

# PROTECTING CYBERSPACE AND THE US NATIONAL INTEREST

BY AKI J. PERITZ & MICHAEL SECHRIST



HARVARD Kennedy School

**BELFER CENTER** for Science and International Affairs

SEPTEMBER 2010

## Protecting Cyberspace and the US National Interest

Aki J. Peritz & Michael Sechrist

September 2010

---

### Executive Summary

*We assess 'protecting cyberspace,' while extremely important, does not rise to the level of a first-order national security challenge as countering nuclear proliferation and defeating al Qaeda because most threats to America's digital infrastructure do not undermine core security interests. Most challenges to cyberspace – such as cybercrime, cyberespionage and cyberterrorism – can be ably handled by domestic law enforcement and intelligence services. The exemption to this assessment would be so-called 'cyberwar' between nations; however, a sophisticated, serious digital attack on the US would likely be attributable and carried out by states in concert with conventional kinetic options – acts of war that would provide the US the legal, moral, and military authorities to respond.*

*Recognizing cyberspace's role as a medium for security, communication and commerce, we detail five ways that the US can better protect cyberspace: establish a comprehensive strategy, maintain strong deterrents, strengthen public-private partnerships; avoid bureaucratic overreach; and forge an international consensus. By doing so, policymakers can make better-informed decisions about how to properly defend the country from threats to America's digital infrastructure.*

---

The US government has recently concluded that protecting cyberspace is critical to national security, and that challenges to the American digital infrastructure are threats of the first order. Various strategic US documents, such as the Department of Defense's 2010 *Quadrennial Defense Review* (QDR), the White House's 2009 *60-Day Cyberspace Policy Review*, the Office of the Director of National Intelligence's (ODNI) 2009 *National Intelligence Strategy* and the Department of Homeland Security (DHS) 2009 *National Strategy to Secure Cyberspace* all concur that protecting cyberspace—the globally-interconnected digital information and communications infrastructure<sup>i</sup>—has become an urgent priority.

To this effect, the Obama Administration in May 2010 released its *National Security Strategy* (NSS), a document that for the first time included 'securing cyberspace' as a *vital* national interest.<sup>ii</sup> Although the NSS provided little further guidance on the topic, the President in a subsequent press conference deemed US

digital communications a “strategic national asset.”<sup>iii</sup> “Protecting this infrastructure,” he said, “will be a national security priority.”<sup>iv</sup>

We disagree. We assess ‘protecting cyberspace,’ while important, does not rise to the level of first-order national security challenges as countering nuclear proliferation, fostering peace in the Middle East and defeating al Qaeda. Instead, most threats to America’s digital infrastructure—such as *cybercrime*, *cyberespionage* and *cyberterrorism*—do not undermine core security interests, and can be ably handled by domestic law enforcement and intelligence services. The exemption to this assessment would be so-called full-scale ‘cyberwar’ between nations; however, cyberwar should be considered a subset of conventional war, since significantly undermining America’s digital infrastructure could be interpreted as an act of war. A true cyberwar situation, then, would most likely cause the US to respond as if it were attacked by conventional means.

We reached a set of conclusions by first identifying what indeed are vital national interests; second, by establishing what are (and are not) the first-order cyberspace challenges facing the nation; third, by determining the most effective means to defend and protect US assets; and finally by analyzing how international treaties may provide the best protection possible in cyberspace.

### **What are America’s National Interests?**

The defensive security interests of a nation-state generally include the ability to overcome adversaries, maintain territorial integrity and prevail in physical conflict. Benedict Anderson’s definition from *Imagined Communities* of a nation works well, as it is “an imagined political community – and imagined as both inherently limited and sovereign,”<sup>v</sup> and is constrained by certain physical and political parameters. A nation’s limited, sovereign abilities to control – much less govern—cyberspace then proves to be problematic. A discussion of American national security interests in cyberspace—namely, a specific nation-state’s interests in an ungoverned virtual space with no borders, no government and few regulations—poses numerous philosophical and political quandaries such as: who are ‘we’; who are ‘they’; how can ‘we’ protect ourselves; what rights and powers can ‘we’ demand in a law-of-the-jungle digital environment; and so on.

These questions (and answers) impact US security requirements. From the US defense perspective, equally fundamental queries arise: who is the ‘enemy’; how ‘we’ can neutralize them; and most importantly, whether stymieing that individual or group is worthy of national-level efforts. Complicating matters is that since much of the global economy is now Internet-based, most major actions undertaken by a nation-state in the digital realm will have long-lasting economic and political ramifications.

Despite these nagging questions, nations are bound to act when their national interests are at stake – even in the nebulous world of cyberspace. This then raises the larger question: what indeed are *vital* national interests?

In 2000, the bipartisan *Commission on America's National Interests* tried to provide an answer.<sup>vi</sup> The Committee defined “vital national interests” as those “strictly necessary to safeguard and enhance Americans’ survival and well-being in a free and secure nation.”<sup>vii</sup> In the decade that followed, the Bush and Obama Administrations have produced numerous strategic documents that reflect upon presumed vital national interests, with varying degrees of specificity.<sup>viii</sup> After examining these strategic national security documents produced during this time, three overall themes emerged:

- Defeat adversaries, win conflicts, and defend US citizens;
- Prevent enemies from acquiring and using Weapons of Mass Destruction;
- Prepare for emerging threats and plan for contingencies.

Whether these overall themes encompass all vital security threats is subject to debate; after all, policymakers’ ideas of what constitutes a national security challenge have changed over time and circumstance. For example, bootlegging and bank robberies were considered to be national security threats in the not-too-distant past. Nonetheless, the aggregated wisdom of current government documents suggests these topics are the most important issues facing the US today.

### **Protecting Cyberspace as a *Vital* National Interest?**

*The Commission on America's National Interests* selected ‘Cyberspace and Information Technology’ as an emerging issue, stating “the US critical infrastructure [should] be reasonably resistant to concerted, sophisticated cyber-attack.”<sup>ix</sup> The report noted “information systems are the vital backbone upon which American financial, energy, transportation, defense and telecommunication infrastructures depend...the US is so dependent on these systems, and the existing vulnerabilities are so pervasive, that enhancing resilience of American infrastructure information systems is a vital national concern.”<sup>x</sup>

Numerous intelligence and defense organizations have agreed with this line of analysis. For example, the Pentagon’s February 2010 QDR stated “A failure by the Department to secure its systems in cyberspace would pose a fundamental risk to our ability to accomplish defense missions today and in the future.” One high-ranking Pentagon official noted in recent Congressional testimony:

*It is impossible to overstate the DoD's dependence on cyberspace. DoD's information networks provide command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.<sup>xi</sup>*  
(italics added)

Along similar lines, the ODNI in August 2009 argued:

...the architecture of the Nation's digital infrastructure, based largely upon the Internet, is neither secure nor resilient. Nation-states and non-governmental entities are compromising, stealing, changing, or destroying information, and have the potential to undermine national confidence in the information systems upon which our economy and national security rests.<sup>xii</sup>

DoD and ODNI officials are correct in stating that protecting cyberspace is important to the functioning of their bureaucracies. However, based on core national security requirements, critical national interests in cyberspace are only threatened when an actor has or uses the ability to launch a comprehensive, civilization-changing attack on the US or our allies that can kill many Americans, or severely impact the ability of major global systems to function for an extended period of time. Otherwise, the US will not react with a national-level response.

As of now, nation-states remain uniquely capable of executing a comprehensive cyberattack against the US because only nations have the resources and trained personnel that can be directed to overwhelm American defenses. While popular perceptions remain that individuals can commit damage in cyberspace on a massive scale, the reality is that striking the US in a coordinated, strategic manner is an extremely complicated endeavor without state sponsorship. This complexity drives the risk of such attacks to low levels, low enough to avoid deeming such events vital national security threats. Hence, a sophisticated, systemic attack on the US via cyberspace will likely be carried out by nation-states in concert with conventional kinetic options—acts of war that would provide the US the proper legal, moral, and military authorities to respond. A massive cyberattack could then be considered a prelude to conventional war.

Nonetheless, countries rarely launch large-scale attacks without some larger national goal in mind; thus far, this presumption has held true in cyberspace. For example, during the mid-2008 Russia-Georgia conflict, attacks on Georgian

government and civilian digital infrastructure occurred while Russian military forces simultaneously penetrated Georgian territory. Similarly, the late-2007 cyber-jamming of Syrian radar installations—a vignette that opened Richard Clarke’s book, *Cyberwar*—happened just as Israeli warplanes streaked across the border and bombed a suspected nuclear facility. Thus, a comprehensive cyberattack against the US will be clearly attributable to another country, as nations acting with hostile intent will first signal their intentions through overt military or diplomatic means.

## Secondary Challenges in Cyberspace

This is not to say that other challenges in cyberspace are not serious. They certainly are and should be treated as such. Reporting as far back as the late 1960’s shows that the DoD recognized the threats and have worked to prevent aspects of it coming to fruition. In 1967, the DoD created a task force to study computer vulnerabilities. By 1970, the ‘Defense Science Board Task Force on Computer Security’ published its findings, with recommendations for protecting classified information on military systems.<sup>xiii</sup> In 1990, the National Research Council published an updated report, stating, “Increasingly, America depends on computers...Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb...We must attempt to build computer systems that are secure and trustworthy.”<sup>xiv</sup> A 1997 report for the White House reiterated similar themes, noting, “Today, a sustained attack on the Internet can have a serious impact on other critical infrastructures in the United States... It is essential to take steps now to ensure that the US can resist Internet attacks and that the Internet can continue to perform critical functions in the face of an attack.”<sup>xv</sup>

This begs the question: if America’s digital infrastructure has had serious vulnerabilities for at least forty years, why is protecting cyberspace only now considered a vital national security interest?

One argument is that the ever-expanding number of Internet users—an estimated two billion people will be online by 2013<sup>xvi</sup>—increases potential challenges to national security. Indeed, infected, compromised computers remotely controlled by a third party called *botnets*<sup>xvii</sup> have proliferated, wreaking havoc on individuals, companies and governments. Another argument is that cyber-criminality and espionage have markedly increased in recent years, harming the US economy and defense structures and therefore must be part of a hidden ‘cyberwar.’ Certainly, the amount of US electronic data stolen by outside actors has reached significant proportions; for example, someone in 2009 pilfered several terabytes of design and electronic system-related data from the Pentagon’s \$300 billion Joint Strike Fighter program.<sup>xviii</sup>

While these arguments underscore the fact that the US faces serious threats, affixing “cyber” as a prefix does little more than give these issues the gloss of 21<sup>st</sup> century urgency. In every other vital interest listed or categorized by the latest NSS, it is clear that the US would wage war – or at the very least commit to wide-scale, long-lasting violence – in pursuit of the objective. In terms of the vast number of challenges to protect cyberspace, however, it remains doubtful that the US would launch a full-scale military operation such as Operation Enduring Freedom or Operation Iraqi Freedom to defeat the threat. In fact, no U.S. official has yet to confirm that a conventional attack might follow a significant cyber attack; for now, no declaratory cyber-policy has been made, leaving only outsiders to speculate.

For example, it would be extremely unlikely that US will go to war or commit large-scale forces to thwart *cybercrime*.<sup>xxix</sup> Obama’s senior director for cybersecurity in April 2010 stated “the predominant threat we face is the criminal threat – the cybercrime threat in all of its varied aspects.”<sup>xxx</sup> So far, the US has approached this problem as a law enforcement challenge, and not as a first-order national security issue for the country.

This criminal activity is indeed profitable – the FBI recently determined that US industry lost some \$400 billion to computer-based crime.<sup>xxxi</sup> Other analysts estimated cybercrime has cost global industry some \$1 trillion in intellectual property violations and data loss.<sup>xxii</sup> Moreover, most cybercriminals escape punishment – the General Accountability Office recently estimated that only 5% of these individuals are ever arrested and convicted.<sup>xxiii</sup> However, it is not evident that this highly lucrative and often unpunished activity is actually a national security threat.

*Cyberespionage* is another security concern, but only as a tool employed by nation-states in a larger effort to steal secrets. Using the Internet is merely an updated version of gleaning your adversary’s secrets through clandestine means.

Just as cyberwar is a subset of physical warfare, cyberespionage is an expanding digital wrinkle in long-established international relations between countries. As such, some officials do not seem to believe this is a fundamental threat facing the US. For instance, former NSA Director Michael Hayden recently noted that cyberspying is a “normal espionage thing that routinely happens between states.”<sup>xxiv</sup> With cyberespionage, however, terabytes of information can be extracted almost overnight. In fact, several agencies, including the Department of State, have lost several terabytes of information.<sup>xxv</sup> But in the vast majority of these cases, it appears unclassified networks are the main targets. In at least one instance, intruders accessed the Secret Internet Protocol Router Network (SIPRINET), the network that houses Secret-level information.<sup>xxvi</sup> There has been

no reporting of cyberespionage on the Joint Worldwide Information Communication System (JWICS), special access programs (SAP) or other compartmented information networks, where many of the nation's most sensitive intelligence and defense information reside. What is left unsaid is that the US also engages in espionage through digital means, so it is doubtful that the US will go to war to end the practice.

Furthermore, the ODNI's National Counterintelligence Executive (NCIX) judges spies working inside the intelligence system are the real threat, far more so than those who commit espionage from faraway computer terminals.<sup>xxvii</sup> This is because the truly important government secrets only exist on closed, classified networks, where only traitors within the system can extract them. The NCIX recently assessed, "Insiders have caused grave, long-term damage to national security. History has demonstrated the intent of foreign intelligence services and entities to penetrate the Intelligence Community and extract information through the use of a trusted insider – recruited or volunteer."<sup>xxviii</sup> The most significant, long-lasting espionage damage in recent times have resulted from moles like Aldrich Ames, Robert Hanssen, and John Walker – all individuals who worked from within the US intelligence structure. Thus, the inside threat will likely remain the primary concern for America's counterintelligence professionals, not the so-called cyberspy.

*Cyberterrorism* is, as of now, negligible as an Internet phenomenon. Depending on how the term is defined,<sup>xxix</sup> few if any actual 'cyberterror attacks' have occurred to date. Of course, terrorist groups use the Internet to disseminate propaganda, recruit followers and communicate among themselves,<sup>xxx</sup> but few if any actually carry out attacks via a computer system.

Even some counterterrorism experts outside the US believe the threat from cyberterrorists is overblown. "We have no examples of cyberterrorism yet," claimed retired Russian general Vladislav Sherstuyuk in April 2010. Sherstuyuk, who sits on Russia's National Security Council and leads Moscow State University's Institute of Information Security Issues further noted, "[The terrorist problem] is more about information that you can get from Internet... information about forthcoming terrorism attacks, so we can watch airport and railway stations to observe whether there are attacks or not."<sup>xxxi</sup>

For now at least, the US remains alert for the potential of cyberterrorism. Much like how the US Coast Guard patrols the physical shoreline, well-funded intelligence and military mechanisms attempt to defend the US digital coast. For instance, the DoD's new Cyber Command (CYBERCOM), in coordination with the FBI and DHS, has significant resources directed to frustrate this potential threat.

Finally, apolitical attacks upon the American digital infrastructure – *cybotage*, as coined by one 1996 study<sup>xxxii</sup> – pose challenges to the US. Cybotage can cause damage because national infrastructure components such as electrical grids are connected to the Internet via smart grids and supervisory control and data acquisition (SCADA) connections, and interrupting their inner workings can have negative effects. One example of such an attack occurred when hackers disrupted Brazil’s electrical grids in 2005 and 2007, although it remains unclear who carried out the attacks, or why they did it.<sup>xxxiii</sup> Malcontents have also disrupted local emergency response systems, caused gas pipelines to malfunction, and vandalized government and commercial websites.<sup>xxxiv</sup>

Still, the impact of such attacks is usually relatively contained; US civilization will not crumble due to these attacks, nor will it likely even be significantly degraded over an extended period of time. Of course, large-scale destruction affecting the well-being of civilians could occur should attackers continue to penetrate infrastructure systems – such as in the Brazilian power outage case. But these blackouts did not cause the fall of the Brazilian government, nor did they cause the Brazilian economy – one of the largest in the world – to collapse or even experience long-term difficulties.

In any case, the US has much larger infrastructure problems to contend with beyond hacker attacks. One expert recently noted that “many of the great public works projects of the 20th century – dams and canal locks, bridges and tunnels, aquifers and aqueducts, and even the Eisenhower interstate highway system – are at or beyond their designed life span.”<sup>xxxv</sup> A 2009 American Society of Civil Engineers (ACSE) report rated overall US infrastructure in “poor” condition, and stated that \$2.2 trillion in investment will be needed over the next five years to raise the overall infrastructure to a “good” condition.<sup>xxxvi</sup> With nearly \$82 billion spent in FY10 on information technology<sup>xxxvii</sup> and an estimated \$20 billion spent by the US government to secure cyberspace<sup>xxxviii</sup>, it pales in comparison to any figure in the trillions. So, while protecting US digital infrastructure has become a major concern for national policymakers, protecting the physical infrastructure that would undoubtedly cause civilian and military damage due to their malfunctioning or destruction – like America’s 47,000-mile interstate highway system, 80,000 dams, 104 commercial nuclear plants, 5,400 power plants and 600,000 bridges<sup>xxxix</sup> – should perhaps be just as urgent a priority for policymakers.

## To Defend and Protect

Protecting America's digital infrastructure are not just defense-related challenges, but also fragmented economic, political and social ones. A heavy-handed approach to securing cyberspace—relying primarily upon increased numbers of cybergates, cyberguards and cyberbureaucracy—would likely be counterproductive because a 'national security only' solution will adversely affect US business and entrepreneurship, possibly more so than the threats itself. This approach would also freeze the free-flow of creative ideas that have brought so much prosperity to millions of Americans.

Unfortunately, the federal government cannot provide total security to all places on the Internet. The US is an open, imperfectly networked country of 300+ million citizens who conduct business and personal interactions on both domestic and foreign servers. Even if the US was willing to clamp down on the free-flow of digital information—akin to China's recent Golden Shield Project, which filters electronic data through computer programs and human review<sup>xi</sup>—security threats and digital vulnerabilities would still exist. One would not have to search long to find that political dissidents, criminals and even American intelligence agents remain on the Chinese network, despite the best efforts of the local security services.

Hence, the US must strike a balance between the need for security and the need to maintain an open virtual world. The White House has noted that "Effectively addressing the fragmentary and diverse nature of the technical, economic, legal, and policy challenges will require a leadership and coordination framework that can stitch this patchwork together into an integrated whole."<sup>xii</sup> How then can the US government reasonably protect cyberspace without compromising its economic competitiveness and political values along the way? We have five recommendations to keep in mind when forging a long-term solution to these concerns:

*Establish a Comprehensive Strategy:* Effectively protecting US interests in cyberspace will only work as an integrated, whole-of-government strategy and not as a hodgepodge of delinked initiatives. The founding of the White House's new *Office of the Cybersecurity Coordinator*, informally referred to as the 'Cyber Czar', is a step toward crafting a better organizational structure than what is currently in place, so long as the appropriate civilian cyber-related organization, DHS's *National Cybersecurity and Communications Integration Center* and CYBERCOM are equal partners in protecting cyberspace. However, in many ways the directive to work together has been difficult to implement; as CIA Director Leon Panetta reflected wistfully in an interview earlier this summer,

“Frankly, [protecting cyberspace] hasn't been brought together in a unified approach.”<sup>xlii</sup>

The US government will have to make some difficult choices in terms of what indeed are and are not national-level cyber assets, based on a firm understanding of what are America's national interests and constraints. Given finite resources, vast swaths of American financial enterprise and government will not receive much federal assistance during a cyberattack, as protecting only the most critical digital infrastructure will take priority in the event of an emergency. This would be analogous to determining who would first receive inoculations during a pandemic – topping the list would be critical government workers, medical first-responders, law enforcement etc. If more time and resources become available, the circle of ‘protected’ individuals may expand. During a systemic cyberattack, the first ‘inoculated’ would be mission-critical actors – various governmental command-and-control structures, first-responders, etc. – but other entities may not receive assistance for a long time after a crisis occurs.

Doomsday scenarios aside, appropriate authorities should continually address and attempt to minimize America's obvious digital vulnerabilities. 2008's *Comprehensive National Cybersecurity Initiative* (CNCI) provides the first steps in the right direction to reduce these types of weaknesses. For example, CNCI's Trusted Internet Connections capability seeks to identify users in cyberspace; should this system work, unauthorized users will have a much more difficult time penetrating SCADA systems. This policy is one among many that should mitigate the threat to civilian computer systems.

Finally, just as regular law enforcement – and not the US military – combats ordinary street crime, local and state law enforcement officials should take the lead in thwarting threats to their own communities' digital infrastructure. If the challenge remains beyond the abilities of local and state enforcement, or cuts across jurisdictional lines, robust and well-resourced federal law enforcement should take charge. Whether the FBI or similar law enforcement organizations are up to the challenge remains a question mark, but this is more an issue of resource, manpower and bureaucratic constraints, than it is a critical national security problem.

*Maintain Strong Deterrents:* Since legitimate, first-order challenges to digital infrastructure are a subset of war between sovereign nations, the US should maintain both overt and covert capabilities to establish that severe consequences will result if the US is seriously threatened.

Deterring potential aggressors in cyberspace through political signaling is also effective. Just as the US military invites countries to participate in military

exercises in order to deter potential hostile behavior, and just as certain countries still parade their latest military hardware on the boulevards in their capital cities, political signaling can indicate that the US is at least publicly serious in thwarting real and potential challenges in cyberspace.

Since foreign policymakers ultimately decide whether or not to engage in cyberwar, they can also be deterred by American warfighting capabilities. Other countries' leaders are aware that the US would not tolerate real threats to its core national interests. Hence, any considerable, systemic attack in cyberspace that might be considered an act of war will most likely result in a devastating counterattack by American conventional and unconventional forces. Therefore, deterrence remains particularly relevant international relations concept, even in the ungoverned political space of the Internet.

Since full-scale conflict has yet to break out between nations with significant cyber capabilities, it remains unclear what, exactly, would happen in the event of major hostilities. Despite one former top intelligence official's claims that the US is already "losing" an unseen cyberwar,<sup>xliii</sup> the actual outcome of such a conflict is still very much in doubt since much of America's cyber-related offensive and defensive abilities remain classified. In any case, cyberwar would not just entail attacking US digital infrastructure, but also striking US interests, taking US territory, and killing US citizens, which would undoubtedly lead to a violent, real-world counter-reaction.

*Strengthen Public-Private Partnerships:* The government has long worked with private industry on digital infrastructure issues, and this recommendation flows from this historical relationship. Public-private partnerships have been the cornerstone of the digital age; the DoD may have established the foundations of the Internet, but it has been private industry that harnessed, expanded and made it what it is today. In February 2010, cybersecurity specialist David Bodenheimer testified to Congress that "virtually every top official, cybersecurity expert, and major review has reached the same conclusion – public-private partnerships are vital to any successful cybersecurity strategy."<sup>xliv</sup>

One government analyst suggested that the private sector owns some 85-95% of the US digital infrastructure.<sup>xlv</sup> It is reasonable then to assume that private companies will defend their parochial patch of cyberspace from malicious endeavors. If the government provides incentives for industry to collaborate in a cyberspace security framework in order to protect their bottom line, private industry will likely take up the plan with gusto.

Furthermore, the US can further protect its government and military infrastructure by harnessing private firms' abilities in the field of corporate and

informational security. In a way, the US government has little choice in the matter—just about all of America’s governmental hardware and software programs are purchased from private companies, and will be so for the foreseeable future. In any case, the US is better served if there is a fruitful relationship between the public and private spheres; a heavy-handed approach by the US government to secure cyberspace will hamper the capitalist and entrepreneurial notions of companies and could cause public outcry and long, costly battles in the judicial system.

*Avoid Bureaucratic Overreach:* Bureaucratic overreach is a natural occurrence when the US government confronts an emerging but undefined security challenge. In the past, such situations have led to cascading reactions across the government, as each department and agency rushed to exploit newly available money and resources. Even now, all US intelligence agencies and branches of the armed forces are already claiming to be ‘on the front lines’ of protecting US interests in cyberspace. Stating that protecting cyberspace is one of the nation’s most vital national security interests has given all agencies a green light to fund all forms of cyber-related projects, whether or not it fits into a larger national strategy.

Unfortunately, the behavior of officials and agencies over the years suggest the government’s intrusive power in the realm of surveillance, free speech and cyberspace can be exploited for political gain. For example, a 1975 Congressional probe discovered that US intelligence agencies and law enforcement routinely abused their powers and illegally wiretapped various Americans for political reasons, including Members of Congress, Supreme Court justices, church officials, union leaders, journalists, Martin Luther King, Jr., and even Eleanor Roosevelt.<sup>xlvi</sup> Concerns about intrusive government monitoring of private citizens during the 1990’s similarly undermined NSA’s attempt to access all encrypted telephone calls via the Agency-designed *Clipper* computer chip. The post-9/11, White House-authorized electronic surveillance program that sidestepped explicit legislation on the topic further raised questions about the government officials’ interest in monitoring communications. Recent efforts, including scant details emerging from NSA’s *Perfect Citizen* program, which theoretically scrutinizes critical infrastructure such as power plants against attacks emanating from cyberspace<sup>xlvii</sup> gave those familiar with the government’s checkered history of intrusion into domestic affairs pause.

Whether or not the NSA or any other organization routinely performs its mission adequately and legally is immaterial; so long as insular government organizations are subject to minimal oversight and less-than-intrusive audits, the public will often assume that excesses will inevitably occur. Government secrecy is important in many respects, but when agencies with secret mandates intersect

with the daily life of ordinary citizens, it usually leads to degraded public trust in overall government security efforts, or an environment that is not conducive to business and entrepreneurship.

One way that the US can limit the possibility of potential overreach by government bureaucracies is for Congress to become much more aggressive and effective in its oversight responsibilities than it has in the past. Despite this simple Constitutional purpose, this mandate is not without complications, as overlapping oversight responsibilities, partisan sniping and inconsistent direction inevitably leads to gridlock and sub-optimal security results. A more effective solution would be for the legislative branch to create two committees – one in the House and one in the Senate – dedicated to protecting cyberspace, akin to Congress’s Armed Services or the Intelligence Committees.

The 9/11 Commission termed Congressional oversight for intelligence and counterterrorism prior to 2001 “dysfunctional”; Congress can avoid the mistakes of the past by taking a proactive role in the emerging issue of protecting cyberspace. By streamlining the process, Congress can not only play a muscular role in protecting cyberspace, but also can show that the body is not so hopelessly gridlocked as to be unable to provide a critical role on such an important topic.

*Forge an International Consensus:* Since safeguarding cyberspace cuts across national boundaries, the challenges to protecting digital infrastructure are global and require international solutions. Protecting cyberspace will ultimately require an international regulatory framework to effectively achieve US national security goals. Therefore, an international consensus on cybersecurity is necessary. After all, it is better to determine solutions that allow for the buy-in of the major nation-states on this complicated topic before an actual shooting war breaks out.

Constructing a flexible international solution is in America’s narrow self-interest. Much like fighting pandemic flu and international terrorism, the US requires the assistance of other nation-states to create the appropriate global legal architecture to achieve better outcomes in cyberspace. International rules of war do constrain America’s unfettered ability to make and wage war, but also provide increased legitimacy when the US commits to large-scale combat. They also bind other nations to behave in a certain way, as well as inoculate the US from threats from other nation-states and perhaps some sub-state actors. Thus, in order to protect its own parochial interests, the US should take the lead in crafting binding international cybersecurity treaties through appropriate international political bodies.

Crafting international solutions to protect cyberspace is in other networked nations' self-interest as well—even those not always aligned with the US. In the event of a major cyberattack, international treaties would provide some degree of protection from possible cyberspace backlash that will result from a systemic attack on America's digital infrastructure. For instance, if US markets were disrupted in such a way that caused the US Treasury securities to decline, Beijing's \$800+ billion investment in US debt would be significantly threatened.<sup>xlviii</sup> Thus, it would be in China's long-term economic interest to work with the US on establishing a framework to protect cyberspace—and vice versa.

International solutions will also lend legitimacy to cyberspace challenges that do not immediately affect any state's vital national interests, such as in the realm of cybercrime or cyberterrorism. An attack on, say, Wall Street will have unknown worldwide financial repercussions, so it would be in the economic interest of all nations linked together by fiber-optic cables and other physical infrastructure to the Internet to create mutually beneficial understandings that would not disrupt the ebb and flow of world commerce.

Of course, these international agreements are subject to parochial understandings of what it means to "protect cyberspace." For example, the US, Great Britain and other countries voted in April 2010 against a Russian-backed UN treaty on cybercrime in favor of previous legislation that would improve individual nations' cybersecurity laws. The 2001 EU Convention on Cybercrime, while considered by some to be a gold standard on this issue, neglects issues outside the realm of criminalizing this sort of behavior; moreover, 30 nations have yet to ratify it. Still, there remains hope that the international legal impasse can eventually be overcome, as countries come closer to understanding that protecting cyberspace is an issue, like disease and the weather, that can affect almost anyone.

### **Final Thoughts**

America's decisionmakers and bureaucracies are oftentimes reactive to 'game-changing' global challenges, with occasionally disastrous results – the 9/11 attacks forced a radical evolution of the way the US dealt with the threat of global terrorism, but in the hurried race to protect the nation from another attack, policymakers made decisions that were in hindsight ill-advised. By exaggerating the threat and forewarning of a 'digital Pearl Harbor' or a 'cyber 9/11' – the US is creating an all-powerful cyber-bogeyman that may only exist in the world of fiction.

Protecting America's digital infrastructure will be a complex but ultimately manageable task, since not every threat is an existential one. Therefore, it is

unwise for US leadership to couch the cyberspace debate in the language of war and warfare, as this type of rhetoric not only oversimplifies a complicated topic, but also fans popular fears among the citizenry. Reclassifying the threat, which is continually trumpeted most recently on the covers of the *Economist* and elsewhere, is needed to relax public concerns. By approaching the protection of cyberspace in a comprehensive, level-headed manner, and by discerning what is a vital national security interest and what is not, US policymakers can make more informed decisions about the challenges facing the nation's digital infrastructure.

We do not deny that protecting US interests in cyberspace is complicated that needs to be discussed on international, national and local levels. This challenge will require a degree of education of both the political and bureaucratic classes, and these efforts will require time, money and persistence. However, we believe American policymakers must place 'protecting cyberspace' in perspective and reevaluate its priority status against other actual threats to the US. By doing so, policymakers can make better-informed decisions about how to properly defend the country from foreign and domestic threats. If America's leaders make the right decisions, the emerging digital century will be a relatively safe and secure one.

---

---

**Endnotes**

- i "Cyberspace Policy Review." *The Office of the White House*. 29 May 2009.
- ii The May 2010 NSS details the critical national security priorities, including: "Strengthen security and resilience at home"; "Disrupt, dismantle, and defeat al Qaeda and its violent extremist affiliates"; "Reverse the spread of nuclear and biological weapons and secure nuclear materials"; "Advance Peace, Security and Opportunity in the Greater Middle East"; "Invest in the Capacity of Strong and Capable Partners"; "Secure Cyberspace."
- iii "Remarks By The President On Securing Our Nation's Cyber Infrastructure." *The Office of the White House*. 29 May 2009.
- iv Ibid.
- v Anderson, Benedict. *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. Verso: July 1991. p.6.
- vi Ellsworth, Robert, Andrew Goodpaster, and Rita Hauser, Co-Chairs. *America's National Interests: A Report from The Commission on America's National Interests, 2000*. Washington, D.C.: Report for Commission on America's National Interests, July 2000.
- vii Ibid.
- viii These major documents, among others, include: three national security strategies; three quadrennial defense reviews; two national defense reviews; two national intelligence reviews; one national military strategy; one defense intelligence strategy; one national strategy for homeland security; one national strategy to secure cyberspace; and one 60-day cyberspace policy review.
- ix *America's National Interests: A Report from The Commission on America's National Interests, 2000*.
- x Ibid.
- xi Statement Of Dr. James N. Miller, Principal Deputy Under Secretary Of Defense For Policy Before The House Of Representatives Committee On Armed Services Subcommittee On Strategic Forces. March 16, 2010.
- xii "The National Intelligence Strategy of the United States of America." *Office of the Director of National Intelligence*. August 2009.
- xiii Ware, Willis H. *Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security*, The RAND Corporation, February 1970.
- xiv "Computers at Risk: Safe Computing in the Information Age." *National Research Council*. National Academy Press, 1991.
- xv "Report to the President's Commission on Critical Infrastructure Protection." *CERT Coordination Center*. 1997.
- xvi Wigder, Zia, Patty Evans, Vikram Sehgal and Brendan McGowan. "Global Online Population Forecast, 2008 to 2013." *Forrester Research*. 21 July 2009.
- xvii Wilson, Clay. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." *CRS Reports*. 29 January 2008.
- xviii *Securing Cyberspace for the 44<sup>th</sup> Presidency: A Report of the CSIS Commission on Cybersecurity for the 44<sup>th</sup> Presidency*.; Gorman, Siobhan, August Cole and Yochi Dreazen. "Computer Spies Breach Fighter Jet Project." *The Wall Street Journal*. 21 April 2009.
- xix Jonathan Oparadt in the Duke Law and Technical Review defined cybercrime as "activity conducted for profit, primarily motivated by financial gain or notoriety. Cyber

crime typically involves the production of malware, the distribution of child pornography, hijacking for ransom, the sale of mercenary services, and the like.” Ophardt, Jonathan A. “Cyber Warfare And The Crime Of Aggression: The Need For Individual Accountability On Tomorrow’s Battlefield.” *2010 Duke Law and Technology Review* 003. 23 February 2010.

xx Talbot, David. “Cybercrime Needs to be Top Priority, Says Obama Aide.” *MIT Technology Review*. 14 April 2010.

xxi Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” *CRS Reports*. 29 January 2008.

xxii “McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property.” 29 January 2009.; Ludvig, Sonja. “Cybercrime Costs the Private sector 1 trillion dollars each year.” *Deloitte.com*. 26 June 2009.

xxiii Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” *CRS Reports*. 29 January 2008.

xxiv Zetter, Kim. “Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible.” *Wired Magazine*. 29 July 2010.

<<http://www.wired.com/threatlevel/2010/07/hayden-at-blackhat/#more-18103>>

xxv *Securing Cyberspace for the 44<sup>th</sup> Presidency: A Report of the CSIS Commission on Cybersecurity for the 44<sup>th</sup> Presidency*, Gorman, Siobhan, August Cole and Yochi Dreazen, page 12.

xxvi Clarke, Richard and Knake, Robert, *Cyber War: The Next Threat to National Security and What to Do About It*, 2010. Page 172. See also Lynn, William J. “Defending a New Domain,” *Foreign Affairs*, September/October 2010

xxvii The National Counterintelligence Strategy of the United States of America. *The Office of the National Counterintelligence Executive*. 2009.

xxviii Ibid.

xxix DHS’s National Infrastructure Protection Center defines cyberterrorism as “a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.” Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” *CRS Reports*. 29 January 2008.

xxx Nakashima, Ellen. “FBI director warns of ‘rapidly expanding’ cyberterrorism threat.” *The Washington Post*. 4 March 2010.

xxxi Talbot, David. Russia's Cyber Security Plans. *MIT Technology Review*. 15 April 2010.

xxxii Arguilla, John and David F. Ronfeldt, “The Advent of Netwar.” Vol 1996, Part 2. United States. Dept. of Defense, National Defense Research Institute (U.S.), *The Rand Corporation*, p.69.

xxxiii “Cyber War: Sabotaging the System.” *CBS News*. 8 November 2009.

xxxiv Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence. “Cyber Operations and Cyber Terrorism: DCSINT Handbook No. 1.02.” *US Army Training and Doctrine Command*. Fort Leavenworth, Kansas. 15 August 2005.

xxxv Flynn, Stephen. “Minn. Bridge Collapse Reveals Brittle America.” *Popular Mechanics*. 1 October 2009.

xxxvi “2009 Report Card for America’s Infrastructure.” *American Society of Civil Engineers*. 2009.

xxxvii See IT Dashboard Portfolio page, accessed at <http://it.usaspending.gov/?q=portfolios>

- <sup>xxxviii</sup> “They cyber war threat has been grossly exaggerated,” Intelligence Squared U.S. debate, June 8, 2010. Page 35. Comments by Bruce Schneier.
- <sup>xxxix</sup> “U.S. Nuclear Reactors.” *US. Energy Information Administration*.  
[http://www.eia.doe.gov/cneaf/nuclear/page/nuc\\_reactors/reactsum.html](http://www.eia.doe.gov/cneaf/nuclear/page/nuc_reactors/reactsum.html); “National Inventory of Dams (NID).” *US Army Corps of Engineers*. October 2007; “Frequently Asked Questions: Electricity.” *Energy Information Administration*.  
[http://ftp.eia.doe.gov/ask/electricity\\_faqs.asp#coal\\_plants](http://ftp.eia.doe.gov/ask/electricity_faqs.asp#coal_plants); “Highway Bridge Program: Condition of Nation's Bridges Shows Limited Improvement, but Further Actions Could Enhance the Impact of Federal Investment.” *Government Accountability Office*. GAO-10-930T. 21 July 2010.
- <sup>xl</sup> “2008 Report to Congress.” US-China Economic and Security Review Commission. *US Government Printing Office*, 2008. p.297.
- <sup>xli</sup> “Cyberspace Policy Review.” *The Office of the White House*. 29 May 2009.
- <sup>xlii</sup> Priest, Dana and William Arkin. “A Hidden World, Growing Beyond Control.” *The Washington Post*. 19 July 2010.
- <sup>xliii</sup> McConnell, Michael. “Mike McConnell on how to win the cyber-war we're losing.” *The Washington Post*. 28 February 2010.
- <sup>xliv</sup> “Statement to the House Armed Services Committee’s Subcommittee on Terrorism, Unconventional Threats and Capabilities,” David Bodenheimer, February 10, 2010.
- <sup>xlv</sup> La Lena, Anne. “PCII & You,” *DCIP News*, November 2009.
- <sup>xlvi</sup> Gravel, Mike and Joe Lauria. *A Political Odyssey: The Rise Of American Militarism And One Man's Fight To Stop It*. Seven Stories Press, 2008; pp.194-195.; Smock, Raymond and Roger Burns. “Contract fraud? CIA abuses? Financial crisis? Congress Used To Investigate.” *The Washington Post*. 8 August 2010.
- <sup>xlvii</sup> Gorman, Siobhan. “U.S. Plans Cyber Shield for Utilities, Companies.” *The Wall Street Journal*. 8 July 2010.
- <sup>xlviii</sup> “Major Foreign Holders of Treasury Securities.” US Treasury. May 2010.  
<<http://www.ustreas.gov/tic/mfh.txt>>