Backgrounder

Published by The Heritage Foundation

No. 2513
January 31, 2011

10 Conservative Principles for Cybersecurity Policy

Paul Rosenzweig

Abstract: *In the age of the Internet, which now determines daily life for Americans, many threats to the U.S. now exist in the cyber domain. Cybersecurity is a near-constant theme in Washington, as well as for private companies around the country. Congress and government agencies are clamoring to develop policies and strategies to protect national security and commercial interests. Internet attacks are already a standard feature of modern life, and the threats and their implications—from hacking into company sites to steal credit card numbers to hacking into government computers for espionage—are growing fast. Cybersecurity must be addressed—the right way. This Heritage Foundation paper outlines the basic facts of the Internet—and the policy principles to which they lead.*

Hardly a day passes in Washington without a legislative proposal or media story about cybersecurity. President Barack Obama has crafted a new cyberspace policy and appointed a "Cyber Czar."[1] Three competing Senate bills clamored for attention on the floor of the chamber during the last session of Congress.[2] Turf wars between the Department of Homeland Security and the National Security Agency are widely reported. The Deputy Secretary of Defense has announced a new "Cyberstrategy 3.0," and a United States Cyber Command has been created at the Pentagon.[3] News reports suggest that someone (nobody quite knows who) has unleashed a cyber attack against Iranian nuclear facilities.[4] Billions of dollars in federal funding hang in the balance; not to mention the vast and immeasurable

Talking Points

- No good data exist on how many cyber intrusions occur annually. The number is so great that in 2004 the U.S. government stopped reporting the number of known intrusions, which in 2003 exceeded 100,000.
- With the current Internet architecture, it is nearly impossible to identify the source of an intrusion. The anonymous nature of the Internet must be acknowledged.
- Policymakers must deal with the world as it is, not as they wish it were. Any legislation must deal with the Internet as it is today, not as the U.S. hopes it will be in the future.
- Cybersecurity is of equal importance to governments and private businesses, so true public–private partnerships must be encouraged, perhaps through a Cybersecurity Assurance Corporation (CAC).
- Since cybersecurity is a global concern, the U.S. must engage with friends and allies.

This paper, in its entirety, can be found at:
http://report.heritage.org/bg2513

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies
of the
Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

consequences that cybersecurity has on the privately owned critical infrastructure in America.

The tumult of policy confusion is substantial, even by Washington standards. Some question whether a threat exists at all, while others deem the threat existential. Novel issues of policy and law surface on a near-daily basis as technological innovation runs headlong forward, leaving policymakers and concerned legislators trailing in its wake.

The time is ripe for conservatives to step back and ask some of the bigger questions about the cyber domain: What is the nature of the Internet? How does that nature affect policy? What aspects of the cyber domain reflect conservative principles of limited government? To which policy recommendations do these principles lead?

Before the Congress's efforts become fraught with special interest group attention and before the heat of the political contest extinguishes the light of reason, it is useful to develop a set of background principles to guide the development of legislation. With a clear sense of principles, Congress will be better equipped to assess how well any piece of legislation addresses cyber intrusions.

Defining the Problem

No good data exist on precisely how many cyber intrusions occur annually. The number is so great that in 2004, the U.S. government stopped reporting the number of known intrusions, which in 2003 exceeded 100,000. Most experts presume that the number today is an order of magnitude larger.

So the problem is a large one. It is also intractable because, with the current Internet architecture, it is nearly impossible to identify the source of an intrusion. Forensic capabilities in the physical realm are far more advanced than they are in the cyber world. The GhostNet cyber spy network, recently evaluated by a Canadian information-security group,[5] successfully perpetrated a sophisticated infiltration of many computers used by governments and non-governmental organizations who had diplomatic contacts with China. Indian embassies were infected, as were the Dalai Lama's information systems. Through sophisticated counter-hacking, the Canadian group was able to trace the cyber signal back to control systems in Hainan, China (perhaps coincidentally, the home of a Chinese signals intelligence facility). But it could go no further. So, in truth, nobody truly knows where GhostNet came from—an intrinsic reality of the nature of the Internet.

Policymakers must deal with the world as it is, not as they wish it were. Any legislation must deal with the Internet as it is today, not as the U.S. hopes it will be in the future.

The task is a daunting one. No background review of cybersecurity that is of any readable length could hope to plumb the depths of the subject. But it is important to start somewhere. Since, as Aristotle said, the nature of the thing "is the thing itself,"[6] this examination begins with what is known about the current nature of the Internet and cyberspace. Following are 10 truths about cyberspace:

1. Cyber Attacks Are Indirect. The cyber domain is basically an incorporeal network of information. It transmits bits of information (essentially "1s" and "0s") across geographic boundaries at amazing speeds, allowing access to information at a distance.

1. The White House, "Cyber Space Policy Review," 2009, at *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf* (January 14, 2011).
2. In the 111th Congress, competing bills were offered by Senators Rockefeller and Snowe (The Cybersecurity Act of 2009, S. 773); Senators Lieberman and Collins (Protecting Cyberspace as a National Asset Act of 2010, S. 3480); and Senators Bond and Hatch (National Cyber Infrastructure Protection Act of 2010, S.3538). Doubtless, similar bills will be advanced in the new Congress.
3. William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, (September/October 2010), p. 97, at *http://www.cfr.org/publication/22849/defending_a_new_domain.html* (January 14, 2011).
4. John Markoff, "A Code for Chaos," *The New York Times*, October 2, 2010, at *http://www.nytimes.com/2010/10/03/weekinreview/03markoff.html?scp=3&sq=stuxnet&st=cse* (January 14, 2011).
5. "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, at *http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network* (January 14, 2011).
6. Aristotle, *Metaphysics*, Book VII, Part 17.

The Heritage Foundation LEADERSHIP FOR AMERICA

With access to information often comes control. Through cyberspace, nation-states can perpetrate espionage; industrial spies can steal trade secrets; criminals can steal money; and militaries can disrupt command-and-control communications.

These are real and powerful dangers. But the cyber domain, while connected to physical and kinetic reality, is not that reality itself. Real-world effects are collateral to cyber effects rather than their immediate and direct product. To be sure, that condition is likely to be temporary. Now that cyber attacks like the recent Stuxnet malware have demonstrated that a virus can, at least in theory, shut down a nuclear reactor or disable an electrical grid, the prospect of serious, second-order, physical effects in the real world is significant.[7]

2. Cyberspace Is Everywhere. The Department of Homeland Security has identified 18 sectors of the economy as the nation's critical infrastructure and key resources.[8] As one would expect of a comprehensive list, it covers everything from transportation to the defense industrial base. It also includes energy, financial systems, water, agriculture, and telecommunications.

The remarkable thing is that virtually all of the sectors now substantially depend on cyber systems. Even those activities most solidly grounded in the physical world—such as manufacturing or food production—have become reliant on computer controls and access to the World Wide Web of information. Manufacturing systems are controlled by computer systems operated at a distance through virtual connections; farmers use global positioning system (GPS) tracking, satellite data, and just-in-time ordering to maintain their operations. The list goes on.

3. The Internet Has No Boundaries. The fundamental characteristic of the Internet that makes it truly different from the physical world is that it lacks any boundaries. It spans the globe and it does so near-instantaneously. There is no kinetic analog for this phenomenon—even the most global-spanning weapons, like missiles, take 33 minutes to reach their distant targets.[9]

This creates a profound challenge for American policy because the reality is that cybersecurity is an international issue. Significant instances of espionage have originated overseas.[10] Some countries, such as Russia and Ukraine, have become known as safe havens for cyber criminals.[11] It can be anticipated that if there ever is a cyber war, America's enemies will launch their attacks from overseas sites that, initially, are beyond U.S. control.

Some countries, notably China, have responded to this reality by attempting to cut themselves off from the Internet or censor traffic arriving at their cyber borders.[12] But such strategies are, in the end, bootless. In the long run, they will prove ineffective, and to the extent they are effective, they cut countries off from the benefits of the Internet. The salient feature of the cyber domain is precisely its ability to accumulate and integrate large bodies of information over long distances in an instant. Any country that erects effective cyber borders is systematically

7. The Stuxnet worm appears to have targeted Iranian nuclear facilities and caused certain centrifuges to malfunction. John Markoff, "A Silent Attack, But Not a Subtle One," *The New York Times*, September 26, 2010, at *http://www.nytimes.com/2010/09/27/technology/27virus.html?_r=1&scp=2&sq=stuxnet&st=cse* (January 14, 2011).
8. As currently defined, these range from agriculture to water systems. Department of Homeland Security, "Critical Infrastructure and Key Resources Sectors," at *http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/sectorMenu.htm* (January 14, 2011).
9. For Heritage Foundation research on missile defense, see "33 Minutes: Protecting America in the New Missile Age," at *http://33-minutes.com/33-minutes* (January 14, 2011).
10. Recent WikiLeaks cables suggest Chinese complicity in several extensive cyber exploits. James Glanz and John Markoff, "Vast Hacking by a China Fearful of the Web," *The New York Times*, December 4, 2010, at *http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?_r=1&hp* (January 14, 2011). The underlying cables remain classified and the government has directed those people, such as this author, who have an active security clearance, to refrain from reviewing the substance of the cables. Hence, the accuracy of the summary of Chinese activity as disclosed in the cables has not been assessed by this author.
11. John Barnham, "Russia's Cybercrime Haven," *Security Management*, November 2008, at *http://www.securitymanagement.com/article/russias-cybercrime-haven-004818* (January 14, 2011).

agreeing to forgo those benefits, to its own detriment. While that might be feasible for a totalitarian state, it will never work for America.

4. Anonymity is a Feature, not a Bug. One of the critical challenges in cyberspace is the problem of anonymity. Because it is often difficult, if not impossible, to identify who is acting at a distance—it took one sophisticated group nearly a year to identify who hacked the Dalai Lama's network and even then they were not 100 percent certain of their conclusion[13]—espionage, theft, and intrusions are often impossible to attribute to a particular actor. How can any nation, company, or individual adequately respond if it is not possible to identify the source of the problem?

This predilection for anonymity is inherent in the structure of the Internet. As originally conceived, the cyber domain serves simply as a giant switching system, routing data around the globe using general "internet" protocols. It embeds no other function (like identity or verification of delivery) into the protocols. The simplicity of this system is, to a large degree, the cause of its pervasiveness. Because it is so simple to use and add content, the cyber domain is readily expandable. It is the minimalist nature of internet protocols that made this particular internet into The Internet.[14]

All of which means that regardless of whether anonymity is good (it protects political speech) or bad (it allows hackers to hide), it is here to stay. One can imagine, of course, the creation of "walled gardens" or "gated communities" on the Internet—sites to which access is strictly controlled, or where users must identify themselves to access a particular portion of the Internet. There already are many classified networks or corporate-only servers that are isolated niches separate from the public Internet. One can also imagine a rule requiring "assured identities," where access to the Internet requires identification. But outside of totalitarian regimes that, too, is unrealistic.

5. Maginot Lines Never Work in the Long Run. In the aftermath of World War I, the French built a strong, immobile defensive system along their border with Germany—the Maginot Line. Everyone knows what happened next: At the beginning of World War II, the Germans simply went around the line and France quickly fell.

In many ways, cybersecurity is in the midst of its Maginot Line period. Governments, companies, and other users hunker down behind firewalls and deploy virus protections and intrusion-detection systems in a principally passive defensive effort. Like the Maginot Line, America's current system of firewalls is rather ineffective. Billions of dollars in theft occur each year. Terabytes of data are stolen.[15] And there is no sense at all of how many intrusions go undetected each day. In short, the offense is stronger than the defense[16] and that means that U.S. reliance on passive defenses is as doomed as the French were in 1940.

12. The most notorious example is China's attempt to construct a "Great Firewall" to keep Internet traffic out of the country. To "test any website and see real-time if it's censored in China," see GreatFireWallofChina at *http://www.greatfirewallofchina.org* (January 14, 2011). But even liberal Western countries like Australia have proposed restrictions on Internet traffic, albeit for more legitimate reasons, such as limiting the spread of child pornography. Associated Press, "Australia Says Web Blacklist Combats Child Porn," March 27, 2009, at *http://www.physorg.com/news157371619.html* (January 14, 2011). In both cases, states have begun to regulate Internet traffic in ways not thought possible until recently.
13. "Tracking GhostNet."
14. David Post, *In Search of Jefferson's Moose* (New York: Oxford University Press, 2009), pp. 24–34, 44–49, 68–89. This book serves as an excellent introduction to the structure of the Internet.
15. One such program, known in the United States by its code name "Titan Rain," infiltrated the systems of several significant U.S. defense contractors. Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, August 25, 2005, at *http://www.time.com/time/nation/article/0,8599,1098371,00.html* (January 14, 2011). This program or a similar one appears to have allowed China to gain access to the plans for the new F-35 fighter planes. See Daniel Nasaw, "Hackers Breach Defenses of Joint Strike Fighter Jet Programme," *The Guardian*, April 21, 2009, at *http://www.guardian.co.uk/world/2009/apr/21/hackers-us-fighter-jet-strike* (January 14, 2011).
16. Lynn, "Defending a New Domain."

Counteracting that vulnerability will require the development of active defenses—that, instead of merely standing guard at Internet system gateways, look beyond those gateways to assess systems patterns and anomalies. With that sort of information, cybersecurity could transition from detecting intrusions after they occur to preventing intrusions before they occur.

6. 85 percent to 90 percent of U.S. Government Traffic Travels Over Non-Government Networks. As a corollary to the idea of active defenses (and to the conception that the cyber domain is pervasive), any policy needs to recognize that huge swathes of essential government activity involve communications via networks that are predominantly operated by the private sector. Much as steel factories were essential to the construction of battleships, Internet communications companies have become an essential component of effective government activity. This is yet another reason why any active defenses must, inevitably, be deployed on non-government networks. In other words the best defenses (whether government or private) must operate in the private-sector domain.

This concept is highly controversial, and rightly so. The specter of a government-operated intrusion-prevention system operating on the private-sector Internet is a daunting one for civil libertarians. Relying on private-sector systems is, in many ways, problematic in its operational effectiveness (for some relatively convincing economic reasons, described below) and will not give the government the assurance of effectiveness that it requires.

But the need for active defenses operating in the private sector cannot really be denied without, again, wishing for a cyber domain that simply is not the one that exists today. Who should operate the defensive systems is a much more difficult question, but the need for an active defense is clear. That means that whoever operates the systems must be subject to strict oversight and scrutiny. There must be an effective means of protecting the privacy and personal liberties of innocent users of the cyber domain.

7.There Is a Legitimate Role for Government. Points 5 and 6 lead to a fundamentally conservative economic point: There is a legitimate—indeed necessary—government role in protecting the Internet against theft, espionage, and cyber attacks. Just as there is a role for government law enforcement to protect tangible private property, there is a role in protecting cyberspace properties. In part, this is because of externalities by which the security failure of one network affects others outside the network. There is also a national security component which necessitates a vigilant federal role.[17]

8. NSA Does It Better than DHS. It seems near inevitable that the federal government will play a role in providing solutions to the cybersecurity problem, if only because it must do so for its own benefit, irrespective of private-sector needs. The question then arises which federal agency to entrust with that task, and there is currently a brutal turf war battle between those who favor a civilian governmental role, mostly through the Department of Homeland Security (DHS), and those who favor a military role, principally the National Security Agency (NSA) and Cyber Command (CYBERCOM). The cultural difference between these approaches is vast and the stakes behind the resolution of this turf war are high.[18]

17. American Bar Association Standing Committee on Law and National Security, National Strategy Forum, and the McCormick Foundation, "National Security Threats in Cyberspace," Workshop Report, September 2009, pp. 11–14, at *http://www.fbiic.gov/public/2010/jan/Cyberspace.pdf* (January 14, 2011). An extended discussion of cyberspace as a "commons" can be found in Greg Rattray, Chris Evans, and Jason Healey, "American Security in the Cyber Commons," in Abraham Denmark *et al.*, "Contested Commons: The Future of American Power in a Multipolar World," Center for a New American Security, January 25, 2010, at *http://www.cnas.org/node/4012* (January 14, 2011).
18. Letter from National Cybersecurity Center (NCSC) Director Rod Beckstrom to Homeland Security Secretary Janet Napolitano, March 5, 2009, at *http://epic.org/linkedfiles/ncsc_directors_resignation1.pdf* (January 14, 2011). Which agency leads the cybersecurity effort makes a difference because an "intelligence culture is very different from network operations or security culture," as Beckstrom stated in the letter. Beckstrom resigned his position as NCSC director in part because of his perception that the National Security Agency was inappropriately "control[ing] DHS cybersecurity efforts." *Ibid.*

In theory, the answer is easy: The strong preference should be for a civilian response for what is, after all, a predominantly civilian network. But the hard truth is that the civilian side of the government lacks the expertise and manpower to effectively do the job—which is why DHS has announced its plan to hire 1,000 new cyber experts. But until these new experts are on board (and finding and hiring that many will be a long process), civilian defenses will have to rely on existing expertise that lies predominantly with NSA.

9. No Defense Will Ever Be 100 Percent Perfect. Indeed, the only certainty is the uncertainty of the efficacy of any protective cyber systems. No matter how well constructed, the cyber domain is sufficiently dynamic that their defeat is inevitable. Someday, somewhere, a cyber attack or intrusion will succeed in ways that one can only imagine, with consequences one cannot fully predict.

It follows that a critical component of any strategy is to plan for the inevitable instances in which the country's defenses fail. This means the creation of incentives and structures that encourage the development of a resilient cyber network that can contain any intrusion and rapidly repair any damage. Some analysts have suggested that this means the U.S. should think of cyber viruses much like one does of public health in the real world.[19] Some computers will inevitably get sick. To deal with this possibility the U.S. should (to carry the analogy forward) have policies that call for widely distributing known vaccines; quarantining sick computers; and swarming resources to the site of the infection to cure those who are ill.

10. Hardware Attacks are Even Harder to Prevent than Software Attacks. One little noticed and poorly understood aspect of cybersecurity is the degree to which American cyber hardware is manufactured overseas. As the Defense Science Board has noted, virtually all of the chips that Americans use in the innards of their computers are constructed offshore.[20]

This is a significant vulnerability. But as another panel of the Defense Science Board recognized (and, indeed, recommended) the U.S. government must continue to purchase commercial goods.[21] It is simply untenable to suppose that the United States will ever forgo the economic benefits of a globalized purchasing system. Yet such a system carries inherent risks.

Both private-sector and public-sector strategies to eliminate those risks are non-existent and those required to mitigate it seem to be mostly nibbling around the edges.[22] The steps that the U.S. government is currently taking to enhance supply chain security cannot eliminate the risks to cyber assurance posed by the use of commercial systems. The dispersed nature of the cyber domain only serves to exacerbate the international character of the problem and render it seemingly insoluble.

First Principles First

The first and most fundamental necessity in crafting smart cyber legislation (or any kind of legislation for that matter) is to ensure that it is consistent with the nation's founding principles. Those principles call on the federal government to provide for the common defense, while at the same time ensuring the protection of civil liberties and the vibrancy of free economic markets.

The Founders were deeply concerned about national security: six of the 17 explicit powers

19. IBM U.S. Federal, "Meeting the Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination," White Paper, February 2010, pp. 11–23, at *http://www-304.ibm.com/easyaccess3/fileserve?contentid=192188* (January 14, 2011), and K. A. Taipale, "Cyber-Deterrence," *Law, Policy, and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization*, IGI Global, January 1, 2009, at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045* (January 14, 2011).
20. Defense Science Board Task Force, "High Performance Microchip Supply," U.S. Department of Defense, February 2005, at *http://www.acq.osd.mil/dsb/reports/ADA435563.pdf* (January 14, 2011).
21. Defense Science Board Task Force, "Mission Impact of Foreign Influence on DoD Software," U.S. Department of Defense, September 2007, p. 51, at *http://www.acq.osd.mil/dsb/reports/ADA486949.pdf* (January 14, 2011).
22. *Ibid.*, and Bureau of Industry and Security, Office of Technology Evaluation, "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, January 2010, pp. 208–211, at *http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf* (January 14, 2011).

granted to Congress pertain to national security.[23] Elsewhere in the Constitution, the Founders sought to foster a stout national defense by identifying the President as the Commander in Chief of America's military forces. In the republican guarantee clause, the Constitution made clear that the "United States shall guarantee to every State a republican form of government and shall protect each of them against invasion."[24]

Yet while calling for a strong common defense, the framers of the Constitution were equally concerned with an overpowering government. They limited and enumerated the nature of the powers granted to the federal government precisely because they did not want to risk destroying liberty while protecting it. Thus, the limited scope of the federal government's authority serves as a bulwark against governmental expansion and as a structural protection of free enterprise and civil liberties. That protection is captured, as well, in the Bill of Rights. Private ownership, market freedom, and individual liberty were fundamental Founding-era principles.

While cybersecurity is certainly a newer "battlefield" than perhaps those encountered by the Founders, the need to protect the nation remains the same. The uniqueness of the cyber domain, however, is that it has become an essential platform that Americans use to go about their daily lives. It has become a means by which Americans do business, keep in touch with friends and family, perform financial transactions, engage in recreation, shop, and express themselves. The expansive role of the Internet and its potential impact on civil liberties and fundamental market freedoms require that attempts at regulation strike the proper role for government while defending the nation against attacks.

Principles for Cyber Legislation

So, what do these principles and the nature of the Internet mean for government today? How should legislation be crafted to deal with cyber vulnerabilities?

1. Any legislation should recognize that the cyber threat is substantial, but probably not an existential one (at least not in the same way as, say, the release of a biological agent or the detonation of a nuclear device). So there is no need to obsess about cyber problems at the expense of other policy issues. Congress should take its time and get the solution right.
2. On the other hand, the cyber domain is sufficiently important that Congress does need to focus more effort on it. In particular, Congress should endow a federal coordinator with real power to make decisions and spend money in a coordinated way. Given that the expanse of the cyber domain is as wide as the federal government and as deep as the entire American economy, the right hand must know what left hand is doing. This requires coordination and integration at the operational level, linking regulation and policy, tying together offensive and defensive cyber measures and allowing the coordination of overt and covert programs.
3. Only a strong member of the Administration can provide that kind of functionality. Policymakers should recognize that this will not be easy—Cabinet agencies will resist strong White House coordination and legislative change may even be required—but the absence of strong regulatory and budgetary coordination will doom any coordination effort to failure. Equally important is that to the extent the coordination in the White House must be strengthened, it must not be done at the expense of lost accountability. Any coordinator with greater powers would need to be subject to Senate confirmation and congressional oversight.
4. Because the problem is a global one, America's strategy must be to engage internationally, both cooperatively with friends and allies, and punitively with those who refuse to prevent crime and espionage at locations within their effective control. This will require a greater willingness to

23. U.S. Constitution, Article I, Section 8, and Jim Talent, "A Constitutional Basis for Defense," Heritage Foundation *America at Risk Memo* No. 10-06, June 1, 2010, at *http://www.heritage.org/Research/Reports/2010/06/A-Constitutional-Basis-for-Defense*.
24. U.S. Const., Art. 4, Sec. 4.

share information and cooperate with appropriate allies (such as the U.K.). America's primary focus should be on working cooperatively thorough existing bilateral partnerships and engaging effective international organizations (like NATO).[25] In addition, the United States should lead in the development of international norms and rules that presumptively assign liability to countries that harbor hackers (like Russia and China).

5. American policymakers need to recognize that anonymity is here to stay. So, rules creating walled gardens or requiring identification are not likely to be tenable. For that, in effect, requires creating a *new* Internet. U.S. policies should accept the reality of anonymity and focus on defensive solutions and deterrence that deal with and acknowledge the challenges of attribution. There is little value in wishing for a system that does not now exist and likely never will.
6. American policymakers should also recognize that being defensive does not mean being supine. The U.S. must, as an essential matter, transition its defenses to "active defensive measures." This means that the first priority must be early warning and situational awareness about what is happening in the cyber domain. That means that governmentally operated intrusion prevention systems (like Einstein 3)[26] can only effectively protect the government and military systems they are designed to protect if they are deployed beyond the ".mil" and ".gov" boundaries of the current systems. Likewise, private-sector defensive systems must operate more broadly outside their own servers at Internet switching nodes.
7. This means that policies must encourage true public–private partnerships. They do not exist now, and the private market has failed to provide adequate security. Congress might formalize the public–private partnership necessary for cyber defense by creating a congressionally chartered, non-profit corporation (akin to the American Red Cross and the Millennium Challenge Corporation). One might notionally call it the Cybersecurity Assurance Corporation (CAC).[27]

   This potential organizational adaption would address many of the concerns that have frustrated the purely private or public responses. It would eliminate the "first mover" economic problem by federalizing the response. And it would allow greater maintenance of the security of classified information within the ambit of a government corporation. As a corollary, the quasi-public nature of the CAC might (if appropriate legal structures were adopted) provide a forum in which defense-related private-sector information could be shared without fear of compromise or competitive disadvantage. Thus the CAC would provide a secure platform that allows the government and the private sector to fully employ the country's information assurance capabilities and call on both public and private resources.[28]

   At the same time, the quasi-private nature of the organization would provide greater assurance that legitimate privacy concerns about government overreach were suitably addressed. The centralization of the effort would allow a unified and continuous audit of privacy compliance by an independent ombudsman. The maintenance of a private-sector control structure would fur-

25. Lynn, "Defending a New Domain."
26. Einstein 3 is a developmental program that, if implemented, would detect planned intrusions into governmental cyber systems and prevent them. To operate effectively it is likely that Einstein 3 may need to monitor private-sector systems traffic to detect anomalies indicative of a cyber attack.
27. For a more detailed summary of this idea, see Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence," in Committee on Deterring Cyberattacks *et al.*, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), at *http://books.nap.edu/openbook.php?record_id=12997&page=245* (January 14, 2011).
28. Appropriate legal structures might include mandatory reporting; source anonymity of information given to the CAC; compartmentalization of information that cannot be made anonymous; and a penalty structure for the misappropriation of CAC-protected information.

ther insulate against misuse and abuse by governmental authorities. The absence of return on investment concerns would allow CAC to focus on privacy protection and network integrity.

The use of a CAC-like structure would also ease concerns about military involvement in cybersecurity. Because the NSA has greater capabilities today than any other federal agency, anything the federal government does will probably have a military character to it for the foreseeable future. That necessity, more than anything else, will require outside observers to table their obsession with NSA involvement, at least temporarily, lest the country paralyze itself into inaction.

8. But it also means that the federal government must convert NSA expertise into civilian expertise as fast as possible. Cyber policies must put human capital first. The government needs to develop operational civilian expertise; its initiatives must have a robust plan to provide leaders with the skills, knowledge, and attributes to supervise the program; and, perhaps most critically, cutting-edge cyber research must be a priority.
9. To protect against the inevitable failures, legislation must foster resiliency. Put in cyber terms, federal standards of procurement (which will drive private-sector responses) need to emphasize backups, self-repairing systems, and other redundant applications. Cyber initiatives must be integrated with and take into account other critical infrastructure to build resilient infrastructure. And any program must account for the most significant possibilities of catastrophic loss of the Internet through attacks, such as electromagnetic pulse (EMP).[29]
10. Finally, because nobody really understands the scope of the commercial off-the-shelf technology problem, the government needs to charter a broad-based study program, perhaps through the National Academies of Science and including both government and private-sector expertise, focused exclusively on the problem of commercial off-the-shelf technology and supply chain security.

Cyberspace Changes Every Day

The foregoing list of principles reflects the author's "best-judgment" assessment of cyberspace conflict today. But the single and most fundamental principle to which Americans must adhere is a sense of humility about anyone's understanding of cyberspace. People must be aware that the cyber domain is a dynamic environment that changes constantly. Today, people use the Internet in ways they did not imagine just five years ago (witness the growth of social networks and the development of Internet communications protocols like Skype), much less a few months ago (as with WikiLeaks and the subsequent cyber hacktivist attacks). So anything that the United States does in terms of legislation or regulation (whether domestically or internationally) must emphasize flexibility and executive discretion over mandates and legislative proscriptions. It is quite possible that today's "great idea" for Internet security will kill tomorrow's essential application. As the White House and Congress address cybersecurity concerns (as both surely must), conservatives should bear in mind that most conservative of all principles: First, do no harm.

*—**Paul Rosenzweig** is Visiting Fellow in the Center for Legal & Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*

29. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, "Critical National Infrastructures," April 2008, at *http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf* (December 27, 2010).