

Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations

John Rollins

Specialist in Terrorism and National Security

Anna C. Henning

Legislative Attorney

March 10, 2009

GalleryWatch.com
http://www.crsdocuments.com
CHP Penny Hill Press

Congressional Research Service

7-5700

www.crs.gov

R40427

CRS Report for Congress

Prepared for Members and Committees of Congress

c11173008

Summary

Federal agencies report increasing cyber-intrusions into government computer networks, perpetrated by a range of known and unknown actors. In response, the President, legislators, experts, and others have characterized cybersecurity as a pressing national security issue.

Like other national security challenges in the post-9/11 era, the cyber threat is multi-faceted and lacks clearly delineated boundaries. Some cyber attackers operate through foreign nations' military or intelligence-gathering operations, whereas others have connections to terrorist groups or operate as individuals. Some cyber threats might be viewed as international or domestic criminal enterprises.

In January 2008, the Bush Administration established the Comprehensive National Cybersecurity Initiative (the CNCI) by a classified joint presidential directive. The CNCI establishes a multi-pronged approach the federal government is to take in identifying current and emerging cyber threats, shoring up current and future telecommunications and cyber vulnerabilities, and responding to or proactively addressing entities that wish to steal or manipulate protected data on secure federal systems. On February 9, 2009, President Obama initiated a 60-day interagency cybersecurity review to develop a strategic framework to ensure the CNCI is being appropriately integrated, resourced, and coordinated with Congress and the private sector.

In response to the CNCI and other proposals, questions have emerged regarding: (1) the adequacy of existing legal authorities—statutory or constitutional—for responding to cyber threats; and (2) the appropriate roles for the executive and legislative branches in addressing cybersecurity. The new and emerging nature of cyber threats complicates these questions. Although existing statutory provisions might authorize some modest actions, inherent constitutional powers currently provide the most plausible legal basis for many potential executive responses to national security related cyber incidences. Given that cyber threats originate from various sources, it is difficult to determine whether actions to prevent cyber attacks fit within the traditional scope of executive power to conduct war and foreign affairs. Nonetheless, under the Supreme Court jurisprudence, it appears that the President is not prevented from taking action in the cybersecurity arena, at least until Congress takes further action. Regardless, Congress has a continuing oversight and appropriations role. In addition, potential government responses could be limited by individuals' constitutional rights or international laws of war. This report discusses the legal issues and addresses policy considerations related to the CNCI.

Contents

Introduction 1
Background on Cyber Threats and Calls for Executive Action 2
Comprehensive National Cybersecurity Initiative and Concerns Regarding Transparency and Effectiveness 5
Legal Authorities for Executive Branch Responses to Cyber Threats 8
Separation of Powers in National Security Matters 10
Congressional Constraints on Executive Action 15
Policy Considerations and Congressional Options 17
Conclusion 18

Contacts

Author Contact Information 18

GalleryWatch.com
http://www.crsdocuments.com

Introduction

Cybersecurity has been called "one of the most urgent national security problems facing the new administration."[1] Cyber and telecommunications activities are sometimes conflated to indicate the same meaning or capability. One might distinguish the term cyber from that of telecommunications with the former being the data or applications residing on the latter which is the electronic medium in which the activity occurs. Electronic information systems, also termed "information infrastructures," now support a wide range of security and economic assets in the public and private sectors.

Such systems have been successfully infiltrated in recent years by a range of attackers, some of whom are suspected to have been working in coordination with foreign military organizations or (foreign) state intelligence services. Thus, like the changing nature of U.S. enemies in the post-9/11 environment, the nature of military and economic vulnerabilities has changed: intelligence-gathering battles in cyberspace now also play a crucial role in national security.

In January 2008, the Bush Administration initiated the Comprehensive National Cybersecurity Initiative (the CNCI) to make the United States more secure against cyber threats. The Homeland Security Presidential Directive 23 and National Security Presidential Directive 54 establishing the CNCI are classified. Some details of the Initiative have been made public in Departmental press releases, speeches by executive branch leaders, and analysis and insight offered by individuals that follow cyber security and terrorism related issues. The CNCI "establishes the policy, strategy, and guidelines to secure federal systems."[2] The CNCI also delineates "an approach that anticipates future cyber threats and technologies, and requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated threats and vulnerabilities."[3] Subsequent to the issuance of the classified directives, congressional committees have held hearings regarding the CNCI and heard testimony from a commission established to address necessary cybersecurity reforms.[4]

In a speech during his presidential campaign, President Obama promised to "make cyber security the top priority that it should be in the 21st century ... and appoint a National Cyber Advisor who will report directly" to the President.[5] Although the Obama Administration might craft a new approach to cybersecurity, some experts have urged the new administration to build on the CNCI,

---

[1] Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency (2008).

[2] Department of Homeland Security, *Fact Sheet: DHS 2008 End of Year Accomplishments* (Dec. 18, 2008), http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm.

[3] *Id.*

[4] See, e.g., House Permanent Select Committee on Intelligence, Cyber Security: Hearing on the Nation's Cyber Security Risks, 110th Cong. (Sept. 18, 2008); House Homeland Security Committee, Cybersecurity Recommendations for the Next Administration: Hearing Before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, 110th Cong. (Sept. 16, 2008).

[5] July 17, 2008 speech at Purdue University. As of the date of this report a national Cyber Security Advisor has not been named.

which they note is a "major step toward improving federal cybersecurity."[6] On February 9, 2009, President Obama directed a 60-day interagency cybersecurity review to develop a strategic framework to ensure the CNCI is being appropriately integrated, resourced, and coordinated with Congress and the private sector.[7]

The new administration's focus on cybersecurity would continue recent emphasis on the issue by the executive and legislative branches. This recent focus emerged partly in response to events such as attacks by outside hackers against a Pentagon computer network and the CyberWar against Estonia, which garnered significant media attention. Agency reports of large numbers of attempts to infiltrate government cyberspace have also prompted action. Both the high-profile attacks and more routine infiltrations have shed light on the vulnerability of critical information infrastructures. For example, the Defense Science Board noted that the U.S. military's information infrastructure is the "Achilles' heel of our otherwise overwhelming military might."[8]

Background on Cyber Threats and Calls for Executive Action

Threats to the U.S. cyber and telecommunications infrastructure are constantly increasing[9] and evolving as are the entities that show interest in using a cyber-based capability to harm the nation's security interests.[10] Concerns have been raised since the 1990s regarding the use of the internet and telecommunications components to cause harm to the nation's security interests. Activities producing undesirable results include unauthorized intrusion to gain access and view protected data, stealing or manipulating information contained in various databases, and attacks on telecommunications devices to corrupt data or cause infrastructure components to operate in an irregular manner. Of paramount concern to the national and homeland security communities is the threat of a cyber related attack against the nation's critical government infrastructures – "systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national

---

[6] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* 3 (2008) (including "do not start over" as one of its recommendations for the 44th presidency).

[7] The White House, Office of the press Secretary, *President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review* (Feb. 9, 2009), http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/.

[8] Department of Defense, Defense Science Board, *Defense Imperatives for the New Administration* 3 (2008), http://www.acq.osd.mil/dsb/reports/2008-11-Defense_Imperatives.pdf.

[9] Peter Eisler, *Reported Raids on Federal Computer Data Soar*, USA Today (Feb. 17, 2009), http://www.usatoday.com/news/washington/2009-02-16-cyber-attacks_N.htm?csp=34. Based on data reportedly provided to USA Today, the U.S. Computer Emergency Readiness Team (US-CERT), a Department of Homeland Security entity, found that known cyberattacks on U.S. government networks rose 40% in 2008 compared to 2007. While this survey focused on U.S. government computer systems, telecommunications networks are maintained by private industry, and any degradation to these services or components would necessarily have negative implications for both public and private cyber activities.

[10] For more information on cyberattackers' capabilities, see CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John Rollins and Clay Wilson.

economic security, national public health and safety, or any combination of those matters."[11] Early concerns noted attacks on components of the energy grid, infrastructure control systems, and military equipment as examples of telecommunications based threats to physical infrastructures.[12]

In response, the Department of Energy conducted an experiment in 2007 in which the control system of an unconnected generator, containing similar components as that of larger generators connected to many power grids in the nation supplying electricity, was damaged and became inoperable.[13] While data from federal agencies demonstrate that the majority of attempted and successful cyber attacks to date have targeted virtual information resources rather than physical infrastructures,[14] many security experts are concerned that the natural progression of those wishing to harm U.S. security interests will transition from stealing or manipulating data to undertaking action that temporarily or permanently disables or destroys the telecommunication network or affects infrastructure components. Many security observers agree that the United States currently faces a multi-faceted, technologically based vulnerability in that "our information systems are being exploited on an unprecedented scale by state and non-state actors [resulting in] a dangerous combination of known and unknown vulnerabilities, strong adversary capabilities, and weak situational awareness."[15] This, coupled with security observers' contention that the United States lacks the capability to definitively ascertain perpetrators who might unlawfully access a database or cause harm to a network, leaves the nation increasingly at risk. It also causes acts or discussions related to deterring cyberattacks to be ignored or negated by entities exploiting known or newly found vulnerabilities.

Prominent national security experts have emphasized the vulnerability of U.S. infrastructures. As recently as January 2009, former Director of National Intelligence (DNI) Mike McConnell equated "cyber weapons" with weapons of mass destruction when he expressed concern about terrorists' use of technology to degrade the nation's infrastructure. In distinguishing between individuals gaining access to U.S. national security systems or corporate data for purposes of exploitation for purposes of competitive advantage, former Director McConnell noted that terrorists aim to damage infrastructure and that the "time is not too far off when the level of sophistication reaches a point that there could be strategic damage to the United States."[16]

---

[11] 42 U.S.C . §5195c(e). For more on U.S. efforts to protect critical infrastructures, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff.

[12] Of note, many of the cyber-related incidences that were found to have negatively affected control systems connected to physical infrastructure components were resolved as being the work of current or former employees who had access to and knowledge of the architecture of the affected network.

[13] Jeanne Meserve, *Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN online (Sep. 26, 2007), http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCVideo. A video of the experiment, named Project Aurora, and the resulting damage to the generator is available on the CNN website.

[14] *See* Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* 12 (2008) ("we expected damage from cyber attacks to be physical (opened floodgates, crashing airplanes) when it was actually informational").

[15] House Permanent Select Committee on Intelligence, *Cyber Security: Hearing on the Nation's Cyber Security Risks*, 110th Cong. (Sept. 18, 2008) (statement of Paul Kurtz, Former Senior Director, Critical Infrastructure Protection, White House Homeland Security Council).

[16] The Charlie Rose Show, "Interview of Mr. Mike McConnell, Director of National Intelligence," PBS, January 8, 2009.

Similarly, in elaborating on the potential consequences of a cyber attack, newly confirmed DNI Dennis Blair offered the following statement during the Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence:

> Growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures. Over the past several years we have seen cyber attacks against critical infrastructure abroad, and many of our own infrastructures are as vulnerable as their foreign counterparts. A successful attack against a major financial service provider could severely impact the national economy, while cyber attacks against physical infrastructure computer systems such as this that control power grids or oil refineries have the potential to disrupt services for hours to weeks.[17]

Also describing the evolving threat to U.S. security interests from a cyber-facilitated incident, Melissa Hathaway, Senior Advisor to the DNI and Chair of the Nation Cyber Study Group and President Obama's appointee to lead the 60-day interagency strategic cyber review, wrote that "both state and non-state adversaries are targeting our information systems and infrastructure for exploitation and potential disruption or destruction."[18] During the question and answer period of the most recent DNI Annual Threat Assessment of the Intelligence Community, Director Blair stated that a "cyber capability is not one in which I feel [terrorists] have the skills for the greatest destruction. I think that they have other terrible things they can do to us that they are working on harder, they're better able to do, and they seem to be more motivated to do. So [a cyber terrorist attack is] possible, but I don't think the combination of terror and cyber is the nexus that we are most worried about."[19] However, threats could originate from foreign military or intelligence operatives rather than from terrorist groups.

In response to reports of the increasing pace and volume of cyber intrusions and a recognition that recent cyber-based threats have compelled the U.S. government to take security related actions that may negatively affect an agency's ability to perform its national security duties,[20] legislators and analysts have expressed concerns that the current statutory framework inadequately addresses modern cybersecurity threats. One prominent voice is the Center for Strategic and International Studies' (CSIS) Commission on Cybersecurity for the 44th President, whose members testified before House and Senate committees and released its formal recommendations in fall 2008. The

---

[17] U.S. Congress, Senate Select Committee on Intelligence, Annual Threat Assessment of the Intelligence Community: Hearing on the Threats to the Nation, 111th Cong. (Feb. 12, 2009).

[18] Melissa Hathaway, Cyber Security – An Economic and National Security Crisis, Intelligencer: Journal of U.S. Intelligence Studies, Fall 2008 at 31-6.

[19] U.S. Congress, Senate Select Committee on Intelligence, Annual Threat Assessment of the Intelligence Community: Hearing on the Threats to the Nation, 111th Cong. (Feb. 12, 2009).

[20] In November, 2008, it was reported that the Department of Defense notified all organizations to stop using portable storage devices as it has become "apparent that over time, our posture to protect networks and associated information infrastructure has not kept pace with adversary efforts to penetrate, disrupt, interrupt, exploit or destroy critical elements of the global information grid." Noah Shachtman, *Military USB Ban Meant to Stop Adversary Attacks*, Wired Blog Network (Nov. 20, 2008), http://blog.wired.com/defense/2008/11/military-usb-ba.html. Also, it has recently been reported that some U.S. military units have resorted to disconnecting computer networks from the internet for fear of cyber related risks and a concern that the affected organization may not be managing its network properly thus "making everyone else vulnerable" to an attack. Noah Shachtman, *Air Force Unplugs Bases' Internet Connections*, Wired Blog Network (Feb. 18, 2000), http://blog.wired.com/defense/2009/02/air-force-cuts.html.

Commission recommended that federal cyber-crime provisions should be reexamined and that the "President should propose legislation that eliminates the current legal distinction between technical standards for national security systems and civilian agency systems and adopt a risk-based approach to federal computer security."[21] In addition, it characterized the current statutory framework, particularly the Federal Information Security Management Act, enacted in 2002 to establish agency-level defenses against cyber threats, as too weak to effectively prevent cyber intrusions.[22]

Legislators made some attempts during the 110th Congress to strengthen or "modernize" the existing statutory framework. For instance, a bill introduced by Senator Carper, the Federal Information Security Management Act of 2008,[23] would have added a "Chief Information Security Officer" position to supplement the Chief Information Officer position required in each federal agency under the Federal Information Security Management Act of 2002 and the Clinger-Cohen Act of 1996.[24] However, analysts have argued that ultimately, no change to the existing statutory scheme will adequately equip executive agencies to prevent infiltrations into U.S. cyberspace. They argue that "only the White House has the necessary authority and oversight for cybersecurity."[25]

Comprehensive National Cybersecurity Initiative and Concerns Regarding Transparency and Effectiveness

As of the date of this report, unclassified versions of the January 2008 directives establishing the CNCI have yet to be released. While the Initiative has yet to be legislatively recognized, presidential directives, sometimes considered types of executive orders and visa versa, have the force of law if they are supported by constitutional or statutory authority.[26] Although much

---

[21] See Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency 12 (2008) at 67.

[22] *See, e.g.*, *Id*. at 69 (stating that the Act "has become a paperwork exercise rather than an effective measure of network security"). The Federal Information Security Management Act is Title III of the E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899 (codified at 44 U.S.C. §3541 *et. seq.*). Among other things, it created a position of Chief Information Officer within each federal agency.

[23] Federal Information Security Management Act of 2008, S. 3474, 110th Cong. (2008). The bill was favorably reported by the Senate Homeland Security and Government Affairs Committee and was placed on the Senate calendar. It has not yet been reintroduced during the 111th Congress.

[24] 44 U.S.C. §3506 (requiring Chief Information Officer positions). The Clinger-Cohen Act is the name given to the Federal Acquisition Reform Act of 1996 and the Information Technology Management Reform Act of 1996, which passed as Sections D and E, respectively, of the National Defense Authorization Act for Fiscal Year 1996, P.L. 104-106, 110 Stat. 642, 679 (1996).

[25] House Homeland Sec. Comm., Cybersecurity Recommendations for the Next Administration: Hearing Before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, 110th Cong. (Sept. 16, 2008) (statement of James A. Lewis, Director and Senior Fellow, Center for Strategic and International Studies).

[26] For more information on presidential directives, see CRS Report 98-611, *Presidential Directives: Background and Overview*, by Harold C. Relyea.

remains unknown about the CNCI due to the classified nature of the presidential directives and supporting implementation documents, federal government agency press releases and statements by government officials provide a bit of insight regarding the program. Some security observers are concerned that because the CNCI is focused on developing and adhering to strategies and policies to secure the federal systems, many of which rely on private sector telecommunications networks for service and support, and identifying current and emerging threats and vulnerabilities, it is incumbent on the federal government to improve its coordination activities with non-federal entities and undertake enhanced sharing of timely and relevant cybersecurity related plans and risk data.

Few details have been publicly released regarding the implementation activities or status of CNCI efforts since the establishment of the initiative. According to one media account, Steven Chabinsky, Deputy Director of the Joint Interagency Cyber Task Force for the Office of the DNI, stated at an information technology security conference that there are 12 objectives supporting the Initiative's goal of comprehensively addressing the nation's cyber security concerns. They are:

1. Move towards managing a single federal enterprise network;

2. Deploy intrinsic detection systems;

3. Develop and deploy intrusion prevention tools;

4. Review and potentially redirect research and funding;

5. Connect current government cyber operations centers;

6. Develop a government-wide cyber intelligence plan;

7. Increase the security of classified networks;

8. Expand cyber education;

9. Define enduring leap-ahead technologies;

10. Define enduring deterrent technologies and programs;

11. Develop multi-pronged approaches to supply chain risk management; and

12. Define the role of cyber security in private sector domains.[27]

One question often raised is whether the CNCI objectives are being pursued concurrently. Some security observers are concerned that the government's focus to date has been on securing federal security systems at the expense of other networks that have similar vulnerabilities. The disruption, or perceived accessing or manipulating of data in non-federal networks that contain personal financial information or manage the control systems of the nation's critical infrastructure

[27] Wyatt Kash, Government Computer News, *Details Merge About the President's Cyber Plan* (Nov. 21, 2008), http://gcn.com/Articles/2008/11/21/Details-emerge-about-Presidents-Cyber-Plan.aspx?Page=4.

could have significant economic, safety, and confidence-in-government implications. It is often noted that in the homeland security and law enforcement communities, where a great deal of post-9/11 emphasis is placed on continuous information exchange and collaboration, efforts to secure the federal technology systems, while relegating state, local, and private sector organizations to lower standards of security, will simply redirect or delay risk that inevitably accompanies increased collaboration. This concern is often expressed by non-federal governmental entities which rely on and routinely coordinate efforts with the U.S. government but have not been apprised of the plans or resources accompanying the CNCI.

Given the secretive nature of the CNCI, one of the common concerns voiced by many security experts is the extent to which non-federal entities should have a role in understanding the threat to the nation's telecommunications and cyber infrastructure and assist with providing advice, assistance, and coordination in preparation and response for ongoing and future intrusions and attacks.[28] As telecommunications providers and internet service providers are corporate entities residing in the private sector, and are relied upon heavily to support federal government activities and services, many cyber-security observers suggest that a comprehensive approach to an effective monitoring, defending, and responding regime is not possible without the collaboration and expertise of the nation's cyber sector owners and operators. As evidenced in the twelve objectives of CNCI, it appears the federal government focus is on the prevention aspects of addressing potential threats to the nation's cyber and telecommunications infrastructure. In contrast, the primary response and recovery activities associated with previous network breaches have been addressed by the private sector entity that has been the victim of the attack. In an apparent admission of the need for further transparency and enhanced public-private partnership to better fulfill the goals of the CNCI, former President Bush's Assistant Secretary of Cybersecurity and Telecommunications at the Department of Homeland Security (DHS), Greg Garcia, recently stated that "there was too much classified (about the CNCI) which was not helpful politically and not helpful in getting the word out." Acknowledging the balance between incorporating the view of non-federal entities and the concern of allowing those that wish to use cyber activities to cause harm, Assistant Secretary Garcia went on to further state that the Department had to "walk the line between raised awareness of what was being accomplished and not letting out too much information that could cause us to be targeted. Still, too much was kept secret."[29]

Based on the number of unknowns concerning the CNCI and the apparent lack of inclusiveness with the private sector telecommunication and internet providers, some analysts are concerned that future opportunities for successfully ascertaining known and future threats and developing a comprehensive set of legal and policy responses may not be achievable. An apparent Obama Administration goal for the current 60-day cyber security review is a more transparent and coordinated approach to the nation's cyber security risks with the perceived end result being that all affected parties are consulted and given the opportunity to provide advice and assistance in proposing changes to existing legislation, policy, and processes.[30]

---

[28] It is unknown whether non-federal entities have been invited to participate in the previously mentioned President's 60-day cyber security review that commenced on February 9, 2009.

[29] Jill Aitoro, *Bush's Cyber Chief Calls National Security Initiative Too Secret*, Nextgov (Feb. 11, 2009), http://www.nextgov.com/nextgov/ng_20090211_6858.php.

[30] *See* Press Release, White House, *President Obama Directs the National Security and Homeland Security Advisors to* (continued...)

Legal Authorities for Executive Branch Responses to Cyber Threats

As discussed, the CSIS report on Securing Cyberspace for the 44th Presidency recommends executive action to protect U.S. cyberspace.[31] This and other calls for executive action, together with the 60-day review of the CNCI, implicate questions regarding legal authorities and the appropriate roles of the two political branches in the cybersecurity context. Questions concern the adequacy of existing statutes and the potential need for new legislation to address the modern threat. In addition, for actions not authorized by the existing statutory framework, questions arise regarding the extent of inherent authority for executive-branch responses under the U.S. Constitution.

To be legally authorized, the CNCI and any other executive-branch action must have some basis in statutory or constitutional law.[32] Several disparate legal authorities offer potential bases for executive responses to cyber threats. These include: (1) various provisions in the criminal code that establish federal cybercrime offenses and authorize prosecution; (2) statutes, such as the Federal Information Security Management Act,[33] which direct executive agencies to establish specific administrative procedures to prevent cyber attacks; (3) more general statutes authorizing executive management of federal agencies; (4) the Authorization for Use of Military Force passed by Congress in 2001,[34] which empowered the President to use "all necessary and appropriate" force against perpetrators of the 9/11 terrorist attacks or those who harbor them; and (4) executive powers inherent in the Commander-in-Chief clause or other constitutional provisions.

Because the CNCI objectives appear to include broad governmental reforms and enhanced partnerships with the private sector, at least some actions contemplated by the CNCI likely fall outside of the relatively straightforward and narrow delegations of authority granted by statutes that specifically address cybersecurity, such as federal criminal law provisions and the Federal Information Security Management Act. As previously noted, the Federal Information Security

---

(...continued)

Conduct Immediate Cyber Security Review, (Feb. 9, 2009), http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/.

[31] U.S. Department of Homeland Security, DHS Data Privacy and Integrity Advisory Committee, *Letter to the Secretary Regarding Data Privacy and Integrity Recommendations*, Executive Summary, Feb. 5, 2009, p. 4.; Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*.

[32] Because the federal government is a government of limited powers, executive actions must find support in either: (1) a power enumerated under Article II of the U.S. Constitution; or (2) authority delegated to the executive by Congress pursuant to one or more of Congress' enumerated Article I powers. Within this framework, some actions are impliedly authorized as means to achieve ends authorized by enumerated powers. *See* McCulloch v. Maryland, 17 U.S. 316 (1819) (upholding Congress' creation of a National Bank as a constitutionally valid means by which to exercise enumerated Article I powers).

[33] 44 U.S.C. §3541 *et. seq.*

[34] Authorization for Use of Military Force, P.L. 107-40, 115 Stat. 224 (2001). For background information on authorizations for use of military force and differences between such authorizations and declarations of war, see CRS Report RL31133, *Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications*, by Jennifer K. Elsea and Richard F. Grimmett.

Management Act requires federal agencies to take steps, such as establishing a Chief Information Officer position, to protect their computer systems from cyber intrusions.[35] In the criminal law context, the federal computer fraud and abuse statute outlaws intrusions upon the security of government computer systems, and in some cases upon the security of computers used in interstate commerce, by trespassing, threats, damage, espionage, or corrupt use of government computers as instruments of fraud.[36] It is likely that some cybersecurity measures envisioned by the CNCI objectives fall outside the scope of both statutory schemes. Most criminal provisions are reactive by nature; they generally do not authorize preventative measures to defend against potential cyber threats, and jurisdictional and practical hurdles could hamper law enforcement's authority over a computer hacker operating abroad. In contrast, the Federal Information Security Management Act and related statutes, like the CNCI, take a preventative approach to stopping cyber intrusions. However, they require federal agencies to take administrative measures that are relatively modest compared with the objectives of the CNCI.

It is possible that some measures contemplated by the CNCI would find authority in statutes that do not explicitly address cyber threats. For example, statutes authorizing executive management of the civil service might authorize some changes to government internet portals or changes in agency personnel.[37] However, such statutes do not address cybersecurity explicitly, nor do they authorize actions taken outside the realm of administrative measures in federal agencies.

Therefore, the existing statutory framework may not provide adequate authority for at least some responses contemplated by CNCI objectives. To fill that possible gap, or to adopt alternative or supplemental approaches, Congress may determine that new legislation is appropriate. Potential legislative approaches are discussed *infra*.[38] However, even if current statutory law is inadequate to protect the country against cyber attacks, it is not necessarily inadequate in the sense of providing insufficient legal authority for the CNCI, because inherent constitutional powers provide an alternative source of legal authority for some executive branch actions. Thus, Congress could decline to act legislatively in some areas, perhaps choosing instead to work with the executive branch in a cooperative or oversight role. If it did so, the executive branch could act in a number of situations by relying on inherent powers under Article II of the U.S. Constitution or, in very limited circumstances, on the 2001 Authorization to Use Military Force.[39]

The Supreme Court's separation-of-powers jurisprudence makes clear that the President may occasionally act pursuant to his inherent powers under the Constitution without express or implied authorization from Congress.[40] Powers most relevant to the CNCI include the President's war and foreign affairs powers.

---

[35] 44 U.S.C. §3541 *et. seq.*

[36] 18 U.S.C. §1030. For an overview of federal cybercrime provisions, see CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

[37] Statutes authorizing executive management of the civil service are codified in Title 5 of the U.S. Code.

[38] The extent of any new law would be limited by individual constitutional rights and by international laws of war.

[39] If the President has authority to act pursuant to powers inherent in the U.S. Constitution, then authority under the Authorization to Use Military Force is unnecessary, and visa versa. Under either source, the scope of executive power might depend upon the intent of and actions taken by Congress.

[40] The executive and legislative branches typically resolve disputes regarding the extent of executive authority without involving the courts. However, the Supreme Court is the final arbiter in such disputes. *See* David J. Barron and Martin (continued...)

Separation of Powers in National Security Matters

The Constitution divides powers relating to national security between the executive and legislative branches. Article I of the U.S. Constitution empowers Congress to "declare war," "raise and support armies," "provide and maintain a navy," and "make rules for the government and regulation of the land and naval forces."[41] Article II states that the "President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States."[42] As a preliminary matter, invocation of war powers begs a question regarding the scope of the Commander in Chief's role in a modern conflict that, not least in the context of cyber warfare, defies traditional military strategies. Many facets of the CNCI – such as components directing planning, development, and education – fall outside of traditional definitions of war. In addition, war powers would likely not apply to actions which mandate private sector security measures. However, many believe the Commander in Chief power extends beyond warfare to encompass a broad conception of national security. In addition, although the phrase "war powers" evokes international conflicts, it seems that the President's war powers authorize at least some domestic action. For example, some have argued that the President's Commander in Chief power authorizes him to create a domestic intelligence agency.[43]

Alternatively, the President's foreign affairs powers might provide an inherent constitutional authorization for executive action on cybersecurity. Given modern communications technology and the ease of travel, it is increasingly difficult to draw clean lines between foreign and domestic affairs. Congress' attempts to distinguish between foreign and domestic actors in other areas impacted by rapidly changing technological environments serve as examples. For instance, in the context of electronic surveillance, statutory provisions have progressed from drawing definitive distinctions between people located in the United States versus abroad in the original Foreign Intelligence Surveillance Act to a 2007 amendment excluding from the scope of foreign surveillance any person "reasonably believed" to be located abroad.[44]

Finally, the President might assert that his oath-based obligation to defend the nation from imminent threats, sometimes termed the "emergency theory," provides a constitutional basis for executive action to prevent cyber intrusions or attacks. Presidents have relied on this authority very rarely.[45]

(...continued)

S. Lederman, *The Commander in Chief at the Lowest Ebb – Framing the Problem, Doctrine, and Original Understanding*, 121 Harv. L. Rev. 689, 722-237 (2008).

[41] U.S. Const. Art. I, §8.

[42] U.S. Const. Art. II, §2, cl.1.

[43] RAND Corp., The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency 108 (2009) (arguing that for establishing a domestic intelligence agency, the Constitution "tilts the balance of power toward the President by virtue of the Commander-in-Chief clause").

[44] The Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§1801 *et seq.*); *see also* Protect America Act, P.L. 110-55 (2007).

[45] Some attorneys within the Bush Administration relied on the emergency powers argument to assert that President Bush had inherent authority to use military force in the war on terror. *See, e.g.*, Memorandum Opinion for the Deputy Counsel to the President, *The President's Constitutional Authority to Conduct Military Operations Against Terrorists* (continued...)

Assuming that the President's war or foreign affairs powers extend to national security efforts such as the CNCI, the next question is whether, and in what circumstances, the executive branch exercise of such powers might be constrained by congressional action. As discussed, Congress and the President share powers to address matters of national security, and no precise line divides the powers of the two political branches. Some have identified a narrow sphere of Article II authority, sometimes called "preclusive" power,[46] which congressional action cannot limit. For most situations, however, Justice Robert Jackson's concurring opinion in *Youngstown Steel & Tube Co.*[47] establishes the leading doctrine governing the executive's inherent constitutional authority vis-a-vis Congress.[48] Justice Jackson's three-category framework requires courts to evaluate, where possible, the interplay between congressional intent and executive action in the context of the Constitution's allocation of powers. This exercise is made more difficult by the murky nature of a small category of inherent constitutional powers some believe are reserved to the President alone.

During the Korean War, President Truman signed an executive order directing the Commerce Secretary to take control of the nation's steel mills in order to prevent a national steelworkers' strike. In *Youngstown*, also known as the "Steel Seizure Case," the government claimed that presidential powers inherent in Article II provisions, most notably the Commander-in-Chief power, authorized President Truman's action.[49] To prove this claim, the government characterized the industry seizure as an action of a Commander in Chief, prompted by exigencies of war: steel production was necessary for military operations in Korea.[50] The Supreme Court rejected this claim,[51] but justices reached the conclusion by different analytical routes.

Writing for the majority, Justice Black took the hard-line view that the Commander-in-Chief clause gives the President no substantive authority. He emphasized that controlling private property to affect labor disputes "is a job for the nation's lawmakers."[52]

In contrast, Justice Jackson argued that the President's inherent constitutional powers "fluctuate," from relatively high when authorized by Congress, to their "lowest ebb" when a president "takes measures incompatible with the express or implied will of Congress."[53] Specifically, Justice

(...continued)

and Nations Supporting Them (Sept. 25, 2001), http://www.usdoj.gov/olc/warpowers925.htm.

[46] The term "preclusive" appeared in Justice Jackson's concurring opinion in *Youngstown Steel and Tube Co.*, 343 U.S. 579 (1952), when he referred to Article I authorities that, if exercised, would preclude a conflicting action by Congress as "at once so conclusive and preclusive [that they] must be scrutinized with caution." 343 U.S. at 638 (Jackson, J., concurring).

[47] 343 U.S. 579 (1952).

[48] *See* Hamdan v. Rumsfeld, 548 U.S. 557, 638 (2006) ("The proper framework for assessing whether executive actions are authorized is the three-part scheme used by Justice Jackson in his opinion in *Youngstown*").

[49] 343 U.S. at 587.

[50] *Id.*

[51] *Id.* The Court noted that "'theater of war' [is] an expanding concept." *Id.* Nonetheless, the Court "[could not] with faithfulness to our constitutional system hold that the Commander in Chief of the armed forces has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production." *Id.*

[52] *Id.*

[53] *Id.* at 635-38 (Jackson, J., concurring).

Jackson articulated three categories of executive action: (1) action supported by an express or implied grant of authority from Congress; (2) a "zone of twilight" between the other categories, in which "congressional inertia" can occasionally "enable, if not invite, measures on independent presidential responsibility"; and (3) action that conflicts with statutes or congressional intent.[54] Actions in the first category enjoy congressional support and thus might not need to rely solely on an inherent constitutional powers argument; assuming that Congress acted pursuant to an enumerated Article I power in delegating the authority, these actions are clearly authorized unless they violate another constitutional provision. Actions in the second, "zone of twilight"[55] category prompt a complicated, totality-of-the circumstances inquiry, in which courts determine congressional intent vis-a-vis executive action. Actions that fall within the third category – that is, actions that conflict with statutory law – generally lack constitutional authority, unless the action is one of the few types of actions over which the President has exclusive authority. In *Youngstown*, Justice Jackson found that President Truman's actions fit within the third category, because Congress had not left the issue of property seizure during labor disputes to an "open field"; rather, Congress had passed statutes designed to stabilize markets when government required supplies.[56] On this basis, Justice Jackson joined the majority to strike down President Truman's seizure of the steel industry.[57]

Given the existing statutory framework, at least some potential responses to cyber threats would likely fall outside of the first of Justice Jackson's categories. Congress has not expressly authorized the cybersecurity reforms proposed by the CNCI, nor do the Federal Information Security Management Act or related statutes appear to impliedly authorize all potential cybersecurity protections. In addition, although the use of cyber force might have congressional authorization under the 2001 Authorization for Use of Military Force[58] if directed against an al Qaeda or Taliban operative, the Supreme Court has appeared to foreclose reliance on the Authorization as a basis for any action that is not a "fundamental" incident to the use of force against those responsible for the 9/11 attacks. The 2001 joint resolution authorized the use of "all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided" the 9/11 attacks.[59] In *Hamdi v. Rumsfeld*, the Supreme Court held that capture and detention of Taliban members constituted "so fundamental and accepted an incident to war as to be an exercise of the 'necessary and appropriate force' Congress has authorized the President to use."[60] The Court seemed reluctant to interpret the Authorization as extending to detentions beyond this "limited category."[61] Cyber security efforts that focus on information gathering activities may parallel the role of intelligence collection as a "central

[54] *Id.*

[55] The phrase "zone of twilight" refers to the mesopelagic region of the ocean – the last region which light reaches, but it also has a non-scientific definition of an indefinite area between two conditions. Under Justice Jackson's framework, the President and Congress might have concurrent authority in this category, such that it is not always clear what, if any, power one branch has to supersede actions of the other.

[56] *Id.* at 639 (Jackson, J., concurring).

[57] *Id.*

[58] P.L. 107-40, 115 Stat. 224 (2001).

[59] P.L. 107-40, 115 Stat. 224 (2001).

[60] 542 U.S. 507, 518 (2004). However, the *Hamdi* court held that such authority is limited by detainees' rights under the due process clause. *Id.*

[61] *Id.*

component of the war on terrorism."[62] However, not all cybersecurity threats fit logically within the scope of the so-called War on Terror. Cyber intrusions conducted by individual computer hackers, not supported by or aligned with a nation or terrorist organization, are perhaps best characterized as ordinary criminal activity whereas orchestrated intrusions by foreign security or intelligence entities might belong in a category of routine foreign-intelligence gathering. Neither activity appears to fit the mold of wartime operations. On the other hand, to the extent that the primary aim of the War on Terror is to prevent terrorists from harming U.S. civilians or assets, one might argue that defending the United States against threats to the U.S. cyber and telecommunications infrastructure fits squarely within the War's parameters.[63] Nonetheless, it seems unlikely that all aspects of the CNCI would fit within the *Hamdi* interpretation of the 2001 Authorization.

On the other hand, unless Congress takes legislative action that contravenes a proposed executive response, the third category in Justice Jackson's framework is inapplicable. In contrast to intelligence collection efforts through the use of electronic surveillance, which Congress explicitly limited in the Foreign Intelligence Surveillance Act,[64] Congress has not expressly limited executive action on cybersecurity. Although Congress has not left the cybersecurity arena an entirely "open field," by virtue of its modest actions with regard to the Federal Information Security Management Act and related provisions, it has not occupied the field to the extent that it had occupied the arena of labor regulation at issue in *Youngstown*.

Therefore, the CNCI and other potential executive actions taken to address cybersecurity likely fall within Justice Jackson's second, "zone of twilight" category, in which the executive and legislative branches have shared authority to act. A 1981 case, *Dames & Moore v. Regan*, refined the Supreme Court's approach to evaluating actions that lie within this "zone of twilight."[65] In *Dames*, then-Justice Renquist, writing for the majority, clarified that in "zone of twilight" cases, the analysis, at least so far as separation-of-powers principles are concerned, "hinges on a consideration of all the circumstances which might shed light on the views of the legislative branch toward [the executive's] action, including 'congressional inertia, indifference or quiescence.'"[66] Thus, the inquiry in such cases becomes a balancing act, aimed toward ascertaining Congress' relationship to the subject matter at issue. In the context of the CNCI, Congress' actions to date on cybersecurity have been primarily criminal or administrative and do not represent a comprehensive response to the issue. In addition, the CNCI involves intelligence and foreign affairs issues that traditionally lie within the purview of the executive branch. Therefore, at least until Congress takes further action in the cybersecurity area, it appears that the executive branch is not precluded from implementing the CNCI or other cybersecurity responses under Justice Jackson's *Youngstown* framework.

---

[62] David J. Barron and Martin S. Lederman, *The Commander in Chief at the Lowest Ebb – Framing the Problem, Doctrine, and Original Understanding*, 121 Harv. L. Rev. 689, 714 (2008) ("a central component of the war against terrorism is, by its nature, the collection of intelligence").

[63] *See Id.* (noting that the war on terrorism differs from conventional conflicts, in part, because "the Executive has identified its principal goal in this conflict not as defeating the enemy in battle, but as preventing the enemy from 'fighting' in the first place").

[64] 50 U.S.C. §§1801 *et seq*.

[65] 453 U.S. 654 (1981).

[66] *Id*. at 669.

A final issue is whether responses to cybersecurity intrusions or attacks might be part of the narrow realm of "preclusive" constitutional powers belonging to the President.[67] Although the scope of, and even the constitutional authority for, such powers has never been fully defined, scholars have noted that a few key rules form a "rarely questioned narrative" regarding arenas in which Congress traditionally defers to executive action.[68] For example, traditional notions dictate executive direction of wartime campaigns.[69] Likewise, the Supreme Court has characterized the President as the "sole organ" of the country in conducting foreign affairs.[70] In addition, some have suggested a distinction between offensive utilization of cyber weapons versus defensive shield to stop attacks:[71] whereas the President must obtain congressional authorization before committing U.S. armed forces in an offensive action, the President's has the exclusive power to repel attacks made against the United States.

Despite this narrative, however, no definitive boundaries have been defined for any such preclusive powers. Perhaps for that reason, Justice Jackson made clear in his *Youngstown* concurrence that the realm of any such preclusive powers must be carefully scrutinized.[72] Thus, although many executive actions in the cyber area would likely fall within the scope of Article II powers for ensuring national security, most actions would probably falls outside of the narrow categories of exclusive executive authority to conduct wartime campaigns and international relations. Similarly, even if the President has an exclusive power to lead the military in defensive actions, actions might not be clearly enough a defensive response to a military threat to trigger an exclusive presidential power.[73]

---

[67] Scholars have expressed doubts regarding the framers' intent to imbue the President with "preclusive" constitutional powers but nonetheless have argued that long-standing assumptions that such powers exist have solidified their constitutional standing. *See, e.g.*, David J. Barron and Martin S. Lederman, *The Commander in Chief at the Lowest Ebb – Framing the Problem, Doctrine, and Original Understanding*, 121 Harv. L. Rev. 689, 802 (2008).

[68] *See, e.g Id*. at 698. For more information regarding divisions between Congress' and the President's war powers and an analysis of that division in the context of the President's authority to use commit armed forces in Iraq, see CRS Report RL33837, *Congressional Authority to Limit U.S. Military Operations in Iraq*, by Jennifer K. Elsea, Michael John Garcia, and Thomas J. Nicola.

[69] *See Hamdan v. Rumsfeld*, 548 U.S. 557, 591-92 (2006) (citing *Ex Parte Milligan*, 71 U.S. 2, 139-40 (1866)). *But see* War Powers Resolution, 50 U.S.C. §§1541-1548, discussed *infra*.

[70] *See United States v. Curtiss-Wright Export Co.*, 299 U.S. 304, 319 (1936) ("'The President is the sole organ of the nation in its external relations, and its sole representative with foreign nations.'" (citing Annals, 6th Cong., col. 613 (statement of John Marshall))). However, the *Curtiss-Wright* case involved executive action that fell in the first of Justice Jackson's *Youngstown* categories – i.e., where Congress and the President acted in concert. Thus, although the case has helped to form a narrative regarding executive-branch prerogative in international relations and has occasionally been cited to support the proposition that the President has some preclusive foreign affairs powers under the Constitution, it would misstate the *Curtiss-Wright* holding to assume that it recognized any broad preclusive foreign relations power.

[71] Aside from the operational distinction that may be made with respect to the types of cyber activities the U.S. may undertake, the offensive versus defensive distinction may also be worth considering from an organizational perspective. Agencies responsible for protecting the government's websites and launching counter-offensive attacks may not be the same entities responsible for assisting in the recovery phase of an attack of national security significance on a U.S. cyber or telecommunications hosted network.

[72] 343 U.S. at 638 (Jackson, J., concurring).

[73] In the context of modern national security threats, the line between offensive and defensive action is not easily deciphered. For example, the United States captured and detained a large number of alleged enemy combatants in the course of post-September 11th military operations. Is the ongoing detention of such persons, often referred to as "preventative detention," an offensive action? The Supreme Court has upheld executive authority for such detentions (continued...)

Thus, it appears that the *Youngstown* framework would apply to a review of the President's authority to implement responses such as the CNCI. Thus, if Congress passed conflicting legislation in the cybersecurity area, some executive actions could be constrained. Alternatively, congressional legislation granting explicit authority for cybersecurity measures would more firmly confirm the executive authority to act in that area.

It is possible that the Supreme Court will address the constitutional authorities for national security in a future case. *Youngstown* represents one of only a small number of cases in which the Supreme Court has reached questions regarding the political branches' shared powers under the Constitution. Modern threats might necessitate new definitions within the Court's separation-of-powers jurisprudence. For example, as cyber activities and telecommunication architectures are networked globally, with it often being difficult to ascertain where an attack or intrusion emanates, distinctions based on notions of conventional war may seem increasingly inconsistent with the modern Commander-in-Chief role.

Congressional Constraints on Executive Action

Even if the CNCI or future cybersecurity initiatives are grounded in statutory or constitutional authority, questions will nonetheless arise regarding the degree to which legislative oversight is appropriate. Congress has attempted to obligate the President to report to relevant congressional leaders for actions taken pursuant to war powers or as part of intelligence operations. In 1973, Congress passed the War Powers Resolution to "fulfill the intent of the framers of the Constitution of the United States and insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities."[74] Although presidents since the Resolution's passage have maintained that the Resolution unconstitutionally limits presidential authority, presidents have in many cases submitted documents for Congress that are "consistent with" the Resolution's requirements.[75]

Similarly, after the Iran-Contra affair, Congress passed legislation increasing congressional oversight of intelligence activities, including significant and anticipated intelligence activities, and covert actions.[76] To the extent consistent with due regard for preventing unauthorized disclosure of classified information regarding sensitive intelligence sources and methods, current law requires that congressional intelligence committees be kept fully informed regarding intelligence activities. If the President determines that it is essential to meet extraordinary

(...continued)

on statutory rather than constitutional grounds; it has not addressed offensive versus defensive distinction. *Hamdi*, 542 U.S. 507. Thus, even if some components of the CNCI qualify as war-related activity, perhaps because they target cyber terrorists, little guidance exists regarding which actions might qualify as defensive rather than offensive actions under the traditional war powers analysis.

[74] War Powers Resolution, P.L. 93-148, 87 Stat. 555 (1973) (codified at 50 U.S.C. §§1541-1548); 50 U.S.C. §1541(a).

[75] For information Presidential actions vis-a-vis the War Powers Resolution, see CRS Report RL33532, *War Powers Resolution: Presidential Compliance*, by Richard F. Grimmett.

[76] Fiscal Year 1991 Intelligence Authorization Act, P.L. 102-88, 105 Stat. 429 (1991) (codified as amended at 50 U.S.C. §§413, 413a, 413b).

circumstances affecting vital U.S. interests, a presidential finding regarding a covert action may be limited to a small number of congressional leaders.[77]

With respect to the CNCI, a key question is whether ongoing or potential U.S. cyber activities, defensive and offensive, may fall within the sphere of a covert activity or an intelligence activity and thus trigger reporting requirements. The statutory definition of "covert actions" includes "activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly," but excludes activities conducted for the purpose of gathering intelligence and "traditional" diplomatic, military, or law enforcement activities.[78] The definition of "intelligence activity" is broader; it includes covert actions and "financial intelligence activities."[79] Because the definitions focus on the influence, rather than the presence, of conditions abroad, it appears that cyber actions targeting or even defending against cyber threats, even if conducted inside the United States, could trigger reporting requirements.

In addition to the potential application of ongoing reporting requirements, Congress could elicit information regarding executive actions by virtue of its enumerated power to control spending. The 110th Congress took several steps to obtain information regarding the CNCI in that manner. A continuing resolution, passed by Congress and signed into law in September 2008, withholds $127 million of a $313.5 million appropriation for cybersecurity until House and Senate appropriations committees "receive and approve a plan for expenditure for [the CNCI] that describes the strategic context of the program; the specific goals and milestones set for the program; and the funds allocated to achieving each of those goals."[80] In addition, the Senate Committee on Homeland Security and Governmental Affairs held a closed hearing in March 2008 regarding the CNCI and later obtained answers to some questions regarding the initiative.[81] Finally, as part of a larger Homeland Security Authorization bill, S. 3623, Senator Lieberman introduced legislation during the 110th Congress that would provide for congressional oversight of the CNCI and establish "a robust National Cyber Security Center with the mission of coordinating and enhancing federal efforts to protect government networks."[82] As an authorization bill for the DHS has not been passed since the creation of the Department, whether the proposed legislative oversight efforts will be effective remains to be seen. Also, as with many programs associated with intelligence community activities and defense, concerns regarding committee jurisdiction in the areas of oversight, authorization, and appropriations might be raised for the CNCI.

---

[77] For more information on congressional oversight of covert actions, see CRS Report RL33715, *Covert Action: Legislative Background and Possible Policy Questions*, by Alfred Cumming.

[78] 50 U.S.C. §413b(e).

[79] 50 U.S.C. §413(f).

[80] Consolidated Security, Disaster Assistance, and Continuing Appropriations Act of 2009, P.L. 110-329, (2008).

[81] NSPD-54/HSPD-23 and the Comprehensive National Cyber Security Initiative: Hearing Before the Sen. Homeland Security and Governmental Affairs Comm., 110th Cong. (March 4, 2008).

[82] S. 3623, 110th Cong. §§601-08 (2008); 154 Cong. Rec. S9687 (daily ed. Sept. 26, 2008) (statement of Sen. Lieberman).

Policy Considerations and Congressional Options

As with executive control over covert actions, foreign affairs, and intelligence gathering, strong justifications support the assertion that the executive branch is best suited to take reasonable and necessary actions to defend the country against cyber-based threats. One such justification stems from the broad diversity of cybersecurity threats: the President is arguably best positioned to take a leadership role or create a uniform response to span the range of cyber vulnerabilities. In addition, the executive branch is likely most able to integrate intelligence-gathering, military, and other vehicles for addressing the cybersecurity challenge. However, in order for Congress to maintain ongoing awareness of CNCI plans and activities and to effectively perform its constitutional duties of oversight based on a thorough understanding of executive branch activities, some security experts suggest a range of legislative activities that might be required. Congress might choose to:

- determine the most appropriate and effective organizational entity in which the nation's principal cybersecurity prevention, response, and recovery responsibilities should reside;[83]
- require the senior U.S. government official in charge of all CNCI related activities be a Senate confirmable position to facilitate ongoing information exchange regarding Initiative plans and areas of progress and difficulty;
- enact legislative language recognizing and defining the classified and unclassified aspects of the CNCI and the need for greater transparency and inclusiveness;
- require the new Administration to develop and revise annually a classified and unclassified national cyber security strategy and intelligence community generated National Intelligence Estimate that provides Congress, the telecommunications industry, and the American public information related to the CNCI, the current and strategic cyber threats facing the nation, and programs being implemented to prepare for evolving technological risks;
- define the privacy and civil liberty considerations that should accompany all aspects of the CNCI;
- include legislative language in applicable authorizations bills to establish a programmatic foundation for CNCI related programs and suggest funding for current and future year's activities; or
- identify and codify relevant laws defining a national security related cyber offense against the United States, offensive versus defensive cyber activities, and

[83] Possible organizational constructs for such an entity range from a single entity placed in charge of all phases of U.S. cyber activity to a coordination office with the authority and responsibility to compel other organizations to adhere to the President's cyber strategy. Entities often noted as having a significant contribution to the U.S. cyber activity, which could add capability and resources to the CNCI's capabilities, include the cyber and telecommunications industries, intelligence and law enforcement communities, and academia.

the situations in which the Congress should be notified prior to the United States undertaking an offensive or counteroffensive cyber act.

Conclusion

As discussed, multiple policy considerations, including the novel and dispersed nature of cyber threats, might justify an executive-led response to cybersecurity. In response to calls for executive action, questions have arisen regarding the adequacy of legal authorities justifying executive responses to cyber threats. Although existing statutes might support some executive actions, the current statutory framework likely does not address all potential actions. Thus, the extent of inherent powers under Article II of the Constitution and the appropriate roles of the two political branches in this emerging national security arena are relevant considerations. Arguably, both the statutory framework and separation of powers analyses might need to be modernized to address appropriate roles in protecting the United States against modern cyber threats.

Finally, even if executive branch responses are authorized, Congress retains an oversight role vis-à-vis the CNCI or other presidential initiatives, for several reasons. First, if Congress passed statutes in contravention of the President's efforts, the President's authority to proceed with those efforts would become more questionable under the *Youngstown* framework. Second, as with covert actions, Congress likely has a legislative oversight role, even if that role merely requires notice of significant actions. Finally, Congress could ultimately withhold funding for the CNCI or specific aspects of the program should it not receive the necessary information to make an assessment of the activities related to each of the twelve objectives.

Author Contact Information

John Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

Anna C. Henning
Legislative Attorney
ahenning@crs.loc.gov, 7-4067