might be possible in a cyber Pearl Harbor (Panetta 2012).

Most problematic, however, is the use of the tactic of projection (Hasian et. al. 2015: 143-144). This rhetorical tactic for focusing attention on cyber threats to the United States involves pointing to actions carried out by the United States or their direct impacts as evidence or reasons why we should be concerned about the potential for a cyber Pearl Harbor attack on the United States by foreign adversaries. There are numerous examples over the years. In 1991, to support his claims of a threat of electronic Pearl Harbor, Schwartau noted, "The U.S. government has issued contracts for studies on methods of infecting enemy military computers with viruses in hopes of shutting down battlefield computing and communications capabilities" (Schwartau 1991). Interviewees in the PBS documentary noted that the U.S. understood the threats it potentially faced from others because it had already conducted offensive cyber attacks

[3] "Closely coupled" is a term often used in complexity science to describe a characteristic of complex systems, which is that their many linkages can make them particularly vulnerable to "cascading failures."

itself (Kirk 2003). Most egregious, however, have been instances when U.S. officials have pointed to the joint U.S.-Israel Stuxnet attack on Iranian nuclear facilities, and its direct implications, as evidence of a possible cyber Pearl Harbor. We see this tactic used in Senator Lieberman, et. al.'s 2011 op-ed where Stuxnet serves as a primary piece of evidence in support of the supposed cyber Pearl Harbor threat (Lieberman, et. al. 2011). We see it again in 2012 when Secretary Panetta points to a series of Iranian cyber attacks that we now know were Iran's retaliation for Stuxnet (Panetta 2012; Kaplan 2016: 213). Even some Obama administration officials have acknowledged (at least internally) the hypocrisy of calling out others while the United States engages in attacks like Stuxnet (Kaplan 2016: 228).

Though the cyber Pearl Harbor narrative has been largely consistent over time, there were some key differences in the early period of its emergence. These sometimes-subtle differences related to the potential impacts and likelihood of such an attack, as well as to the lessons that the analogy should teach in terms of preparedness and response. We can observe such differences, for example, between Schwartau and Hamre, as well as in an interaction between Sen. Nunn and DCI Deutch.

In the first case, in Schwartau's account, "electronic Pearl Harbor" serves as a description of a possible attack and its impacts--i.e. sudden and catastrophic. There is no effective response to such an attack after the fact, he said. Therefore, our response to the possibility of such an attack should be to take action now to prevent such an attack from occurring in the first place (Schwartau 1991). Comparatively, John Hamre's 1997 and 1998 uses of the Pearl Harbor analogy are subtly but importantly different. In his testimony, Pearl Harbor does not serve as a description of what a future cyber attack might look like. Though Hamre would certainly hope to prevent such an attack, nonetheless, his use of the Pearl Harbor analogy serves instead as a lesson in the importance of preparedness to cope with and respond in the wake of a large attack, just as the United States had been able to do in the wake of the Pearl Harbor attack (Hamre 1997).

Likewise, on both occasions, 1997 and 1998, Hamre was careful not to portray a catastrophic cyber attack as imminent. "I don't think such an event is imminent," he said, adding, "I am not warning that the sky is falling. We have time to prepare" (Hamre 1997, 1998). Again in 2003, Hamre and other cyber security experts interviewed for PBS Frontline's documentary, *Cyber War!*, expressed skepticism about the likelihood of a cyber Pearl Harbor-like attack. Hamre called into question the value of such attacks for terrorist groups that are primarily interested in causing a level of shock and destruction that he believed impossible to achieve at that time with cyber attacks alone. Similarly, James Lewis of the Center for Strategic and International Studies and John Arquilla of the Naval Postgraduate School also discounted the possibility of the kind of catastrophic attack contemplated with the use of the cyber Pearl Harbor analogy (Kirk 2003).

We can observe similar differences in an interaction between Sen. Nunn and DCI Deutch during the latter's 1996 Congressional testimony. Though some news media accounts of this interaction reported that DCI Deutch had warned of a possible cyber Pearl Harbor ("Cyber

terrorists threaten US, CIA boss warns," 1996; "CIA warns of cyber-terror attacks," 1996), this is not correct. It was Sen. Nunn who raised the possibility of such an attack when he asked, Carter, A.B., Deutch, J. and Zelikow, P. (1998) "Catastrophic Terrorism: Tackling the New Danger," *Foregin Affairs,* November/December.

> "There are some who believe we are going to have to have an electronic Pearl Harbor, so to speak, before we really make this the kind of priority that many of us believe it deserves to be made. Do you think we're going to need that kind of real awakening, or are we fully alerted to this danger now, and are we allocating sufficient resources?"

In response, though he said that the United States and its allies faced serious cyber threats, Deutch downplayed the possibility of a cyber Pearl Harbor. He said,

> "I think that we are fully alerted to it now. I don't know whether we will face an electronic Pearl Harbor, but we will have, I'm sure, some very unpleasant circumstances in this area or our allies will have unpleasant circumstances in this area. So I think while we are fully alerted to it, it's not as if we're asleep on the subject, but I'm certainly prepared to predict some very, very large and uncomfortable incidents in the area. What about resources? I think resources are being allocated to this problem in its many different dimensions… So the answer to your question is I think the resource stream is moving in that regard. The priority has been given, and it's moving along, sir" (Deutch 1996).

Sen. Nunn, seemingly more concerned with such a possibility, pushed DCI Deutch on whether the United States must spend more on intelligence and adopt a strategy of cyber deterrence modeled on Cold War nuclear deterrence. DCI Deutch, less concerned with cyber Pearl Harbor, expressed his assessment that current efforts were sufficient and that deterrence was not the most appropriate model for constructing cyber strategy because it implied threats of military force in response to the vast majority of cyber threats that were really a "peacetime" problem, not a military concern (Deutch 1996).

By 2011, however, Schwartau and Nunn's uses and lessons of cyber Pearl Harbor seem to have won out at the highest levels of U.S. cyber security discourse. This is borne out in public statements by Secretary Panetta, as well as internal U.S. Cyber Command documents issued by Gen. Keith Alexander. Both adopt the cyber Pearl Harbor analogy, with Panetta describing such an attack in catastrophic terms (Panetta 2012). In terms of response, both assert the need to develop a deterrent capability, in part through the development and use of "active defense" (what some would call "offensive") capabilities (Kaplan 2016: 212). Gen. Alexander recommends in 2012 that the "DOD must be capable of stopping attacks while in progress--or before," to use NSA spying capabilities to "identify threats (exploits and attacks) before they are launched against us and enable USCYBERCOM to deploy defenses in advance of their use," to "neutralize adversary capabilities affecting DoD systems at the point of origin," and ultimately to "deter attacks in the long term" (Alexander 2012). These goals were reflected in Secretary Panetta's public statements in 2012. He reiterated, "In addition to defending the

Department's networks, we also help deter attacks" and that "we won't succeed in preventing a cyber attack through improved defenses alone. If we detect an imminent threat of attack...we need to have the option to take action to defend the nation" (Panetta 2012).

Cyber Pearl Harbor in the News

The analysis above provides an account of the emergence and evolution of cyber Pearl Harbor among elite actors like government officials and industry experts. But, as James Wirtz notes, the notion of a cyber Pearl Harbor "is reinforced by recurring media reports" (Wirtz 2014: 7). Thus, analysis of a wider data set is necessary to gain a better understanding of who is truly responsible for spreading the analogy in the wider public imagination, as well as what a cyber Pearl Harbor entails and the reasons commonly provided for taking such a threat seriously. As explained above, to address these issues, we performed a content analysis of a sample of 203 articles from U.S. newspapers spanning the period from 1991 to early 2016.

First, our results demonstrate that cyber Pearl Harbor has maintained a presence in news media reporting during the last twenty-five years, but has peaked at certain moments that correlate with the emergence of other prominent national security concerns (See Figure 1). We see a spike in concern with cyber Pearl Harbor after 1995, which then declines around 2003 and spikes again in 2011 and 2012. The first spike correlates to increased concern among U.S. officials with the possibility of mass casualty, new technology-enabled, "new terrorism." Reasons for such concerns could be found in the 1993 World Trade Center bombing, the 1995 Aum Shinrikyo nerve gas attack on the Tokyo subway system, and the 1995 Oklahoma City bombing. The possibility for cyber terrorism piggy-backed off of concerns about other, similar kinds of terrorism, e.g. bioterrorism, agricultural terrorism, etc. (Carter et. al. 1998; Hoffman 1998; Laqueur 1999; Lifton 1999). Similarly, Secretary Panetta's public statements drove much of the coverage of cyber Pearl Harbor in 2011 and 2012. In turn, we know that those were sparked, in part, by a series of retaliatory cyber attacks on the United States and its Persian Gulf allies by Iran in response to the U.S.-Israeli Stuxnet attack on Iranian nuclear facilities. That strike, in turn, came at a time of increased nuclear tensions between Iran and the West. In both cases, increased concern with cyber Pearl Harbor in the news is correlated with other, pressing (but not necessarily cyber-related) national security concerns of the day.

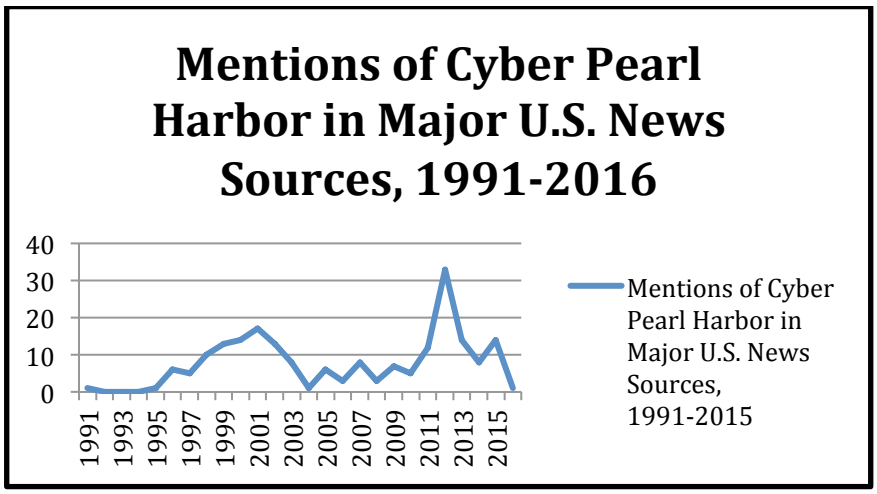
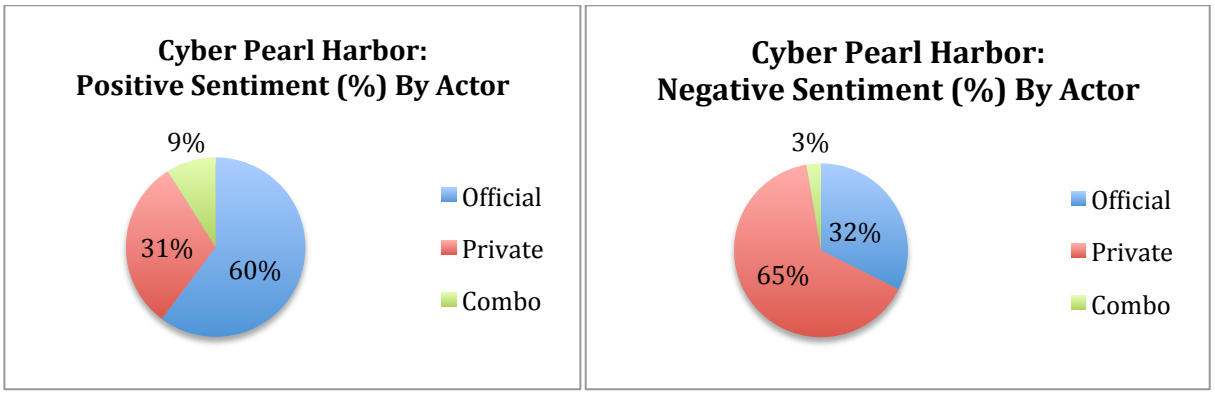


Figure 1. Mentions of Cyber Pearl Harbor in Major U.S. Newspapers.

Second, coding of news articles for (de)securitizing actor indicates that government officials are primarily responsible for spreading concern about the possibility of a cyber Pearl Harbor. Thus, in 60% of cases where cyber Pearl Harbor was depicted in the news as a realistic threat, government officials were the ones cited as promoting this idea. Conversely, in 65% of cases where cyber Pearl Harbor was portrayed as unlikely or unrealistic, private actors such as industry experts, academics, or journalists were cited (See Figures 2 & 3).



Figures 2 & 3: Positive & Negative Pearl Harbor Sentiment by Actor.

Those officials who promote concern for a possible cyber Pearl Harbor do so, however, with a great deal of help from news media. The vast majority of news stories (77%) presented only the perspective of those promoting the idea of possible cyber Pearl Harbor. On only a few occasions did news articles provide a balanced view, including perspectives skeptical of cyber Pearl Harbor alongside those promoting the idea (3%), or providing a purely negative assessment of cyber Pearl Harbor (18%; see Figure 4). Interestingly, there has been less skepticism and more positive reporting about the potential for cyber Pearl Harbor over time (See Figure 5).

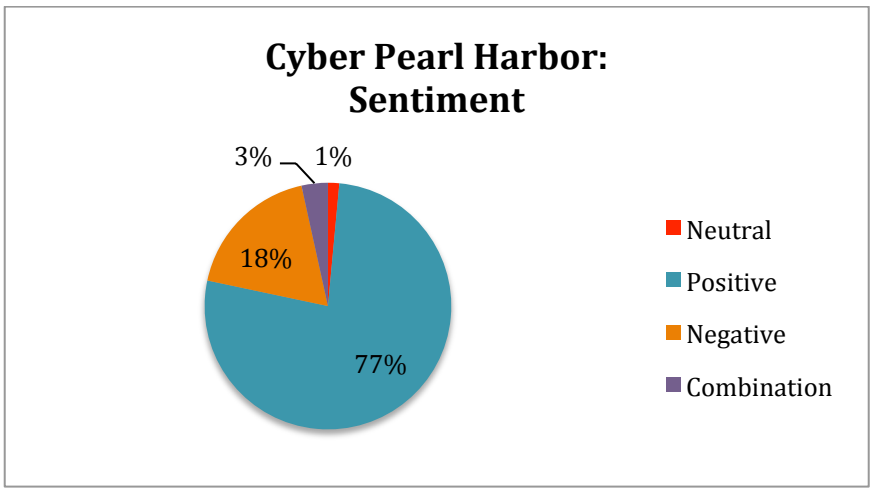


Figure 4. Cyber Pearl Harbor Sentiment in Major U.S. Newspapers.

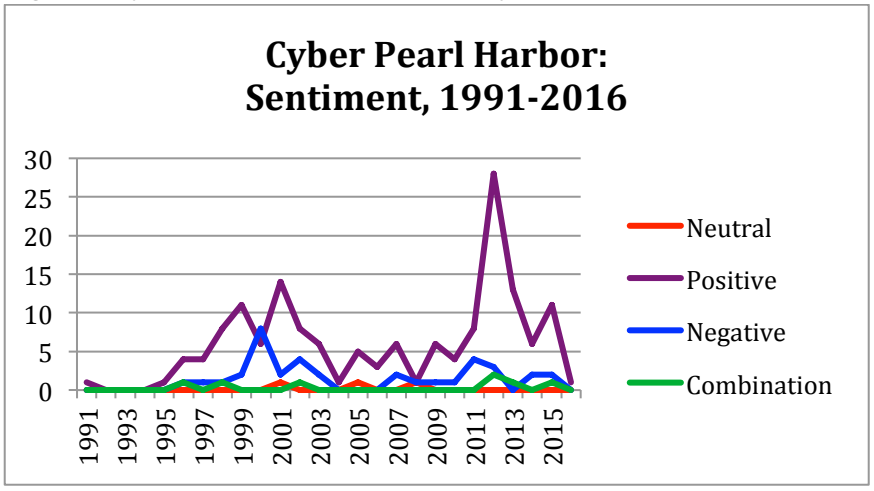


Figure 5. Cyber Pearl Harbor Sentiment Over Time.

As we might expect based on the analysis of key texts above, when cyber Pearl Harbor appears in news articles, it is largely unclear just who might carry out such an attack (See Figure 6). Overall, in 31% of articles, threat subject remains unspecified, the largest threat subject variable. Next is a laundry list combination of threat subjects at 22%. This means that in over half the articles, it remains unclear who might carry out such an attack. Where state versus non-state threats are concerned, we can see overall more concern with non-state actors. However, if we look at frequency of mentions for state versus non-state over time, we can see the increasing concern with states observed in the key texts also reflected in the news articles (See Figure 7).

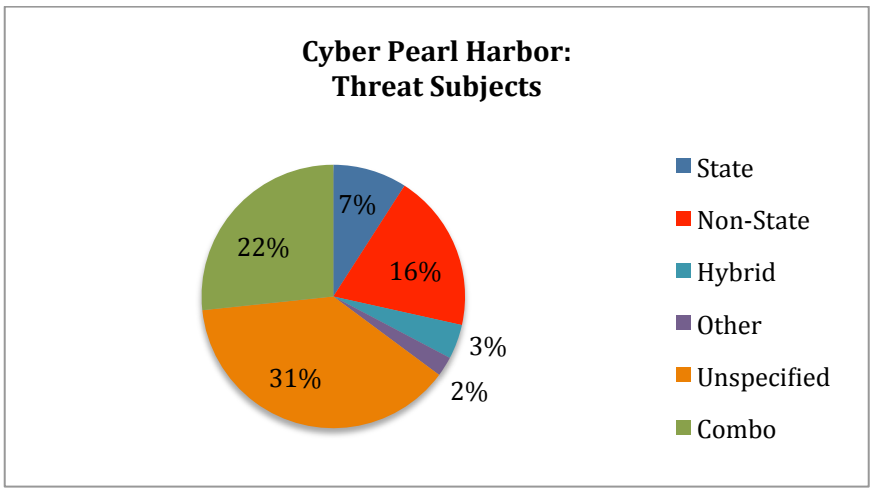


Figure 6. Cyber Pearl Harbor Threat Subjects

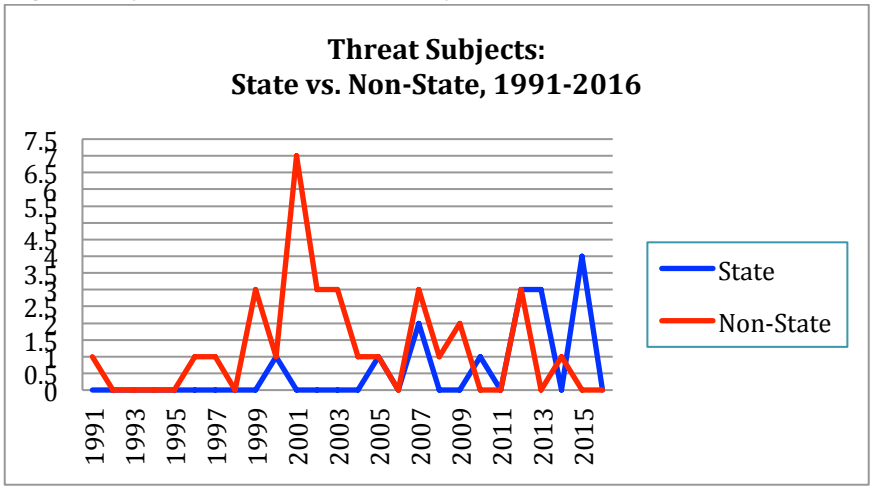


Figure 7. Cyber Pearl Harbor Threat Subjects (State vs. Non-State), 1991-2016

Likewise, analysis of key texts would indicate that civilian infrastructure is the primary referent object of concern in the cyber Pearl Harbor narrative. That is reflected in the news articles as well, where 45% identify civilian infrastructure as a likely target of such an attack. However, there are also a significant number of articles that do not specify a target for such an attack or merely provide a laundry list of potential targets (29%), which has the effect of leaving the question of referent object largely unanswered (See Figure 8).

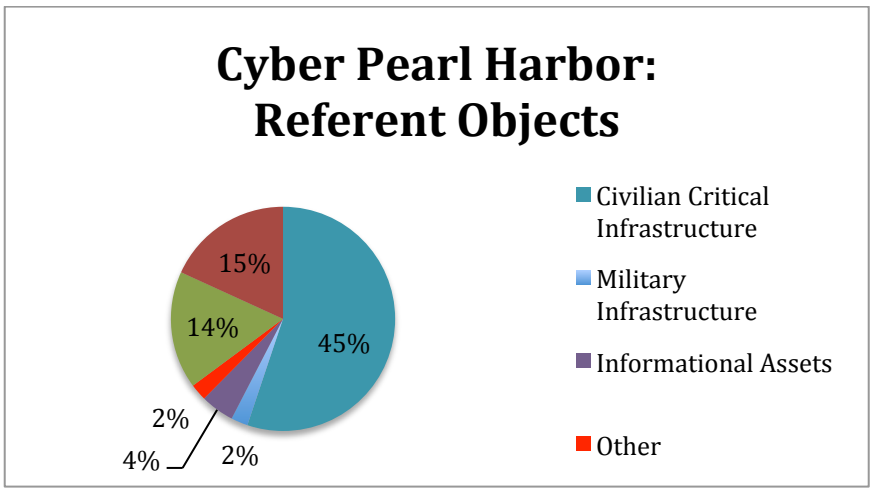


Figure 8. Cyber Pearl Harbor: Referent Objects.

Finally, similar to the key texts that we analyzed, news articles primarily point to prior cyber incidents or vulnerabilities (33%) as evidence or reason for taking the threat of cyber Pearl Harbor seriously. Fictional scenarios (12%) and reference to non-cyber events (7%) are also deployed as reason for concern about cyber Pearl Harbor. Most problematic, however, is that many news articles (19%) provide no clear reason or evidence at all in support of the idea that cyber Pearl Harbor is realistic or likely (See Figure 9).

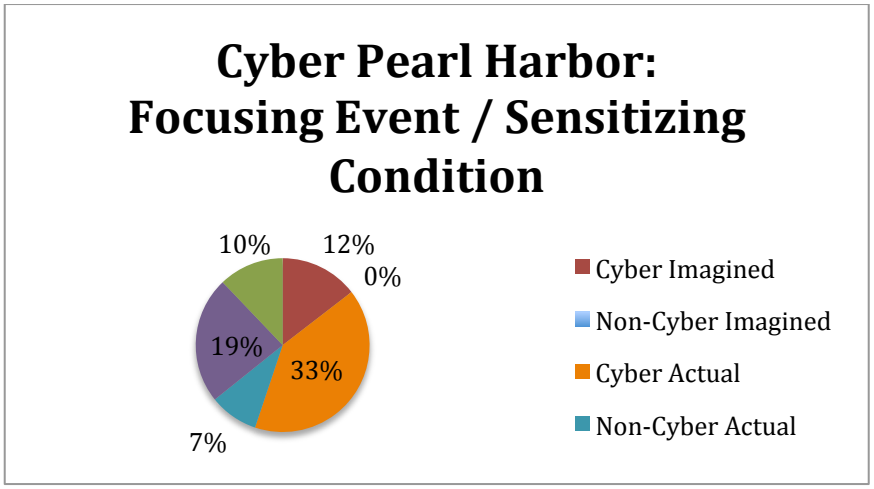


Figure 9. Cyber Pearl Harbor: Focusing Event/Sensitizing Condition.

Analogy, Framing, and Fear

We have explored the emergence and evolution of cyber Pearl Harbor in key texts and have traced how its circulation in news media has reinforced its presence in discussions of cyber security. However, mapping the use of cyber Pearl Harbor in both elite stakeholder discourse and broader media coverage only points to the ubiquity of its use and the preferred meanings that have attached to the analogy over time, what remains unconsidered are the consequences of the cyber security terrain shaped by these texts. As noted above, various observers, including

some who have themselves been responsible for promoting the idea of a cyber Pearl Harbor, like John Hamre, have worried that the use of Pearl Harbor as analogy or metaphor might have negative implications for our ability to understand and respond appropriately to the cyber threats that we face. In this section, we argue that these are valid concerns.

First, we know from decades of research in a number of disciplines, from cognitive science to communication studies and more, that language and rhetoric has an important structuring effect on how we see and respond to the world around us, a fact that many in the national security community are coming to recognize in recent years. A growing body of scholarship has demonstrated that "language, perception, and knowledge are inextricably intertwined" (Ortony 1993: 2). Far from being "a matter of...mere words," leading researchers Lakoff and Johnson argue that, "human *thought processes* are largely metaphorical ... the human conceptual system is metaphorically structured and defined" (Lakoff and Johnson 1980: 6). This means that metaphors (and analogies) shape the way we perceive and understand the world around us. But, this is not just an individual affair; our use of language helps "to structure collective, human knowledge" and to "bridge the gap between individual human cognition and collective understanding and action" (Lawson 2012). What's more, like potato chips, with metaphors it is hard to have just one. This is because individual metaphors often come with "entailments" that necessarily implicate other, related metaphors (Lakoff and Johnson 1980: 9). Even more important is that because metaphors can also operate as normative "structuring devices" (Wyatt 2004: 245), they can entail, "often covertly and insidiously, natural 'solutions'" (Ortony 1993: 5–6). The language we use, our metaphors and analogies, can enable or constrain our perceptions and understanding of the world around us, as well as our avenues of possible action in response (Lakoff and Johnson 1980: 10).

In recent years, military and national security professionals have increasingly recognized the importance of language, including metaphor and analogy, for correctly framing and responding to a range of complex, uncertain national security threats. This recognition is perhaps most prominent in the U.S. Army and Marine Corps, both of which have been influenced by the notion of operational design. So-called "design thinking" places a premium on the importance of problem framing and, in doing so, the important role of language. Top leaders in these services have promoted this idea and, in the case of the Army, have incorporated it into official doctrine and officer education (Mattis 2008; Department of the Army 2015; School of Advanced Military Studies n.d.).

The cyber security debate has not been immune to this rhetorical turn in national security discourse. As early as 1997, for example, Martin Libicki worried about the use of facile metaphors in the information warfare debates of the day. He warned, "To use metaphor in place of analysis verges on intellectual abuse. It invites the unquestioning extension of a logic that works across the looking glass but lacks explanatory power in the real world. Those who forget this are apt to try to make their metaphors do their thinking for them" (Libicki 1997: 6).

More recently, U.S. Cyber Command (USCYBERCOM) and its parent organization, U.S. Strategic Command (USSTRATCOM), have officially recognized the critical importance of

language and analogy for understanding cyber threats and then developing and carrying out a cyber strategy. In 2009, USSTRATCOM released, *The Cyber Warfare Lexicon*. The document began with a series of epigraphs. The first, from Dee Hock, read, “Language is only secondarily the means by which we communicate, it is primarily the means by which we think.” The second informed readers, “You can't talk about a subject if you don't have the words. And, some psychologists would argue, you can't even think about it. At least not very productively.” And finally, the document quoted Lt. Gen. Paul Van Riper (USMC, Ret.) as saying, “The seeming inability to express ideas clearly, loose use of words, and ill-considered invention of other terms have damaged the military lexicon to the point that it interferes with effective professional military discourse” (USSTRATCOM 2009: 4). Applied to cyber warfare, such deficiencies in language could have serious, real-world consequences:

> “Without a shared understanding of the accurate meanings of a significant number of frequently used terms, it will be difficult to make progress on the more complex and unresolved technical and operational issues for non-traditional weapons: actionable requirements, technical and operational assurance, effective mission planning techniques, and meaningful measures of effectiveness” (USSTRATCOM 2009: 4).

Three years later, in 2012, USCYBERCOM launched the Cyber Analogies Project at the Naval Postgraduate School. Led by respected scholars and policy makers, the project’s mission was “to assist U.S. Cyber Command in identifying and developing relevant historical, economic, and other useful metaphors that could be used to enrich the discourse about cyber strategy, doctrine, and policy” (Goldman & Arquilla 2014: 1). The final report of the project explained the importance of analogies:

> “Ability to keep pace with the cyber evolutionary curve, or perhaps to stay a step ahead of those who wish to do harm, depends on the ability to visualize how to fight in this new domain, just as strategists from earlier eras had to imagine how operating in the air, or with nuclear weapons, changed military affairs. Analogies drawn from earlier eras and different disciplines have the potential to help with visualization, allowing us to think through new or difficult subjects. They offer us an inductive approach to developing an understand- ing of high-level conceptual and operational issues related to cyber security and cyber warfare” (Goldman & Arquilla 2014: 1).

Ultimately, the report argues that appropriate “analogies, metaphors, and parables” are necessary to facilitate learning, communicating, and “winning H.G. Well’s ‘race between education and catastrophe’” (Goldman & Arquilla 2014: 5-6).

Second, we also know that news media not only plays an important role in promoting policy makers’ preferred agendas and problem frames for a wider public, but also in shaping policy makers’ understanding of the world. In this literature, “frames” are ‘‘schemata of interpretation’’ for individuals and groups to ‘‘locate, perceive, identify, and label’’ occurrences and events (Goffman 1974: 21). These “interpretive frameworks embedded in media messages” aid individuals and groups in “forming political attitudes and value judgments” by “evok[ing] as well

as constrain[ing] the interpretative activities of audiences" (Deluca et. al. 2012: 490). Policy makers are not immune from such effects; "In some such cases the media can participate in a positive feedback loop, which drives upward policymaking attention and outcomes very rapidly" (Wolfe et. al. 2013). Similarly, in her cultural history of the Internet, Stephanie Schulte observes, "Neither media representations nor policy formulations operate in isolation. Rather, they interact with each other, shaping each other's vocabulary and working in tandem within the minds of the public" (Schulte 2013: 366-367).

This feedback loop is at work in the case of cyber Pearl Harbor too. As noted above, James Wirtz has argued that concern with possible cyber Pearl Harbor "is reinforced by recurring media reports" (Wirtz 2014: 7). Peter Singer of Brookings has been extremely critical of this situation, saying,

> "[T]here is the histrionic — the "get scared"– category [of cyber security writing], then repeated back in the wider media, such as through the half-million references to "cyber 9/11." Journalists need to be more discerning consumers when they hear that kind of thing. There is a joke in our field that there should be a drinking game based on any time someone references a "cyber Pearl Harbor." More seriously, when someone says that, journalists should be prepared to follow up. Those phrases are the bumper stickers, not the end of the statement or argument. Yet they are used in business pitches, governmental speeches and Congressional hearings in that way. We've been caught between this state of ignorance and this fear factor. That's not a good place for anybody, either in the public space or on the journalistic side" (Singer & Wihbey 2014).

There is reason to believe that reliance on cyber Pearl Harbor to frame our thinking and responses has had real, negative impacts. General Alexander's internal 2012 memo about preventing a cyber Pearl Harbor indicates that this analogy and metaphor is not merely used by officials in public speeches, which is then picked up and repeated uncritically in news media, but that it also feeds back into the system of internal cyber security discourse and strategizing as a device that structures official thinking and planning behind the scenes (Alexander 2012). As we would expect from research by Lakoff and Johnson and others, the use of this analogy and metaphor has come with entailments and natural solutions. We got a preview of those in 1996 in Sen. Nunn's questioning of DCI Deutch. For those whose understanding of cyber threats have been shaped by the vision of cyber Pearl Harbor, natural solutions have entailed militarization, deterrence, and even offense.

But there is reason to be concerned that these public appeals to fear of catastrophic cyber Pearl Harbor may also have negative impacts on discourse and decision-making more broadly. The continuing use of cyber Pearl Harbor, even in the face of increasing recognition of its failures, is exemplary of the fact that policy makers and news media often rely on appeals to fear in their efforts to promote a policy agenda and frame issues for the public and themselves (Altheide 2002, 2006; Glassner 1999). However, a growing body of research in communication studies

(Peters et. al. 2013; Pfau 2007; Walton 2000; Witte 1998, 2000), psychology,[4] and even information security (Lee, et al., 2006; Herath & Rao, 2009; Pfleeger & Caputo, 2011; Siponen, et al., 2014; Boss, et al., 2015), demonstrates that such rhetoric can have a negative impact on our ability to motivate appropriate responses to otherwise legitimate problems, just as Hamre has worried might be the case with cyber Pearl Harbor. One recent study suggests that depictions of cyber doom scenarios in popular media "can lead to a sense of fatalism and demotivation to act" and "could impair efforts to motivate appropriate policy responses to genuine cyber security threats" (Lawson et. al. 2016: 65).

Similarly, there is evidence to support Healey's concern that constant worry about cyber Pearl Harbor has distracted us from the real threats we face, both cyber and non-cyber. In the cyber realm, Peter Singer writes, "Indeed, while the focus of US debate is more frequently on fears of a so-called 'digital Pearl Harbor', the more serious problem may actually be a long-term economic 'death by a thousand cuts.'" (Singer 2014: 70). Likewise, we can see repeated examples over the years of officials and experts warning of imminent cyber doom, or even ranking cyber threats higher than threats of terrorism or weapons of mass destruction, all while the real world continues to defy their predictions (Lawson 2016). While officials and experts worried about cyber terror attacks against the World Trade Center, al-Qa'ida plotted to bring down the Twin Towers with box cutters and airplanes. Nonetheless, we worried that "the next attack" would certainly be a cyber attack. But still terrorists attacked using cars, bombs, guns, and their very bodies. In more recent times, we have been warned that state adversaries would soon carry out a cyber Pearl Harbor, or perhaps that they already have, as when Director of NSA called the North Korea hack of Sony a cyber Pearl Harbor. Meanwhile, in reality, the North Koreans have stunned the world with their brazen tests of missiles and nuclear weapons. For their part, in cyberspace, the Russians have not carried out catastrophic cyber attacks on the U.S. power grid, but have instead attempted to manipulate the U.S. presidential election in a manner to which Washington seems unprepared to respond.

Conclusion

For twenty-five years, cyber Pearl Harbor has remained a go-to analogy and metaphor for officials and others looking to raise awareness of and motivate a response to perceived cyber threats, even when those threats remain ambiguous and evidence mounts that cyber Pearl Harbor is not an accurate reflection of the real threats that we face. So what are the prospects for the future of this analogy and metaphor in U.S. cyber security discourse?

Cyber Pearl Harbor is not going away any time soon, no matter how inaccurate it is as a descriptive device. This is because its rhetorical force and appeal are not a product of its ability to accurately describe, but rather, of its users' belief, rightly or wrongly, that the fear it evokes in listeners can call attention to and motivate a response to cyber threats, whatever their true

[4] For an overview of findings on fear appeals in psychology, see the website, "Fear appeals: Research into the effectiveness of threatening communication," http://fearappeals.com/ (accessed 15 September 2016).

nature may be. For this reason, and as argued above, we share John Hamre's concerns about the potentially negative impacts of this analogy in cyber security policymaking. This includes concern with the possibility that our ongoing, incorrect use of this analogy may have set in motion a self-fulfilling prophecy of militarization, including development and use of offensive cyber capabilities, which may have actually made the kinds of scenarios envisioned in cyber Pearl Harbor rhetoric more, rather than less, likely.

In the face of increasing criticism combined with an ongoing penchant for appealing to fear, one option for the future of cyber Pearl Harbor is rehabilitation through redefinition. This involves redefining cyber Pearl Harbor as many small attacks, or even large attacks, that occur but somehow go unnoticed. In short, it involves exaggerating the impacts of actual events, as when the NSA Director called the hack of Sony a cyber Pearl Harbor in February 2015 (Lyngaas 2015). Examples of this rhetorical move have been ubiquitous over the years. As far back as 1996, Sen. Sam Nunn floated the possibility that a large-scale cyber attack could occur without us noticing (Deutch 1996). In 2007, computer security expert, Rick Wesson, claimed that mass cyber crime meant that cyber Pearl Harbor had "already happened… It's just that people don't understand it has happened" (Blitstein 2007). In 2009, Amit Yoran, former head of the Department of Homeland Security's National Cyber Security Division, claimed that a "cyber-9/11" has already occurred, "but it's happened slowly so we don't see it" (Singel, 2009). In 2012, Richard Clarke told the *Washington Post* that "we're suffering the death of a thousand cuts in the little Pearl Harbors that are happening every day, where cyber-espionage and cybercrime are having a huge cumulative and negative effect" (Censer 2012). In 2014, Secretary of Defense Ashton Carter said, "We had a cyber Pearl Harbor. His name was Edward Snowden" (Whitlock 2014). The following year, the breach of the Office of Personnel Management by Chinese hackers sparked a similar round of comments. One conservative commentator said of the OPM breach, "We have our cyber Pearl Harbor" (Geraghty 2015). A law professor and privacy expert said the breach may be our "cyber 9/11" (Weisman 2015). Influential military futurist, technologist, and entrepreneur, John Robb, called the breach an "infobomb" and "a catastrophe we won't understand the consequences of until the US loses the next big conflict" (Robb 2015). Finally, one lawmaker even claimed that the OPM breach was actually more serious than 9/11 (Carman 2015).

But, as Tim Stevens notes, these kinds of redefinitions of cyber Pearl Harbor serve to "pluralize[] the previously singular 'event' and locat[e] them across multiple sectors… The integrity of the historical event is subverted still further by reference to the possibility of multiple 'small-scale' digital Pearl Harbors." In particular, he calls Clarke's assertion of daily digital Pearl Harbors "an idiosyncratic leap of logic too far, which all but destroyed any sensible use of the metaphor" (Stevens 2015: 131-132). It is hard to see, therefore, how redefining and "pluralizing" cyber Pearl Harbor will clarify our understanding of the real threats we face.

At the very least, another kind of modification will be necessary if we are to continue using the cyber Pearl Harbor analogy at all. In the examples of early differences in the cyber Pearl Harbor narrative examined above, we can see that it is neither natural nor inevitable that Pearl Harbor be deployed as it has been over its twenty-five year circulation in elite and popular discourses.

Instead of serving as a description of a crippling, catastrophic attack, Hamre's initial use demonstrates that the same analogy can be used to promote the idea that, with proper preparation, a large-scale cyber attack need not be crippling or catastrophic. This subtly different usage, we would suggest, is a potentially more appropriate one.

However, in the end, we would prefer to see the analogy abandoned altogether. Officials have had the tendency over the years to grow the threat to match the cyber Pearl Harbor metaphor instead of matching their metaphors to the threat. Such hyperbolic rhetoric is unnecessary for taking cyber security seriously. The interaction between Sen. Nunn and DCI Deutch indicates that the cyber Pearl Harbor analogy can come with the entailment of framing cyber security threats in military terms and seeking inappropriate military solutions. Importantly, DCI Deutch's response to Sen. Nunn indicates that it is possible to take cyber security threats extremely seriously (perhaps even too seriously in comparison to other threats), while still rejecting hyperbolic analogies and militaristic responses.

What's more, there is no shortage of other, potentially more appropriate and useful analogies and metaphors that may be enlisted to help us think about cyber security challenges. These can include other forms of conflict or weapons systems like piracy, counterinsurgency, or biological weapons, or even non-war analogies and metaphors such as the immune systems, public health, ecosystems, or complex adaptive systems. A number of scholars, technologists, and policy makers have begun to think along these lines, offering many possibilities for moving away from the stale, inaccurate, and potentially detrimental threat of a cyber Pearl Harbor (Charney 2010; JASON 2010; Liles 2010; Department of Homeland Security 2011; Lapointe 2011; Lawson 2012; Axelrod 2014).

The importance of language and rhetoric for appropriately framing and responding to problems is abundantly clear. Increasingly, military and national security professionals are coming to this understanding as well. This includes those who are wrestling with complex problems like threats to cyber security, where there is increasing recognition that hyperbolic analogies and metaphors like cyber Pearl Harbor are not only inadequate, but may actually be harmful, to our ability to understand and respond to the cyber threats we face today. It is our hope that the research presented here can aid scholars and policy makers in understanding the emergence, evolution, and persistence of the cyber Pearl Harbor analogy as a first step towards developing more appropriate and productive frames for understanding and responding to cyber security threats.

References

Adhikari, R. (2009) "Civilization's high stakes cyber-struggle: Q&a with gen. Wesley clark (ret.)," *TechNewsWorld*, 2 December 2009. Online. Available HTTP: <http://www.technewsworld.com/story/Civilizations-High-Stakes-Cyber-Struggle-QA-With-Gen-Wesley-Clark-ret-68787.html?wlc=1259861126&wlc=1259938168&wlc=1290975140> (accessed 2 December 2009).

Altheide, D.L. (2002) *Creating Fear: News and the Construction of Crisis,* New York: Aldine de Gruyter.

Altheide, D.L. (2006) *Terrorism and the Politics of Fear,* Lanham, MD: AltaMira Press.

Axelrod, R. (2014) "A Repertory of Cyber Analogies," in Goldman, E.O. and Arquilla, J. (eds) *Cyber Analogies,* Monterey, California, Naval Postgraduate School, pp. 108-16.

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, pp. 49-73.

Bendrath, R., Eriksson, J. and Giacomello, G. (2007) "From 'Cyberterrorism' to 'Cyberwar', Back and Forth: How the United States Securitized Cyberspace," in Eriksson, J. and Giacomello, G. (eds) *International Relations and Security in the Digital Age,* London: Routledge.

Benoit, W.L. (2011) "Content Analysis in Political Communication," in Bucy, E.P. and Hoblert, R.L. (eds) *Sourcebook for political communication research: Methods, measures, and analytical techniques,* London: Routledge, pp. 268-279.

Betz, D.J. and Stevens, T. (2013) "Analogical Reasoning and Cyber Security," *Security Dialogue,* 44, 2: 147-64.

Bigo, D. (2000) "When Two Become One: Internal and External Securitisations in Europe," in Kelstrup, M. and Williams, M. (eds) *International Relations Theory and the Politics of European Integration: Power, Security, and Community,* London: Routledge, pp. 171-204.

Bigo, D. (2006) "Security, Exception, Ban and Surveillance," in Lyon, D. (ed.) *Theorizing Surveillance: The Panopticon and Beyond,* Cullompton, Devon: Willan Publishing, pp. 46- 58.

Blitstein, R. (2007) "Part I: How online crooks put us all at risk," *San Jose Mercury News*, 8 November 2007, LexisNexis.

Boss, S.R. et al. (2015) "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly,* Forthcoming: 1-28.

Brockriede, W. (1974) "Rhetorical criticism as argument." *Quarterly Journal of Speech*, 60, 2: 165-174.

Bussey, J. (2016) “Gen. Michael hayden gives an update on the cyberwar,” *Wall Street Journal*, 9 February 2016. Online. Available HTTP: < http://www.wsj.com/articles/gen-michael-hayden-gives-an-update-on-the-cyberwar-1455076153> (accessed 9 February 2016).

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

Carman, A. (2015) “Opm breaches more serious to national security than 9/11, congresswoman argues during hearing,” *SC Magazine*, 16 June 2015. Online. Available HTTP: < http://www.scmagazine.com/house-committee-on-oversight-and-government-reform-hosts-hearing-on-data-breaches/article/421052/> (accessed 16 June 2015).

Carter, A.B., Deutch, J. and Zelikow, P. (1998) “Catastrophic Terrorism: Tackling the New Danger,” *Foreign Affairs,* November/December. Retrieved from https://www.foreignaffairs.com/articles/united-states/1998-11-01/catastrophic-terrorism-tackling-new-danger.

Censer, M. (2012) “Little cyber attacks have big effects,” *The Washington Post*, 7 May 2012, A10.

Charney, S. (2010) *Collective Defense: Applying Public Health Models to the Internet,* Redmond, WA: Microsoft Corp.

"CIA warns of cyber-terror attacks" 1996. *The Australian.* 27 June 1996. Date Accessed: 2016/09/17. www.lexisnexis.com/hottopics/lnacademic.

Clapper, Gen. J. R. (2015) “Statement for the Record: Worldwide Cyber Threats,” United States House of Representatives, House Permanent Select Committee on Intelligence, 10 September 2015.

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

Collins, S. (2015) “Senator collins continues to sound the alarm on the urgent need to bolster cybersecurity,” *Press Release, Office of Senator Susan Collins*, 06 August 2015. Online. Available HTTP: < http://www.collins.senate.gov/public/index.cfm/2015/8/senator-collins-continues-to-sound-the-alarm-on-the-urgent-need-to-bolster-cybersecurity> (accessed 06 August 2015).

Conway, M. (2008) “Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures,” in Dunn Cavelty, M. and Kristensen, K.S. (eds) *Securing the ‘Homeland’: Critical Infrastructure, Risk and (in)security,* London: Routledge, pp. 109-29.

"Cyber terrorists threaten US, CIA boss warns" 1996. *Hobart Mercury (Australia).* 27 June 1996. Date Accessed: 2016/09/17. www.lexisnexis.com/hottopics/lnacademic.

Darsey, J. (1994) “Must we all be rhetorical theorists?: An anti□democratic inquiry.” *Western Journal of Communication*, *58,* 3:164-181.

Debrix, F. (2001) “Cyberterror and Media-Induced Fears: The Production of Emergency Culture,” *Strategies,* 14, 1: 149-68.

DeLuca, K., Lawson, S. and Sun, Y. (2012) “Occupy Wall Street on the Public Screens of Social Media: The Many Framings of the Birth of a Protest Movement,” *Communication, Culture & Critique,* 5, 4: 483-509.

Department of the Army. (2015) *ATP 5-0.1: Army Design Methodology*. Washington, D.C.: Department of the Army.

Department of Homeland Security. (2011) *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem With Automated Collective Action,* Washington, D.C.: Department of Homeland Security.

Dunn Cavelty, M. (2008) *Cyber security and Threat Politics: U.s. Efforts to Secure the Information Age,* New York: Routledge.

Dunn Cavelty, M. and Van Der Vlugt, R.A. (2015) “A Tale of Two Cities: Or How Wrong Metaphors Lead to Less Security,” *Georgetown Journal of International Affairs,* Fall: 21-29.

Elias, T.D. (1994) “Toffler: Computer attacks wave of future,” *South Bend Tribune (Indiana)*, 2 January 1994, F10.

Eriksson, J. (2002) “Cyberplagues, IT, and Security: Threat Politics in the Information Age,” *Journal of Contingencies and Crisis Management,* 9, 4: 211-22.

Füredi, F. (2009) *Invitation to Terror: The Expanding Empire of the Unknown,* London: Continuum.

Geraghty, J. (2015) “‘the opm hack was just the start and it won’t be the last.’,” *National Review*, 12 June 2015. Online. Available HTTP: < http://www.nationalreview.com/corner/419678/opm-hack-was-just-start-and-it-wont-be-last-jim-geraghty> (accessed 12 June 2015).

Glassner, B. (1999) *The Culture of Fear: Why Americans Are Afraid of the Wrong Things,* New York, NY: Basic Books.

Goffman, E. (1974) *Frame Analysis: An Essay on the Organization of Experience,* New York: Harper & Row.

Goldman, E.O. and Arquilla, J. (eds) (2014) *Cyber Analogies*, Monterey, California, Naval Postgraduate School.

Hansen, L. and Nissenbaum, H. (2009) "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly,* 53, 4: 1155-75.

Hart, R.P. (1990) *Modern rhetorical criticism*. New York. Scott Foresman & Company.

Hasian, M., Lawson, S.T. and McFarlane, M. (2015) *The Rhetorical Invention of America's National Security State,* Lanham, MA: Lexington Books.

Hardt, M. and Negri, A. (2004) *Multitude: War and Democracy in the Age of Empire,* New York: The Penguin Press.

Herath, T. and Rao, H.R. (2009) "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems,* 18, 2: 106-25.

Hoffman, B. (1998) *Inside Terrorism,* New York: Columbia University Press.

Hoffman, D. and Waisanen, D. (2015) "At the Digital Frontier of Rhetoric Studies: An Overview of Tools and Methods for Computer-Aided Textual Analysis" in Ridolfo, J. and Hart-Davidson, W. (eds) *Rhetoric and the Digital Humanities*, Chicago, University of Chicago Press, pp. 169-183.

JASON. (2010) *Science of Cyber-Security,* McLean, VA: JASON, The MITRE Corporation.

Kaplan, F. (2016) *Dark Territory: The Secret History of Cyber War,* New York: Simon & Schuster.

Koppel, T. (2015) *Lights Out: A Cyber attack, a Nation Unprepared, Surviving the Aftermath,* New York: Crown.

Krippendorff, K. (2004) *Content analysis: An introduction to its methodology*. New York: Sage.

Lakoff, G. and Johnson, M. (1980) *Metaphors We Live By,* Chicago: University Of Chicago Press.

Lapointe, A. (2011) "When Good Metaphors Go Bad: The Metaphoric "Branding" of Cyberspace," *Center for Strategic and International Studies.*

Laqueur, W. (1999) *The New Terrorism: Fanaticism and the Arms of Mass Destruction,* New York: Oxford University Press.

Lawson, S. (2012) “Putting the ‘War’ in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States,” *First Monday,* 17, 7.

Lawson, S. (2013) “Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats,” *Journal of Information Technology & Politics,* 10, 1: 86-103.

Lawson, S. (2016) “On this date in cyber doom history: An example of getting it so wrong for so long,” *Forbes.com*, 25 June 2016. Online. Available HTTP: < http://www.forbes.com/sites/seanlawson/2016/06/25/on-this-date-in-cyber-doom-history-an-example-of-getting-it-so-wrong-for-so-long/#37c553327f41> (accessed 25 June 2016).

Lawson, S.T. et al. (2016) “The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate,” in Pissandis, N., Roigas, H. and Veenendaal, M. (eds) *Proceedings of the 8th International Conference on Cyber Conflict (CyCon),* IEEE, pp. 65-80.

Lee, D., Larose, R. and Rifon, N. (2008) “Keeping Our Network Safe: A Model of Online Protection Behaviour,” *Behaviour & Information Technology,* 27, 5: 445-54.

Leff, M. (1990) "Words the most like things: Iconicity and the rhetorical text." *Western Journal of Communication,* 54, 3: 252-273.

Lewis, J.A. (2010) “The Cyber War Has Not Begun,” unpublished manuscript.

Libicki, M.C. (1997) *Defending Cyberspace, and Other Metaphors,* Washington, DC: U.S. Government Printing Office.

Libicki, M.C. (1997) *Defending Cyberspace, and Other Metaphors,* Washington, DC: U.S. Government Printing Office.

Lifton, R.J. (1999) *Destroying the World to Save it: Aum Shinrikyo, Apocalyptic Violence, and the New Global Terrorism,* New York: Henry Holt and Co.

Liles, S. (2010) “Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency,” in Czosseck, C. and Podins, K. (eds) *Conference on Cyber Conflict Proceedings 2010,* Tallinn, Estonia: CCD COE Publications, pp. 47-58.

Lyngaas, S. (2015) “Nsa’s rogers makes the case for cyber norms,” *FCW*, 23 February 2015. Online. Available HTTP: < https://fcw.com/articles/2015/02/23/nsa-rogers-cyber-norms.aspx> (accessed 23 February 2015).

Markoff, J. (1999) “Blown to bits; cyberwarfare breaks the rules of military engagement,” *The New York Times*, 17 October 1999, LexisNexis.

Martinez, J. (2012) “Napolitano: Us financial institutions ‘actively under attack’ by hackers,” *The Hill*, 31 October 2012. Online. Available HTTP: < http://thehill.com/policy/technology/265167-napolitano-us-financial-institutions-qactively-under-attackq-by-hackers> (accessed 31 October 2012).

Mattis, J.N. (2008) “USJCOM Commander’s Guidance for Effects-Based Operations,” *Joint Forces Quarterly,* 51, 4: 105-8.

McKerrow, R. E. (1989) "Critical rhetoric: Theory and praxis." *Communications Monographs,* 56, 2: 91-111.

McGee, M.C. (1990) "Text, context, and the fragmentation of contemporary culture." *Western Journal of Communication,* 54, 3: 274-289.

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

Neuendorf, K.A. (2011) Content analysis—A methodological primer for gender research. *Sex Roles*, *64,*3-4: 276-289.

Obama, B. (2015) “Remarks by the president at the cybersecurity and consumer protection summit,” *Office of the Press Secretary, The White House*, 13 February 2015. Online. Available HTTP: < https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit> (accessed 13 February 2015).

Ortony, A. (1979) *Metaphor and Thought,* Cambridge ; New York: Cambridge University Press.

Pagliery, J. (2015) “Senate overwhelmingly passes historic cybersecurity bill,” *CNN*, 27 October 2015. Online. Available HTTP: < http://money.cnn.com/2015/10/27/technology/cisa-cybersecurity-information-sharing-act/> (accessed 27 October 2015).

Peoples, C. and Vaughan-Williams, N. (2010) *Critical Security Studies: An Introduction,* London: Routledge.

Peters, G.-J.Y., Ruiter, R.A.C. and Kok, G. (2013) “Threatening Communication: A Critical Re-Analysis and a Revised Meta-Analytic Test of Fear Appeal Theory,” *Health Psychology Review,* 7, sup1: S8-S31.

Pfau, M. (2007) “Who’s Afraid of Fear Appeals? Contingency, Courage, and Deliberation in Rhetorical Theory and Practice,” *Philosophy and Rhetoric,* 40, 2: 216-37.

Pfleeger, S.L. and Caputo, D.D. (2012) “Leveraging Behavioral Science to Mitigate Cyber Security Risk,” *Computers & Security,* 31, 4: 597-611.

Robb, J. (2015) “The OPM infobomb explodes,” *Global Guerrillas*, 24 June 2015. Online. Available HTTP: < http://globalguerrillas.typepad.com/globalguerrillas/2015/06/the-opm-infobomb-explodes.html> (accessed 24 June 2015).

Rothkopf, D. (2011) “Where fukushima meets stuxnet: The growing threat of cyber war,” *Foreign Policy*, 17 March 2011. Online. Available HTTP: < http://foreignpolicy.com/2011/03/17/where-fukushima-meets-stuxnet-the-growing-threat-of-cyber-war/> (accessed 17 March 2011).

School of Advanced Military Studies. (n.d.) *Art of Design: Student Text, Version 2.0*. Leavenworth, KS: Command and General Staff College.

Schulte, S.R. (2013) *Cached: Decoding the Internet in Global Popular Culture,* New York: New York University Press.

Singel, R. (2009) “Is the Hacking Threat to National Security Overblown?,” *Threat Level,* 3 June 2009, Online. Available HTTP: < http://www.wired.com/threatlevel/2009/06/cyberthreat> (accessed 3 June 2009).

Singer, P.W. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know,* London: Oxford University Press.

Singer, P.W. and Wihbey, J. (2014) “Research chat: Peter Singer on cybersecurity and what the media needs to know,” 14 April 2014. Online. Available HTTP: < https://www.brookings.edu/on-the-record/research-chat-peter-singer-on-cybersecurity-and-what-the-media-needs-to-know/> (accessed 14 April 2014).

Siponen, M., Adam, M., M. and Pahnila, S. (2014) “Employees’ Adherence to Information Security Policies: An Exploratory Field Study,” *Information & Management,* 51, 2: 217-24.

Stevens, T. (2015) *Cyber Security and the Politics of Time,* Cambridge: Cambridge University Press.

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,* 46, 4-5: 223-38.

The Atlantic. (2010) “Fmr. Intelligence director: New cyber attack may be worse than 9/11,” *The Atlantic*, 30 September 2010. Online. Available HTTP: < http://www.theatlantic.com/politics/archive/2010/09/fmr-intelligence-director-new-cyber attack-may-be-worse-than-9-11/63849/> (accessed 30 September 2010).

USSTRATCOM. (2009) *The Cyber Warfare Lexicon: A Language to Support the Development, Testing, Planning, and Employment of Cyber Weapons and Other Modern Warfare Capabilities,* USSTRATCOM.

Valeriano, B. and Maness, R.C. (2015) *Cyber War Versus Cyber Realities: Cyber Conflict in the International System,* London: Oxford University Press.

Wall, D.S. (2008) "Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge About Cybercrime," *Information, Communication & Society,* 11, 6: 861-84.

Walton, D.N. (2000) *Scare Tactics: Arguments That Appeal to Fear and Threats,* Boston: Kluwer Academic Publishers.

Weimann, G. (2005) "Cyberterrorism: The Sum of All Fears?," *Studies in Conflict & Terrorism,* 28, 2: 129-49.

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

Weisman, S. (2015) "The hacking of opm: Is it our cyber 9/11?," *USA Today*, 13 June 2015. Online. Available HTTP: < http://www.usatoday.com/story/money/columnist/2015/06/13/hacking-opm-weisman/28697915/> (accessed 13 June 2015).

Whitlock, C. (2014) "Ashton carter, passed over before, gets picked by obama to be defense secretary," *The Washington Post*, 5 December 2014. Online. Available HTTP: < https://www.washingtonpost.com/world/national-security/ash-carter-passed-over-before-gets-picked-by-obama-to-lead-pentagon/2014/12/05/33a2429a-7c95-11e4-9a27-6fdbc612bff8_story.html> (accessed 5 December 2014).

Wirtz, J.J. (2014) "The Cyber Pearl Harbor," in Goldman, E.O. and Arquilla, J. (eds) *Cyber Analogies,* Monterey, California, Naval Postgraduate School, pp. 7-14.

Witte, K. (1998) "Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Process Model to Explain Fear Appeal Success and Failure," in Anderson, P.A. and Guerrero, L.K. (eds) *Handbook of Communication and Emotion: Theory, Applications, and Contexts,* San Diego, CA: Academic Press, pp. 423-50.

Witte, K. and Allen, M. (2000) "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns," *Health Education & Behavior,* 27, 5: 591-615.

Wolfe, M., Jones, B.D. and Baumgartner, F.R. (2013) "A Failure to Communicate: Agenda Setting in Media and Policy Studies," *Political Communication,* 30, 2: 175-92.

Wyatt, S. (2004) "Danger! Metaphors At Work in Economics, Geophysiology, and the Internet," *Science, Technology & Human Values,* 29, 2: 242.

DRAFT

Appendix A

Content Analysis Codebook

	Variables	Definition
Sentiment	Neutral	Cyber Pearl Harbor is mentioned but is neither endorsed or rejected.
	Positive	Endorsing, promoting, affirming, etc. the idea that a cyber Pearl Harbor is a real threat
	Negative	Ambivalence, skepticism, rejection, etc. towards cyber Pearl Harbor as a threat.
	Sentiment Combination	The article provides both positive and negative assessments of cyber Pearl Harbor.
	Sentiment Note	If there is a combination of sentiments, use the notes field to provide a brief explanation.
(De)securitizing actors	**Variables**	**Definition**
	Official\Civilian bureaucrat	A nonmilitary member of government, unelected individual such as a cabinet secretary, presidential advisor, etc.
	Official\Elected official	An individual such as the President, member of Congress, governor, etc.
	Official\Military officer	A uniformed military member, like Chairman of the Joint Chiefs, a service chief, etc.
	Official\Law enforcement	An individual such as FBI director or agent, other law enforcement, or Department of Justice official, US Attorney, etc.
	Official\Intelligence analyst or official	An intelligence official like director or deputy director of NSA or CIA, or generic intelligence officials or intelligence analysts.
	Official\Anonymous or unnamed	Citation of anonymous officials who remain unnamed.
	Official\Other	An official not covered in other definitions.
	Private\Computer security industry	A cited expert who is a researcher, analyst, expert, etc. from a private computer security firm such as Symantec, Kaspersky, etc.
	Private\Defense contractor	A cited expert who is a researcher, analyst, expert, etc. from a defense contractor like Lockheed, Booze Allen, etc.
	Private\Think tank	A cited expert who is a researcher, analyst, expert, etc. from a think tank like CSIS, Brookings, etc.
	Private\University researcher/academic	A cited expert who is a researcher, analyst, expert, etc. from a university.
	Private\Other	Another kind of private source not defined above.
	Private\Journalist	Citation of another journalist or use of the metaphor by the journalist him/herself without citing someone else.
	Actor Combination	More than one securitizing actor is cited
	Actor Note	If there is a combination of actors cited, use the notes field to provide a brief explanation.
Threat subjects	**Variables**	**Definition**
	State\China	China identified as a possible source of a cyber Pearl Harbor attack.
	State\Russia	Russia identified as a possible source of a cyber Pearl Harbor attack.
	State\Iran	Iran identified as a possible source of a cyber Pearl Harbor attack.
	State\North Korea	North Korea identified as a possible source of a cyber Pearl Harbor attack.
	State\Iraq	Iraq identified as a possible source of a cyber Pearl Harbor attack.
	State\Generic, unspecified state(s)	Generic hostile, foreign, etc. but unnamed states identified as a possible source of a cyber Pearl Harbor attack.
	State\Other, specified	Other named states not listed above identified as a possible source of a cyber Pearl Harbor attack.
	Non-state\Terrorists	Terrorist group(s) identified as a possible source of a cyber Pearl Harbor attack, such as al-Qa'ida, ISIS, etc.
	Non-state\Criminals	Criminals identified as a possible source of a cyber Pearl Harbor attack.
	Non-state\Hacktivists	Political hacker-activists ("hacktivists"), generic or specified (e.g. Anonymous), identified as a possible source of a cyber Pearl Harbor attack.
	Non-state\Generic, unspecified hackers	Generic "hackers," not identified as political, terrorists, criminals, or otherwise, identified as a possible source of a cyber Pearl Harbor attack.
	Non-state\Other	Some other non-state actor not listed above identified as a possible source of a cyber Pearl Harbor attack.
	Hybrid	A combination state and non-state threat actor, such as state-sponsored, supported, or inspired hackers, criminals, or terrorists, identified as a possible source of a cyber Pearl Harbor attack.
	Other	Some other source of threat not listed above (e.g. system failure, accident, disgruntled insider, etc.) identified as a possible source of a cyber Pearl Harbor attack.
	Unspecified	No threat actor is identified as a possible source of a cyber Pearl Harbor attack.
	Subject Combination	Some combination of states or non-state actors identified as the possible source of a cyber Pearl Harbor attack.
	Subject Combination Note	If a combination of state or non-state actors is identified, use the notes field to provide an explanation.
	NA	Article rejects the notion of cyber Pearl Harbor so the concept does not apply.
Referent objects	**Variables**	**Definition**
	Civilian critical infrastructure	Infrastructure such as electrical power, water, transportation, financial system, or similar systems identified as an object of attack resulting in a cyber Pearl Harbor.
	Military infrastructure/systems	Military command, control, communications systems, computers, logistics systems, etc. identified as an object of attack resulting in a cyber Pearl Harbor.
	Informational assets	Information such as government secrets or private intellectual property identified as an object of attack resulting in a cyber Pearl Harbor.
	Other	Some other asset or system not listed above identified as an object of attack resulting in a cyber Pearl Harbor.
	Unspecified	No asset or system identified as an object of attack resulting in a cyber Pearl Harbor.
	Object combination	Multiple objects are identified as a possible target of a cyber Pearl Harbor attack.
	Object combination note	If multiple objects are identified as a possible target, use the notes field to provide an explanation.
	NA	Article rejects the notion of cyber Pearl Harbor so the concept does not apply.
Focusing events/ sensitizing conditions	**Variables**	**Definition**
	Cyber imagined	An imagined cyber event in the form of a fictional scenario, wargame, work of popular fiction, or similar used as evidence or reason why we should be concerned about the possibility of cyber Pearl Harbor
	Non-cyber imagined	???
	Cyber actual	A cyber event such as DDOS, defacement, data breach, system vulnerabilities, other cyber attack, or (non)government report/study provided as evidence or reason why we should take the threat of a cyber Pearl Harbor seriously.
	Non-cyber actual	A non-cyber event such as a traditional terrorist attack or natural disaster (e.g. 9/11, OKC, Sandty, etc.) used as evidence or reason why we should be concerned about the possibility of a cyber Pearl Harbor.
	Unspecified	No event or condition provided as evidence or reason why we should take the threat of a cyber Pearl Harbor seriously.
	Event/condition combination	Multiple events or conditions are provided as evidence or reason why we should take the threat of a cyber Pearl Harbor seriously.
	Event/condition combination note	If multiple events or conditions are provided, use the notes field to provide an explanation.
	NA	Article rejects the notion of cyber Pearl Harbor so the concept does not apply.

Table 1. Codebook for U.S Newspapers

Appendix B

Intercoder Reliability Table

Intercoder Reliabilty Values	
Sentiment	α = 1.0
(De)Securitizing Actor	α =.78
Threat Subject	α =.95
Referent Object	α =.83
Focusing Event/Condition	α =.93

Table 2. Intercoder reliability values (Krippendorf's alpha).

Appendix C

Cyber Pearl Harbor: Key Texts, 1991-2016
Alexander, G.K. (2012) *United States Cyber Command (Uscybercom) Commander's Strategic Assessment for Operating in Cyberspace--preventing a Pearl Harbor Environment,* Fort George R. Mead, MD: United States Cyber Command. Deutch, J.M. (1996) "Statement to Senate Governmental Affairs Committee," *Vulnerability of United States Government Information Systems to Computer Attacks*, Hearing, 25 June 1996. Hamre, J. (1997) "Prepared Statement to Senate Judiciary Committee, Technology, Terrorism, and Government Information Subcomittee," *The Nation at Risk: Report of the President's Commission on Critical Infrastructure Protection,* Hearing, 5 November 1997. Hamre, J. (1998) "Prepared Testimony of John J. Hamre to the House National Security Committee, Military Procurement and Military Research and Development Subcommittee," *Information Assurance and Critical Infrastructure Protection,* Hearing, 11 June 1998. Hamre, J. (2015) "The 'electronic pearl harbor'," *Politico*, 9 December 2015. Online. Available HTTP: <http://www.politico.com/agenda/story/2015/12/pearl-harbor-cyber-security-war-000335> (accessed 9 December 2015). Kirk, M. (2003) "CYBER WAR!," *PBS Frontline,* Transcript Online. Available HTTP: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html> (accessed 15 August 2016). Lieberman, J., Collins, S. and Carper, T. (2011) "Avoiding a digital Pearl Harbor," *The Washington Post,* 8 July 2011, A13. Panetta, L. (2011) "Testimony at The Senate Armed Services Committee," *Nomination of Leon Panetta to the Position of Secretary of Defense,* Hearing, 9 June 2011. Panetta, L. (2012) "Defending the national from cyber attacks," presented at Business Executives for National Security, New York, NY. 11 October 2012. Schwartau, W. (1991) "Fighting terminal terrorism," *Computerworld*, 28 January 1991, 23.

Table 3. Key Texts in the Cyber Pearl Harbor Discourse, 1991-2016