What Analogies Can Tell Us About the Future of Cybersecurity

David SULEK[a], and Ned MORAN[b]
[a] *Principal, Booz Allen Hamilton*
[b] *Senior Consultant, Booz Allen Hamilton*

Abstract. For more than a decade, leading experts in government and industry have warned of an impending Cyber Pearl Harbor, a surprise electronic attack with the potential to neutralize U.S. military power and cause massive disruptions in U.S. and global computer networks. This is a powerful historical analogy—but is it the right one? This paper articulates a framework to better explore and examine the use of historical analogies in their application to conflict in cyberspace. The resulting analysis does not seek to argue the Pearl Harbor analogy is a bad one. Quite to the contrary—our thesis is that while a cyber Pearl Harbor remains a possibility, is should not be treated by decision makers as an inevitability and that there may be equally powerful historical analogies to guide future cyber strategies.

Keywords: cyber conflict, cybersecurity, decision science, decision-making, historical analogies, public policy

Introduction

In their study Thinking in Time: The Uses of History for Decision-Makers, authors Richard Neustadt and Ernest May speak to the power and perils of making decisions through the use of historical analogies. They argue for a structured, critical inquiry to address an issue or crisis rather than leaping to a single analogy for which to formulate strategies and policy options (e.g., "Appeasement at Munich"). Systematic use of appropriate historical analogies can clarify the present situation, offer strategic insights, and inform policy options. On the other hand, incorrectly applying an analogy can muddy objectives, narrow policy options, and create blind spots for decision-makers.

One can debate when cybersecurity first emerged as an issue, but many consider the 1988 Morris Internet Worm a common marker. In the 20 years since this self-replicating program spread across the Internet at remarkable speed, attention has turned to countering fast-moving, continuously evolving cyber threats and vulnerabilities. In that time, a single historical analogy has appeared to dominate US Government thinking: the threat of a cyber Pearl Harbor.

This is a powerful, even seductive possibility. It connotes a bold stroke launched by an enemy without warning designed to neutralize US military power. This represents an imminent threat that is ignored only at one's own peril. The introduction of new weapons, strategies, doctrines, and tactics suddenly tilt the military balance toward the offense. Even those who do not directly advocate the Pearl Harbor analogy

often employ similar imagery. For example, a number of cyber experts have suggested the potential for a "cyber 9/11"[1] or a "cyber Katrina.[2] While important distinctions exist between these analogies (e.g., Pearl Harbor centered on a state-based actor, 9/11 on a non-state actor, and Hurricane Katrina on an 'act of God'), the implications are clear. Drawing from history's lessons, experts warn of the potentially catastrophic dangers facing our cyber networks unless immediate, decisive action is taken.

If the Pearl Harbor analogy proves correct, one can argue the US and other countries will be better prepared. What if, however, the analogy proves erroneous or the wrong lessons are drawn? For example, could the focus on a single analogy ultimately create a self-fulfilling prophecy, something more akin to a modern *Guns of August?* This paper will not argue the Pearl Harbor analogy is a bad one. Instead, our thesis is that *while a cyber Pearl Harbor is a possibility, it should not be treated as inevitable.* To test this thesis, this paper will explore a range of historical analogies that might inform different options and courses of action available to decision-makers.

1. Thinking in Time

An inspiration for this paper is Thinking in Time, which outlined a systematic framework for policy practitioners to critically analyze key policy challenges and formulate well-reasoned strategies and options. Through case study analysis, Neustadt and May point to six problems that often negatively impact the quality of decisions:[3]

- A plunge toward action
- Overdependence on fuzzy analogies
- Inattention to an issue's own past
- Failure to think about key presumptions
- Stereotyped suppositions about persons or organizations
- Little or no effort to see choices as part of a historical sequence

To address these common shortcomings, the authors conclude that "better decision-making involves drawing on history to frame sharper questions [about a crisis or policy challenge] and doing so systematically, routinely."[3] Specifically, in response to a crisis or policy challenge, they recommend that decision-makers develop a detailed issue history. This history will enable them to clarify the overarching policy objectives and anticipate those conditions that are desired in the future after actions are taken. At the same time, an issue history provides the basis for determining which historical analogies might apply—and why. Neustadt and May then outline a process for developing issue history, summarized below:[1]

- **Determine the *Story* and *Timeline*.** The centerpiece of an issue history is a narrative story (what is happening today and why) accompanied by a timeline. The authors emphasize the timeline should begin at the earliest possible and relevant date of significance to ensure proper context for analysis.

[1] Authors note: we have taken the liberty of condensing and summarizing steps that are spelled out in detail in Chapters 6-14 of *Thinking in Time* [3].

- **Identify *Change Points*.** On that timeline, understand where significant changes altered the trajectory or thinking about the current issue.
- **Separate the *Known*, *Unclear*, and *Presumed*.** The authors point to the need early in a policy crisis to determine what is known (facts), what is unclear (absence of facts or evidence), and what is presumed (assumptions).
- **Challenge *Presumptions*.** Decision-makers must carefully review the core presumptions. Good presumptions are those that clarify and define a situation and surface concerns. Bad presumptions are value-laden, things that cannot be challenged save in its own terms by opposed values (e.g., the authors use the model of "communists are bad; market mechanisms good").

An issue history becomes the foundation from which decision-makers can judiciously compare current and past events to determine likenesses and differences. Embedded in these likenesses and differences are key insights that can shape future strategies. In concluding their analysis, the authors state, "Sensing that the present was alive with change, they knew the past would be outmoded by a future that had never been…but their image of that future could be realistic because [it was] informed by understanding its sources in the past"[3] In other words, no single historic event will prove a perfect analogy to the present moment—the underlying conditions will be different. However, thoughtful selection of historical analogies can offer decision-makers insights that enrich and inform the choices they must make while also enabling them to better anticipate the downstream implications of those choices.

2. The Cyber Issue History—In Brief

In April 2007, the Estonian government and many of that country's key lifeline infrastructures faced a barrage of coordinated cyber attacks. An unseen adversary launched sophisticated attacks to cause massive network disruptions—"a flood of bogus requests for information from computers around the world conspired to cripple the websites of Estonia banks, media outlets, and ministries for days."[4] Without delving into the specific causes, actors, and motives of the Estonian attacks, the entire event confirmed what many experts warned about cybersecurity. An adversary was able to employ cyber weapons and strike without warning. Directly attributing the source of the attack proved fleeting. Critical infrastructures appeared fragile in the face of withering DDoS attacks. Computer attacks were accompanied by social engineering and flash mobs to magnify effects. In response to this and other cyber events, the U.S. launched a comprehensive review of its national cybersecurity strategies.

Today's cyber issues, however, trace their lineage to the Superpower technology rivalry that was energized in 1957 with the launch of Sputnik. Following that psychological shock of this event, the US embarked on an ambitious program to ensure technological superiority for the foreseeable future. While the Space Program is often cited as the most significant post-Sputnik achievement, the seeds of the Internet were planted during this same era. The period beginning in the early 1960s and lasting through the late 1980s (see Figure 1) was dominated by government, industry, and academic researchers in their drive to develop internetworking technologies.

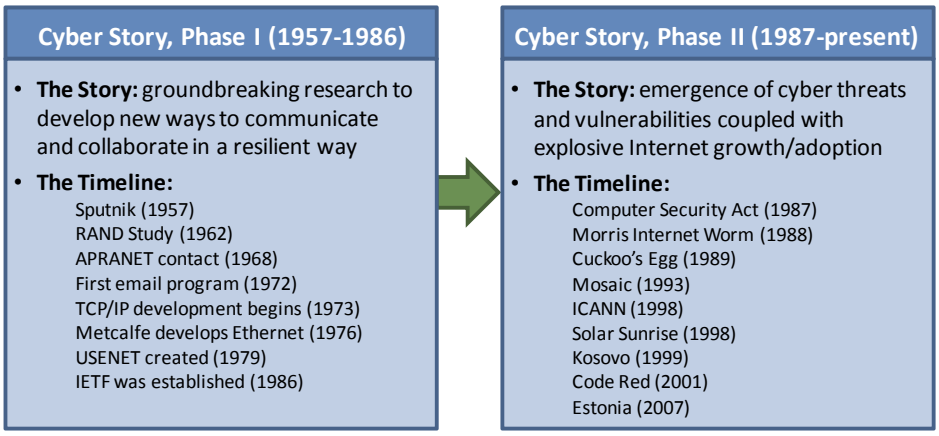

Figure 1. The Two Phases of the Internet's Issue History [5] [6]

Events in the late 1980s, however, would introduce vital change points—the emergence of cyber threats and vulnerabilities. After a raucous debate between the Executive and Legislative branches over roles and responsibilities for computer security, President Reagan signed the *Computer Security Act* in 1987. In 1988, the Morris Internet Worm is released and quickly self-replicates across the Internet, causing major disruptions. In response, the Defense Department creates the Computer Emergency Response Team at Carnegie Mellon University. In 1989, Stanford University professor Cliff Stoll publishes the *Cuckoo's Egg,* which detailed the real-life penetrations into US systems by a German hacker.

Two mega-trends dominate this second phase. The first is exponential growth in the number of hosts, users, computing power, and network capacity. For example, in 1984 there were 1,024 hosts worldwide; by February 2008, this number grew to more than 500 million.[6] Steep, explosive growth curves in these areas were accompanied by a growing military, economic, and societal dependence on the Internet and computer networks that permeate nearly every aspect of our lives. The second trend is the dramatic increase in cyber threats and vulnerabilities. During this period, cyber attacks grow in terms of *velocity* (speed of transmission), *volume* (attack frequency), *virulence* (impact, both direct and cascading), and *vector* (types of actors with the capability to launch attacks). The 2007 Estonian cyber attacks validated the dangers associated with the mix of growing dependencies, threats, and vulnerabilities. As one of the most wired societies in the world, Estonia was particularly vulnerable to this type of attack by a determined adversary employing hacking tools as the weapon of choice.

Before turning to consider historical analogies that might assist decision-makers formulate strategies and options for cybersecurity, Figure 2 outlines what we consider (at a high-level) known, unclear, and presumed about the cybersecurity issue of today.

What is Known	What is Unclear	What is Presumed
• Cyber threats, vulnerabilities, and risks continue to grow in terms of velocity, volume, virulence, and vector • Nation-states and non-state	• How grave is the threat? • Will next generation Internet technologies and applications be more secure? • Is there sufficient political will	• The United States will retain a key leadership role in governing and influencing the Internet • Nation-states are a more

actors are investing in cyberwar capabilities • Decreased resources are needed to develop cyberwar capabilities • Internet access and network capacity will continue to grow—with Asia becoming a more influential actor • Attribution complicates response and deterrence	(US, global) to address cybersecurity issues? • What types of policy approaches (regulation, market forces, international agreements, others) can change the current security conditions of the Internet?	serious threat than non-state actors • Cyberwar is low risk and high reward • Increased public-private cooperation will improve security

Figure 2. For today's cybersecurity challenge, what is known, what is unclear, and what is presumed

3. A Framework to Explore Cyber Analogies

The use of analogies is rampant in cybersecurity—and this should come as no surprise. Neustadt and May note throughout their text that analogies are most often used when issues are complex and decisions time constrained. Cybersecurity is an enormously complex issue with high tech threats and vulnerabilities, a community jargon that appears to layman as science fiction, attacks that appear with no warning, and a dizzying array of potential adversaries. Moreover, we live in a fast adapting socio-technology environment where users routinely change their favorite "killer applications" on an accelerated cycle, opening new doors of vulnerability.

While Cyber Pearl Harbor is perhaps the most prevalent historical analogy used to describe the cybersecurity challenge, others (such as Cyber 9/11 and Cyber Katrina) are being used with increasing frequency. Beyond these, some experts point to the need for a "Cyber Manhattan Project" or a cyber legal convention modeled after the Law of the Seas. Still others believe we are in the beginning phases of a "Cyber Cold War"[2] and most recently one cyber expert spoke of the need for a "Cyber Monroe Doctrine."[7]

Figure 3 depicts a framework to help sort through a plethora of analogies that might apply to cybersecurity. This model is built along two axes. The vertical axis divides those analogies motivated by *inspiration* (hope and possibility) versus those motivated by *desperation* (fear and danger). Consider, for example, the contrast between efforts to deploy the telegraph versus preparations for the Y2K software vulnerability. The former was motivated by a desire to speed communications across an unwieldy continent and to facilitate transatlantic communications; the latter driven by a time-certain fear of a major technological calamity. The horizontal axis divides analogies where change is *systematic* (linear, evolutionary) versus those where change is *disruptive* (transformative, revolutionary). For example, both the 9/11 attacks and the outbreak of the First World War were events that significantly altered the course of history. The former was a disruptive event occurring with little warning and of a scale not imagined, the latter a product of a system of mobilization and planning that made war unavoidable once a chain of events commenced (and of a scale not imagined).

[2] Panel at the 2009 RSA Security Conference entitled, "Is There A Cyber Cold War?"

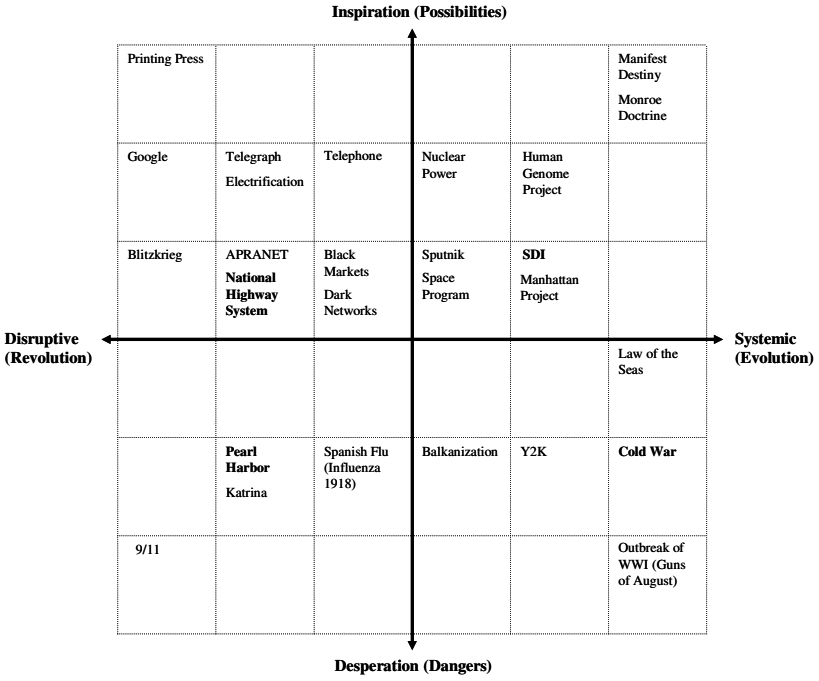

Figure 3: Framework to Analyze Cyber Analogies.

The remainder of this paper focuses on analyzing four analogies, one from each of the four quadrants of our framework: the Strategic Defense Initiative, the Cold War, the National Highway System, and Pearl Harbor. Each will be explored for its likenesses and differences to today's cyber issues.

4. The Strategic Defense Initiative (Inspiration, Evolution)

4.1. Overview

During the height of the Cold War, President Reagan proposed the developed of the Strategic Defense Initiative (SDI). Commonly referred to as the Star Wars program, SDI was envisioned as a system and capability to destroy Soviet Intercontinental Ballistic Missiles (ICBMs) while in flight in outer space. This proposed defensive shield held the potential of negating the carefully constructed logic of Mutually Assured Destruction (MAD) and conferring the United States a strategic military advantage over the Soviet Union. The mere threat of SDI forced the Soviet Union to respond by investing increased resources into its military programs in an effort to overcome the purported defensive shield constructed by the SDI. While SDI was never deployed or even proven to be technically feasible, the Soviets were compelled respond and many analyst believe the economic costs associated with this military buildup in response to SDI were a contributing factor to the downfall of the USSR.

While SDI provoked an offensive response from the USSR, the threat of cyber warfare has prodded the US to commit investments toward improving its cyber defense

posture. The Bush Administration's Comprehensive National Cybersecurity Initiative (CNCI) is reported to have allocated close to $30B over the life of the program [8]; and this may, in fact, only represent a fraction of the resources required to protect the US from a cyber attack of national significance.

Despite the recent cyber attacks against Estonia and Georgia, the threat of large-scale cyber warfare between states is still theoretical. To counter the potential of this threat, the US has invested increased amounts of resources (both public and private expenditures) into cyber defenses designed to protect critical infrastructure—the purported targets of any cyber attack of national significance. As cyber defenses are not static and must constantly be monitored, evaluated, and improved in order to counter determined adversaries, resources must be committed over the long-term. This point is exacerbated by a fact of life in cyberspace—today, the balance strongly tilts toward the offense, where the ability to conduct offensive operations is cheaper, easier, and more effective in comparison to the high costs of mounting credible defenses.

4.2. Similarities and Differences

The similarities between SDI and cyber warfare lie in the responses to perceived threats. In both cases, the efficacy of the strategies and tactics were unproven. In the case of SDI, it was not clear the system would ever work—but the USSR could not take the chance that it might. Similarly, there may be open questions about whether a large-scale cyber attack might work over a sustained period of time against US military and infrastructure targets—but the US cannot take the chance that it might. Another similarity between these analogies is the relative costs of offense to defense. In the Cold War, the ability to produce nuclear missiles and other delivery systems was relatively inexpensive and certainly less expensive than trying to develop defensive systems that would be full-proof. Today in cyberspace, developing offensive capabilities is inexpensive, especially compared to the enormous costs of developing cyber defense-in-depth strategies.

The obvious differences between SDI and cyber warfare center on their application. SDI was inherently defensive in nature, whereas cyber warfare is perceived as primarily a stealthy, offensive weapon. Further, SDI held the potential to completely destroy the existing strategic paradigm of Mutually Assured Destruction and dramatically titling the global balance of power. Cyber warfare is still a new, yet-to-be-defined strategic paradigm where questions of balance of power are complicated by the roles and capabilities of governments, private corporations, and a host of non-state networks of actors (terrorists, organized crime, other dark networks).

4.3. Lessons That Can Be Drawn From This Analogy

SDI never actually worked or was deployed against the Soviet nuclear arsenal. And yet it has three important lessons for those who seek to develop cybersecurity strategies. First, it was a program largely motivated by inspiration. Always the eternal optimist, Reagan sought to find a solution that helped the world escape the horrors of Mutually Assured Destruction (MAD). Second and related, SDI did not accept the notion that the offense would always trump defense in the nuclear world. The entire MAD concept rested on the fact that during any nuclear exchange, both sides would retain sufficient offensive force to destroy the other. SDI was a bold move to change that paradigm. Third, in doing so, the US raised the costs for the offense. Today in cyberspace, the

generally held view is the offense trumps defense with cost being the primary differentiator—it costs billions to erect defense-in-depth in cyberspace, and only thousands to attack it. However, SDI shows that it may be worth investigating strategies that seek to significantly increase the costs of the offense rather than trying to build the perfect defense.

5. The Cold War (Desperation, Evolution)

5.1. Overview

According to McAfee's 2007 Virtual Criminology Report, we are in the midst of a "cyber cold war." Specifically, the report states "attacks have progressed from initial curiosity probes to well-funded and well-organized operations for political, military, economic and technical espionage."[9] The analogy between the modern day cyber era conflict and the cold war conflict between the Soviet Union and the United States is primarily anchored in the idea that powerful nation-states are competing for influence and power without resorting to a direct conventional or nuclear war.

5.2. Similarities and Differences

The cyber as a Cold War analogy is ripe with similarities. The most obvious parallel between the Cyber and Cold War eras is the central role of espionage. The Department of Homeland Security's U.S. Computer Emergency Readiness Team received 37,000 reports of attempted breaches on U.S. Government and private sector systems, which included 12,986 direct assaults on Federal agencies in 2007 [10]. In addition, there were more than 80,000 attempted attacks on Department of Defense computer network systems. Countries such as China and Russia have been publicly implicated in many of these cyber attacks against US military cyber assets. In fact, Major General William Lord—the Commander of Air Force Cyberspace Command, has publicly stated, "China has downloaded 10 to 20 terabytes of data from the NIPRNet already." This appears to parallel efforts during the Cold War, where the Superpowers each invested resources into the creation and maintenance of rival spy networks. These networks were primarily designed to gather intelligence in an effort to gain a competitive advantage in diplomatic, economic, informational, and military confrontations.

Despite these similarities, this analogy is far from a perfect fit. First, the Cyber Era is multipolar as opposed to the bipolar structure of the Cold War. While the United States remains an unparalleled superpower, a number of other nation-states are quickly emerging as potential rivals to the US. In addition, there are a number of non-state actors (most notably terrorist groups) that threaten to acquire the means to launch cyber attacks of equal or greater capability that some nation-states. From a military perspective, this has occurred because the "costs of entry" are low—developing and maintaining a cyber capability is (in relative terms) remarkably inexpensive.

That stands in stark contrast to the Cold War, where the US and USSR needed to invest tremendous resources including time, treasure, and knowledge in order to become nuclear powers and to retain rough technological parity with respect to nuclear and conventional military forces. According to the Brookings Institute, the US spent approximately $5.5 trillion dollars on the construction and maintenance of its nuclear arsenal. The cost of becoming of nuclear power was high in part because of the

tremendous capital investment required in the construction nuclear power plants, the physical weapons, and acquiring source materials.

In the Cyber era, organizations require only a fraction of these resources to become a "cyber power." According to a study conducted by the Naval War College and Gartner Inc. in 2002, it would require only five years and $200 million to execute a major cyber attack. [11] As the knowledge and the weapons, in the form of exploit code, required to conduct a major cyber attack has become increasingly available since the release of the Naval War College and Gartner study it is likely that such an attack could be carried out with less resources. The cost of a cyber warfare program is further reduced because there is very little capital investment required. Unlike nuclear weapons, cyber weapons are virtual and can be duplicated at very little cost.

5.3. Lessons That Can Be Drawn From This Analogy

The Cold War offers a powerful image, that of a protracted struggle between powers for political, military, and ideological supremacy. There are obvious similarities—the cat-and-mouse game of espionage the boils below the geopolitical surface; the proxy wars that may suddenly break out in cyberspace; and the importance of retaining technological superiority. There are obvious differences too—the Cold War was an ideologically-motivated, bipolar struggle between competing nation-states and the fear of MAD served as a governor on the actions of the two major actors.

However, one important similarity – and lesson to be drawn – is the close entanglement of economic, political, and security interests in devising a comprehensive strategy. In the Cold War, the US and USSR brought to bear all instruments of national power—economic, military, scientific and technological. In particular, the Mr. X telegram developed by George Kennan at the start of the Cold War outlined a comprehensive strategy where the US was able to bring all elements of its national power together toward a common objective, the containment of the USSR. A key predicate of that telegram was that conflict was inevitable between the two powers, and the U.S. required a proactive, comprehensive strategy to prepare for the characteristics of this new conflict. Given the new order being created in cyberspace – where the Internet touches all aspects of political, military, economic, and sociological life – perhaps one of the most important lessons from the Cold War is the idea of developing a Mr. X-like telegram for cyberspace that defines the boundary conditions for future conflict.

6. The National Highway System (Inspiration, Revolution)

6.1. Overview

In his 1955 State of the Union Address, President Dwight D. Eisenhower declared, "A modern, efficient highway system is essential to meet the needs of our growing population, expanding economy, and our national security." Nearly every aspect of this ambitious project sought to balance national security, public safety, and commerce as the country invested billions of federal dollars in road, bridge, and tunnel construction. The resulting National Highway System represented a remarkable achievement. More than 50 years after President Eisenhower's address, our automobile culture has fundamentally transformed America's way of life.

6.2. Similarities and Differences

A historian looking back 100 years from now might rightly proclaim the National Highway System and the Internet as two of the world's greatest cultural achievements, the Great Infrastructure Wonders of our age. There are numerous similarities. First, both represented significant step improvements in citizen access and mobility. Second, both were children of the Cold War. Eisenhower, fresh from his WWII experience in Europe where transportation and logistics were vital in achieving victory, the National Highway System was designed in part to ensure the US could quickly mobilize its forces and deploy them to Europe if the Cold War turned hot. The genesis of the Internet was, in part, efforts to build a resilient command and control system that could withstand a Soviet nuclear strike. Third, both infrastructures led to sudden—and unpredictable—cultural and societal shifts. In less than a decade, the National Highway System facilitated the growth of suburbs and accelerated the emptying of center cities. Within a decade, the Internet has created global online communities, perhaps a new form of "cyburbanization."

There are two additional, more subtle similarities. First, both infrastructures emerged from a combination of inspiration and desperation. In selling the idea of the National Highway System, President Eisenhower often changed his message to suit the audience. When speaking to war veterans, he emphasized security. When talking to Chambers of Commerce, he focused on the need to continue post-war economic growth. When talking to the Rotary Club, he stressed the need to reduce the number of highway fatalities. While the Internet has its roots in military resiliency, the research community helped guide and shape its development to promote greater collaboration. Second, both represented significant shifts in how the United States built infrastructures. Prior to Eisenhower, the States all developed their own roads and highways with differing standards and approaches. Eisenhower's approach "federalized" highways, leading to unchartered territory in terms of nationwide investments. Similarly, the Internet's development is truly unique as an infrastructure. Most US infrastructures began as regulated monopolies (telephony, power, banking, air travel) and were slowly deregulated. The Internet has never been regulated—and with its global reach and impact, has entered equally unchartered territories.

The differences between these two infrastructures are easily identifiable. One was US-centered; the other is global. The National Highway System was a top-down, Federally driven program; the Internet is, by its very nature, decentralized and governance is perhaps best described as ad hoc. Perhaps most germane, the National Highway System never could be viewed as the avenue of attack against the United States—it was a force multiplier and enabler. Cyberspace can and has offered some of the same features to the US as a force multiplier. But cyberspace also introduces (through technical vulnerabilities in networks) the means by which an adversary may attack and disrupt critical military and infrastructure operations.

6.3. Lessons That Can Be Drawn From This Analogy

Today, debates in cyberspace are far broader and more encompassing than cybersecurity. In the United States, we see a need to respond to our vulnerabilities to growing cyber threats and develop the ability to attribute attacks to better deter, prevent, and respond to them. At the same time, many of our citizens (and those of other countries) have expectations of online privacy. Beyond this, since entering office, the

Obama Administration has pushed for greater Internet access, online collaboration, open government, and transparency. At the international level, we are potentially entering a new era of Internet governance and influence where other nations share a common interest in limiting perceived U.S. dominance of the Internet and its governance structures.

While many of the analogies used today in the U.S. for cybersecurity have at their core a message of impending danger, President Eisenhower was able to demonstrate how to strike a balance in his messaging around the National Highway System. His message was large dose of inspiration—to lower highway fatalities, to create jobs, to improve the post-war economy—coupled with a tinge of danger, to remain vigilant should the US have to mobilize to Western Europe in the event of a communist invasion. Equally important, his approach blended the introduction of revolutionary concepts (e.g., a stronger Federal role in transportation) with evolutionary steps (e.g., the use existing State apparatus' to facilitate the flow of money). Any significant effort to address cybersecurity issues will require a similar approach—introducing new constructs, ideas, and strategies for cyber laws, Internet governance, etc., coupled with working within the existing confines of the system (at least initially).

The National Highway System analogy also offers a secondary lesson—that these types of decisions can carry a long tail and produce many unanticipated outcomes. Our transition en masse to automobiles changed our society (suburbs, summer vacations, an emphasis on automobile safety), changed our economics (dependence on foreign oil, rise of trucking), and our environment in ways President Eisenhower could never have predicted. Ultimately, this makes the case for adopting a balanced approach like that Eisenhower assumed in the mid-1950s: part inspiration, part desperation; part revolutionary, part evolutionary.

7. Pearl Harbor (Desperation, Revolution)

7.1. Overview

On December 7, 1941, the Imperial Japanese Fleet launched a surprise attack against the US fleet anchored at Pearl Harbor. The intent of this attack was to neutralize US military power in the Pacific as Japan continued to expand its empire.

7.2. Similarities and Differences

Many similarities exist between what happened at Pearl Harbor and what many experts believe theoretically could happen in cyberspace. Among the most obvious is the introduction of new strategies, tactics, and doctrine. During the First World War, aircraft were used to perform a variety of military missions, including bombing runs. As early as the 1920s, Navy's from across the globe began to recognize the potential of airpower as a new, offensive form of naval warfare. For example, General Billy Mitchell theorized that battleships could be sunk via an air bombing campaign. In the 1930s, Japan, the U.S., and Great Britain began to add aircraft carriers to their naval fleets. Theory was put to the test in November 1940, when the British launched the "first all-aircraft naval attack in history, flying a small number of aircraft from an aircraft carrier in the Mediterranean Sea and attacking the Italian fleet at harbor in Taranto. The effect of the British carrier-launched aircraft on the Italian warships

foreshadowed the end of the 'big gun' ship and the rise of naval air power." [12] The Japanese studied this raid and built a war plan designed to strike at the heart of US military power in the Pacific, the US Naval Fleet anchored at Pearl Harbor. One can argue a similar progression has taken place in cyberspace, from the initial use of electronic warfare techniques during Operation Desert Shield/Storm through the spike in hacking attacks during the 1990s and 2000s witnessed in the US Government to the more coordinated and sophisticated cyber attacks launched against Estonia and Georgia (the modern day Taranto?).

As noted earlier in this paper, other similarities exist. This includes the notion of strategic surprise, with an enemy launching a no warning attack with devastating consequences and the desire to neutralize US military advantages. The general sense that intelligence and other information exists to point to the attack, information that may be overlooked or misunderstood if not placed in the correct strategic context.

At the same time, important differences exist in these two situations. First and foremost, in the case of Pearl Harbor, the enemy and its intentions were well known. For more than a decade (following the Japanese invasion of Manchuria in 1931), tensions between the US and Japan spiked. In previous conflicts, Japan had used strategic surprise to gain military advantage. The US was well aware of Japan's force projection capabilities given its large fleet of aircraft carriers. There would be no confusion about which adversary had determined to strike the United States in the Pacific. The same cannot be said in cyberspace, where the lack of attribution adds considerable complexity. Not only is strategic surprise possible in cyberspace, but it is also possible to veil the source of the attack. Complicating matters, there may be a number of actors (rival nation-states, rogue states, terrorist groups, and others) with an interest in not only launching a surprise attack, but potentially even attempting to stimulate conflict between the victim and a third party. For example, a rogue state might attempt to launch a large-scale cyber attack against the United States and make it appear the attacks emanated from another country.

Second, Pearl Harbor required a great deal of lead time and risk for Japanese planners, moving a giant fleet across half the Pacific Ocean while concealing their movements. At best, discovery of a large Japanese fleet would have removed plausible deniability about Japanese intentions. At worst, it could have resulted in military disaster, as it ultimately did at Midway. In cyberspace, concealment and plausible deniability are not only possible but relatively easy to achieve and the speed at which DDoS and other attack techniques can be produced eliminate much of the lead time that might result in an inadvertent discovery. In other words, strategic surprise in cyberspace may prove far easier to achieve than in other historic examples, such as Pearl Harbor or the Israeli attacks commencing the Six-Day War.

7.3. Lessons That Can Be Drawn From This Analogy

A critical lesson to be drawn from the Pearl Harbor analogy points back to a recommendation by Neustadt and May—understand the timeline and start it at the earliest possible point. The Pearl Harbor analogy is often used to describe either a successful surprise attack and/or the failure of a country to anticipate an attack despite weeks and even months of mounting evidence. Thus, with respect to cybersecurity today, the analogy is often used to create a sense of imminent danger. But when does the Pearl Harbor timeline begin? Should one think of the Pearl Harbor analogy beginning in the fall of 1941 as negotiations between Japan and the US begin to

breakdown? Does the timeline begin with the Japanese invasion of Manchuria, which signaled larger imperial ambitions? In the 1920s with Billy Mitchell, or over the fields of Flanders during WWI when aircraft first played critical roles in military operations? Or does it begin in 1890 when Alfred Thayer Mahan published The Influence of Sea Power Upon History, 1660-1783, a book that was extraordinarily influential with two generations of Japanese naval strategists? From the Japanese perspective, does it begin with the arrival of Admiral Perry and his black ships in 1853?

Choosing the appropriate timeline for Pearl Harbor can greatly change the lessons cybersecurity strategists might learn from—particularly in identifying relevant historic parallels and how change points (Taranto, Estonia) altered decision-makers perceptions and actions.

8. Conclusion: The Power and Perils of Cyber Analogies

Analogies are powerful instruments in the hands of decision-makers. They can: create and cement an image in the public's mind about an issue; prove useful in sorting through the details of a crisis to find key insights; support efforts to develop sound strategies and well-reasoned policy options; and help leaders anticipate the future, ripple effects of decisions made today. The paper does not define the "best" historical analogy for decision-makers to consider in formulating cybersecurity strategies. A number of factors (e.g., new threats, breakthrough technologies, changing business conditions) can dramatically alter how the cyber issue may unfold—and, consequently, which analogies may best apply. The goal of this inquiry was to test our thesis by creating a framework that puts future cybersecurity events or crises in context—and to help decision-makers select the most relevant and applicable historical analogies. In doing this analysis, we've reached four conclusions.

First, no single analogy will suffice in considering the complex challenges of cyberspace. While the cyber Pearl Harbor analogy is rich in imagery, connoting urgency, it may not be applicable to the full range of cyber scenarios that may confront the US and the world. Moreover, it holds the potential to produce a dangerous blind spot—we may wait for the "big one," a large-scale surprise attack while suffering from "pinpricks" that, in the end, have a far more debilitating and degrading impact on our networks (and public confidence).

Second, our examination of historical analogies reveals those that strike a balance between inspiration and desperation tend to produce the most permanent, lasting results. The Strategic Defense Initiative, the Manhattan Project, the National Highway System, and even the creation of the Internet itself have their roots in a mixture of inspiration (e.g., to destroy incoming ICBMs, to end WWII quickly, to reduce highway fatalities, and to promote collaboration across a research community) and desperation (e.g., to counter a growing Soviet nuclear arsenal, to develop the Atomic bomb before Germany and Japan, to enable rapid mobilization should the Cold War turn hot in Europe, and the ensure command and control resiliency in the worst case event of a nuclear war).

Third, today many of the analogies used to describe cyber rest at the extremes of our model. Again, this is not a surprising outcome—these analogies present vivid images that grab the public's attention. At the same time, continuously planning only for the worst-case scenarios can erode public support when these events don't occur or their effects are far less than predicted. The Y2K issue offers an excellent illustration of this. The reality is that early vigilance and a date certain event helped the world prepare

for this software glitch. The perception, however, was that Y2K was anticlimactic and created more skepticism around gloom-and-doom cyber warnings.

Fourth, one of the most important lessons from *Thinking in Time* is understanding the correct, appropriate timeline of an issue: when did this issue start? What are key change points or trends? The authors argued these timelines should start at the earliest possible date to fully understand the historical context. For example, one could examine the analogy of 9/11 in multiple contexts—the year leading up to the attacks; a timeline starting with the 1993 bombing of the World Trade Centers; or beginning with the 1982 US Marine barracks bombing in Lebanon. In this case, the same event can produce different timelines (and resulting historical lessons) that may ultimately change the focus and core meaning of an analogy. For leaders exploring the future of cyberspace or dealing with an active cyber incident, starting with the right timeline may prove critical in making good decisions.

References

[1] National Counterintelligence Executive Joel Brenner in a January 2009 CBS News television interview (http://www.dni.gov/interviews/20090118_interview.pdf) and by Michael Chertoff, Secretary of Homeland Security at 2007 RSA Conference (http://www.theinquirer.net/inquirer/news/1021392/cyber-attacks-significant)

[2] Remarks by Paul Kurtz on February 18, 2009 at the 2009 Black Hat conference in Washington, DC (http://www.blackhat.com)

[3] Neustadt, Richard E. and May, Ernest R., Thinking in Time: The Uses of History by Decision Makers, The Free Press, New York: 1986.

[4] Bruno, Greg, The Evolution of Cyber Warfare, The Council on Foreign Relations, February 28, 2008 (http://www.cfr.org/publication/15577)

[5] History of the Internet, http://www.davesite.com/webstation/net-history.shtml

[6] The Hobbes Internet Timeline (http://www.zakon.org/robert/internet/timeline/)

[7] Testimony by Mary Ann Davidson, Chief Security Officer at Oracle, to the United States House of Representatives Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Source: http://homeland.house.gov/SiteDocuments/20090310143850-78976.pdf

[8] Andy Greenberg, Sketching Obama's Cyberplans, Forbes, Feb 20, 2009. http://www.forbes.com/2009/02/20/paul-kurtz-security-technology-security_kurtz.html

[9] Virtual Criminology Report – Cybercrime : The Next Wave, McAfee. Source: http://www.mcafee.com/us/research/criminology_report/default.html

[10] Jeff Bliss, "Dearth of Technical Experts Leaves US Open to Cyber Attack, Panel Says," Boston Globe, March 20, 2009.

[11] Margaret Kane, US Vulnerable to Data Sneak Attack, CNET News, August 13, 2002. Source: http://news.cnet.com/U.S.-vulnerable-to-data-sneak-attack/2100-1029_3-949605.html

[12] Source: http://wapedia.mobi/en/Battle_of_Taranto