ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey

CYBER STATECRAFT INITIATIVE

The US Cyber Policy Reboot

Over the course of 2011, the United States government released a coordinated set of policies that represents the most energetic cyber statecraft in nearly a decade.

This Issue Brief will provide a broad overview of today's US cyber policies and programs and takes a relatively optimistic slant. This optimism is unfortunately rooted not in confidence that the projects and initiatives make us more secure, but rather that there is any fresh progress at all. We have been wandering a policy desert for years and while we may not have reached an oasis, we have found a glass with some water in it. The glass is not even full, but it can give us hope for what lies ahead.

To support this conclusion, this brief examines the current US policies and documents, starting with their background, along with ongoing projects, how this compares to other nations, and what to expect next.

How We Got Here

Despite the recent headlines announcing the advent of "cyberwar," the problems of computer security and "cyber" are not new.[1] Over the past several decades, numerous reports have indicated that cyberspace is important, even critical, and extremely vulnerable in the face of growing threats from state and non-state actors. Of course, all have called for immediate action—usually the same actions called for, and ignored, in all the earlier reports. These warnings go as far back as reports from the Defense Science Board in 1970 and the National Research Council in 1991. Additional commissions and boards followed, including Defense Science Board reports in 1996 and 2001, the Marsh Commission (President's Commission on Critical Infrastructure Protection) in 1997, and more recently the Commission on Cybersecurity for the 44th Presidency in 2008.

More striking than the words in these reports are the catastrophes taking place in the networks. Of the thousands of cyber incidents since the late 1980s, at least six were serious enough to be considered "wake up calls."[2] Each had similar underlying causes (vulnerable systems and distracted people) and seized the attention of senior government officials who rightly decided "never again." Yet despite some progress over these intervening decades, the problems highlighted in the reports—subsequently made real in the incidents—remain unsolved: The wake-up calls have been greeted by our hitting the snooze bar.

About the Cyber Statecraft Initiative

The Atlantic Council's Cyber Statecraft Initiative helps foster international cooperation and understanding of new forms of cooperation and conflict in cyberspace through global engagement and thought leadership.

An earlier version of this Issue Brief appeared as a chapter in *Securing Cyberspace: A New Domain for National Security*, published by the Aspen Strategy Group in February, 2012.

The Cyber Statecraft Initiative is generously supported by The Morganti Group Inc.

[1] TIME magazine seems to have had the first major cover story of "Cyber War" on 21 August 1995, nearly 16 years before the another major cover story from Bloomberg Businessweek, which declared on 25 July 2011 that the "Cyber War Has Begun."

[2] The list of wake-up calls include the Morris Worm and Cuckoo's Egg intrusion (late 1980s), the SOLAR SUNRISE intrusion and exercise ELIGIBLE RECEIVER (late 1990s), MOONLIGHT MAZE intrusions (circa 2000), Chinese espionage intrusions (early 2000s to the present), attacks against Estonia and Georgia (2007 and 2008), and BUCKSHOT YANKEE intrusions (2008). Note this list does not even include intrusions into Google, stolen F-35 information, WikiLeaks, or other recent newsworthy intrusions.

Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council of the United States. You can follow his comments on cyber issues on Twitter at **@Jason_Healey**.

Despite the recent headlines announcing the advent of "cyberwar," the problems of computer security and "cyber" are not new.

Fortunately, the United States government is in the midst of the third major phase of new policymaking. It is still too early to know if this current policy rollout will lead to any more substantive changes than the last two, in 1998 and 2003.[3] However, there is, as the remaining sections of this chapter will discuss, room for optimism.

Current US Cyber Policies and Documents

The bad news is that, even after the recent activity, the United States still does not have an overarching cyber strategy. The comprehensive 2003 Strategy to Secure Cyberspace is largely ignored;[4] the 2008 Comprehensive National Cybersecurity Initiative was not comprehensive, focusing solely on government networks; and while the 2009 Cyberspace Policy Review listed ten specific near-term actions, it was not a strategy.[5]

The good news is that there has been more momentum for strong cyber policies in the last few months than in the last eight years. The outlines of these new policies include:

1. **Basic Continuity:** These policies generally continue to prioritize cyber efforts in similar ways to past policies. These include strengthening cybersecurity for federal systems, improving protections for consumers, and broadly increasing international cooperation.
2. **Some New Ideas:** However, this essential continuity should be considered updated, as the US government has learned from the lessons of the past two decades. For example, the Department of Defense is no longer emphasizing offense or deterrence by punishment, and "regulation" is no longer quite as dirty a word as it used to be.
3. **A Light but Expanding Government Touch:** Programs remain generally voluntary, though there is proposed new legislation calling for regulation of companies in critical infrastructure sectors.
4. **Inclusion and Balance of New Areas of Cyber Statecraft:** Whereas past cyber strategies typically only covered security and, at times, innovation, the new policies are more holistic. The inclusion of new areas of cyber statecraft (including norms of international behavior, Internet freedom, and development) allows the government to better prioritize and balance between policies. The DoD has struck a better balance by emphasizing defense over offense, and all cyber strategy documents highlight the importance of the American values of free speech and commerce.

White House leadership on this issue is perhaps stronger today than it has been since 2003, when much responsibility passed from the White House to the Department of Homeland Security, though institutional power remained with the larger and better-organized Department of Defense (and to a lesser extent, the Department of Justice). Since the appointment of Howard Schmidt as the president's cyber coordinator, the National Security Council has been the focus of the US government's efforts. The Department of State is also newly invigorated, with the appointment of its own cyber coordinator, veteran cyber expert Chris Painter, who reports directly to the secretary. The Department of Defense, meanwhile, is still the biggest, most capable player but appears to be accepting a somewhat smaller intergovernmental profile, letting DHS and State take the lead on many issues.

The surge of new policies in the last year includes several highlights: The White House issued its first-ever legislative proposal on cybersecurity along with a strategy to better

[3] The 1997 release was based on the Marsh Commission report and led to President Clinton's PDD-63 and the establishment of new organizations at the Federal Bureau of Investigation and Department of Commerce. The 2003 release was part of the overall focus on homeland security after the 9/11 attacks and included HSPD-7, NSPD-38, the National Strategy to Secure Cyberspace, and the National Infrastructure Protection Plan and accompanying organizations, especially within the Department of Homeland Security. The Comprehensive National Cybersecurity Initiative of 2009 remains important, but was still limited to government actions and networks.

[4] Indeed, this author, while working as a policy director in the White House office that published the 2003 strategy, was told to ignore it less than a year after it was published.

[5] Though many observers thought it would itself be the new strategy, this was only #2 on the list of near-term actions.

engage internationally; these documents were herded together through the interagency process along with new cyber strategies from the Departments of Defense, Commerce, and Homeland Security.

The Department of Commerce's strategy highlights the avoidance of strong regulation, calling for voluntary codes of conduct to decrease vulnerabilities and new incentives to reduce threats, as well as new efforts for consumer education and research for new security technologies. The Department of Commerce is also responsible for implementing an earlier White House strategy for creating "trusted identities" to improve Internet commerce. More recently, the Securities and Exchange Commission has issued guidelines for publicly traded companies to disclose information to investors when they have been subjected to a significant cyber incident. This guidance has already resulted in a number of interesting disclosures from VeriSign, Citi, and other companies.

> *The Department of Defense Strategy for Operating in Cyberspace continues the trend of de-emphasizing the "militarization" of cyberspace, with five initiatives that both normalize and prioritize cyberspace operations.*

Moving from domestic affairs to national security, international audiences were often confused by seemingly conflicting statements from the US government that the Internet should be free and yet should be policed for the purposes of security and the protection of intellectual property rights. Moreover, the US military's stated goal of achieving cyber "superiority" or "dominance" served to further obfuscate the US government's views on cybersecurity. The Obama administration's *International Strategy for Cyberspace* was particularly ground-breaking, as for the first time it combined these uncoordinated and unconnected policies into one, calling for new norms and practices in cybersecurity, while emphasizing traditional American values of free speech, innovation, free trade, and international engagement.

The *Department of Defense Strategy for Operating in Cyberspace* continues the trend of de-emphasizing the "militarization" of cyberspace, with five initiatives that both normalize and prioritize cyberspace operations. The strategy notes that DoD will treat cyberspace as an operational domain—equal to air, land, sea and space—and calls for new concepts to improve its defenses and embrace undefined "active cyber defenses" (more on this, below). It also announces that it will work with partners in the US government, the private sector, and internationally (starting with traditional allies), and improve the Department's workforce and technology acquisition. DoD continues to plan to conduct intelligence and offensive operations in cyberspace and still hopes to deter some adversaries by threatening kinetic or cyber retaliation but these priorities do not feature in the new strategy.

The most recent document is the *Blueprint for a Secure Cyber Future* from the Department of Homeland Security, which outlines two separate but interrelated cyber "focus areas" of protecting critical information infrastructure and strengthening general cybersecurity. The former helps protect finance; oil, gas and electricity; the backbone telecommunications networks; and similarly important sectors. To enhance general cybersecurity—including corporate networks, home users, and everyone in between—DHS is expanding on their previous idea of a improving security through a distributed and interlinked "cyber ecosystem."

In addition to these Executive Branch policy documents, several legislative initiatives are underway. A wide-ranging White House legislative proposal would standardize requirements for reporting to consumers when their personal information may have been compromised, mandate outside audits and reporting to the Securities and Exchange Commission, and includes a number of security provisions and projects. Two Senate bills have been sponsored by Senators Lieberman and Feinstein McCain (supported by the administration) and Senator McCain. The House has its own bills, one by Congressman Lungren and another by Congressmen Rogers and Ruppersberger. In general, these are similarly comprehensive in their approach, though they compete on some details such as regulation and the role of the National Security Agency. It is still too early to know how this legislation will emerge or even if any cyber bill could can pass during an election year.

Ongoing Projects and Programs

The **Department of Homeland Security** has put in place many robust initiatives, starting with strengthening their capability to respond to serious incident. At the center of their response efforts are the National Cybersecurity and Communications Integration Center and US CERT, whose role is to coordinate information sharing before and response after significant cyber incidents. DHS has also set up a new response team to focus solely on industrial control systems—the digital devices that control electrical grids, dams, power plants, and factories which are increasingly being connected to the Internet, dramatically increasing the chances of a major cascading failure.

A second major DHS initiative is pushing the EINSTEIN family of systems throughout the federal government to better detect and stop intrusions. Among the many steps DHS has taken to improve Federal cyber security, these programs are best known, largely because they have been a lightning rod for attention from the media and privacy activists. Whereas EINSTEIN 2 is meant to only detect attacks, which overworked defenders must then respond to, EINSTEIN 3 is designed to more actively and automatically stop attacks while they are underway. In addition, EINSTEIN 3—developed by the National Security Agency—will detect threats using "signatures" based on NSA's classified sources and methods. Accordingly, there are concerns that the system would be used to inappropriately collect information submitted by citizens online to federal agencies (a reasonable concern considering the role of NSA in the wake of the wiretapping scandals).

DHS is also working to improve their outreach and cyber education, such as through National Cybersecurity Awareness Month, and a focus on improving the nation's cyber workforce. The DHS also conducts major exercises, with Cyber Storm being the biennial capstone, to test incident response plans and information sharing within government and the private sector.

The **Department of Defense** is pursuing several other major initiatives. The one most covered in the media is the creation and maturation of US Cyber Command. However, there is increasing attention on developing "active cyber defenses." Though officials are generally reticent to describe what this actually means, such defenses were summarized by the deputy secretary in a Foreign Affairs article as being "part sensor, part sentry, part sharpshooter."

The **Department of Commerce**'s most important projects have been to implement the new strategy on trusted Internet identities, oversee the Internet domain name system, and assist other nations with capacity development. The State Department, with its new coordinator reporting directly to the secretary, has been increasingly active, especially on issues of Internet freedom, and has taken the lead in bilateral (such as with Russia) and multilateral (in the G8 and OECD) discussions. The **Justice Department** continues to prosecute criminals and train judges, prosecutors, and law enforcement to recognize cybercrimes and get convictions.

Approaches of Other Governments

With the new *International Strategy for Cyberspace*, the United States has leapt ahead of other governments, by putting forward a complete vision of cyber statecraft, combining security, intellectual property, Internet freedom, and deterrence. We should expect all future national cyber strategies to become similarly encompassing.

Until recently, the United States had one of the most "militarized" approaches to cyberspace, with a strong visible role for the Department of Defense. Though the size and scope of US Cyber Command are still unparalleled internationally, the recent administration strategies have downplayed the military role. Many other nations, though, see cyber commands as the new must-have accessory. Russia, South Korea, Germany, the United Kingdom, and Japan have all recently created, or are in the process of creating, new military cyber centers.

The **United Kingdom** has been very active in broadly similar ways to the United States, with an Office of Cyber Security and Information Assurance (OCSIA) under the Cabinet Office's National Security Secretariat. The OCSIA, along with the Government Communications Headquarters (the equivalent of the National Security Agency), oversee the more technical Cyber Security Operations Centre. A new Joint Forces Command will give a more centralized and streamlined military cyber chain of command.

France was one of the first Western nations to declare sovereign borders for Internet content, forcing Internet companies in 2000 to respect French laws limiting access to Nazi material. Over time, more nations have been adopting the French model, insisting on some national oversight of content. France used its G8 presidency in 2011 to find agreement on the best balance between cyberspace regulation and innovation.

Australia has tackled cybersecurity with a stronger regulatory approach, making a novel distinction between cyber security (concerned with confidentiality, integrity, and availability) and cyber safety (focused on harmful content, such as exposure to illegal and offensive content, cyberbullying, and stalking and is building up its technical perimeter to keep out such "safety" threats.

Estonia has been hitting above its weight since the 2007 attacks, especially with regards to seeking global cyber norms. Its cyber strategy set a goal to "achieve worldwide moral condemnation of cyber attacks that affect the functioning of society and impinge directly on people's wellbeing."

Russia has long been active in cyber operations and seems to have both significant capability and strong oversight from its Security Council. Internally, Russian leadership seems to depend more on "scientific" and "technical" experts for what in the United States would be pure policy issues but there appears to be strong internal and international dialogue. Recently, an intelligence official announced Russia would create their own cyber command.

Unfortunately, **China** is hyperactive in cyber espionage but without similarly strong oversight. Though China has a good interagency process at the mid-levels, there is no clear link for interagency experts to pass information up to their leaders. This also means that those leaders cannot quickly get answers during fast-moving crises, such as in response to questions from Washington, London, or even Moscow. Conflicts and competition involving China in cyberspace will thus only become less transparent and more unstable, and it will become more difficult for opposing sides to signal each other.

What to Watch Next?

This paper has described an American cybersecurity apparatus that has recently taken large leaps toward getting its act together. If enacted, these new policies will help the government significantly improve at many basic tasks and start forward on a few more advanced areas. However, weighty problems loom:

1. **Limited Action and Scale:** The last year has seen an amazing release of policies but not as much action. Moreover, many of the initiatives that do exist are little more than pilots that may be difficult to scale up to cover even just the companies in the critical infrastructure sectors.
2. **Legislative Hurdles:** Congress may soon pass cyber security legislation, which will drastically change the dynamic of how US companies and the government solve cyber issues. In the end, unfortunately, the issues are so complex—and government so risk averse—that any legislation is likely to only make only marginal improvements and have to be revisited in five to ten years.
3. **Lack of Budget Authority:** Several important commentators and commissions have called for the White House Cyber Coordinator to have budget authority for more bureaucratic clout. Without this, the interagency process may be effective when there is general consensus but lack teeth to enforce less popular decisions.
4. **Mixed Leadership:** There are few senior leaders who have a deep understanding of cyber issues and national security, while also being familiar with individual departments and the interagency process.
5. **Too Light a Touch?** These new policies begin to open the door to new regulation (such as requiring auditors and SEC reporting for critical infrastructure companies), although today it is still relatively limited. There is a good chance, however, that free market policies have failed and legislation will push stronger enforcement measures.
6. **Lack of Measurement and Control:** Better security is difficult to attain when it cannot be measured and when control comes at a high cost. Currently, the federal government has a poor understanding of its inventory and has in place only the most rudimentary, often misleading, measurements (such as the FISMA act). In comparison, the best practice companies have a standard baseline that is continually monitored, patched, measured, and reported to senior levels.
7. **Changing Technology:** The new cyber strategies are a great leap ahead, but they may not have gone far enough. Mobile and cloud technologies are just the most obvious disruptive technologies that will challenge the plodding US policy process. Certainly, there will be more technologies, promising longer-lasting disruptions not far ahead.

8. **Focus on International Norms:** During 2012, the issue of international norms, the “rules of the road” by which nations tacitly or explicitly agree to follow, will gain momentum. A UN Group of Government Experts will reconvene in the summer, two years after issuing their last report during which the nations involved (including the United States, United Kingdom, Russia, and China) reached far more consensus than expected. This year’s report is likely to be much more contentious, especially in the wake of how cyberspace was used by dissidents during the Arab Spring, an example deeply concerning to nations that control information to their citizens.

With the recent strategies, the United States government has much to be proud of.[6] Optimism is called for, even though it is the optimism of low expectations. As there have been so many failures, it is easy to become excited at just getting by. While there are many more challenges to come, the government has finally shown it can learn lessons and produce strong policies. Implementation will be harder, but at least there are real ends in sight.

MARCH 2012

[6] This is the first time in a long time this author has felt jealous of White House staffers, who have penned an extraordinary, brilliant international strategy and shepherded it through a long interagency marathon.

The Atlantic Council's Board of Directors

**Members of the Executive Committee*
List as of March 7, 2012

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005 (202) 463-7226
www.acus.org