President Obama speaks at DHS about how his budget would safeguard cyberspace and strengthen national preparedness and resilience (DHS/Jetta Disco)

Detangling the Web

A Screenshot of U.S. Government Cyber Activity

By G. Alexander Crowther and Shaheen Ghori

The world must collectively recognize the challenges posed by malevolent actors' entry into cyberspace, and update and strengthen our national and international policies accordingly. Activities undertaken in cyberspace have consequences for our lives in physical space, and we must work towards building the rule of law, to prevent the risks of logging on from outweighing its benefits.

—U.S. International Strategy for Cyberspace, May 2011

Blackouts. School testing. Electrical grids. Insurance. These all have one major thing in common: they have all been targets for cyber attacks in a period of two weeks during March 2015. The United States faces thousands of cyber assaults every day. States, state-sponsored organizations, other groups and individuals all combine to incessantly probe, spy on, and attack public and private organizations as well as denizens of the United States. These ongoing problems require a U.S. Government response, so it adopted a bureaucratic approach that

Dr. G. Alexander Crowther is Deputy Director of the Center for Technology and National Security Policy (CTNSP), Institute for National Strategic Studies, at the National Defense University. Shaheen Ghori has a Bachelor of Arts in International Relations from American University and is entering the Intelligence Community.

has resulted in a complex system that is constantly evolving as new problems are recognized. This article provides a comprehensive look at how the United States has organized to address these challenges. Although U.S. Government efforts seem sizable, private use of the Internet dwarfs government usage.[1]

Policies and Strategies

The U.S. Government articulates its cyber policy through a series of initiatives, policy decisions, and published strategies. The foundational document of the U.S. Government's approach to cyber policy is National Security Policy Decision 38, *The National Strategy to Secure Cyberspace*, dated July 7, 2004. Since its publication, a number of new policies and strategies have appeared that refine the government's approach. A short list includes:

- *Comprehensive National Cybersecurity Initiat*ive, March 2, 2010
- *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, July 6, 2010
- *International Strategy for Cyberspace*, May 2011
- Presidential Policy Directive (PPD) 20, *U.S. Cyber Operations Policy*, October 16, 2012
- National Cybersecurity Protection Act of 2014, December 18, 2014
- Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing,* February 13, 2015.

The capstone document is the 2015 *National Security Strategy*, which states:

Our economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution. Drawing on the voluntary cybersecurity framework, we are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure.[2]

The President has further refined the document and identified his five priorities for cyber issues:[3]

- protecting the country's critical infrastructure—our most important information systems—from cyber threats
- improving the public- and private-sector abilities to identify and report cyber incidents to enable responses in a timely manner
- engaging with international partners to promote Internet freedom and build support for open, interoperable, secure, and reliable cyberspace
- securing Federal networks by setting clear security targets and holding agencies accountable for meeting targets
- shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.

Cyber Legislation

The Executive Branch's approach to the U.S. Government's cyber posture has yet to be mirrored in legislation affecting the private sector. There are four major problems. First is the sheer size and complexity of the U.S. infosphere, still the largest national component of the global system. The second involves conflicting political aims—the desire to provide effective information-sharing to identify potential threats versus the deeply ingrained national desire for personal privacy and suspicion of government overreach. The size and nature of the U.S. economy poses a third challenge. Private companies fear that information-sharing will lead to exposure to potential prosecution, the loss of proprietary information to competitors, and a loss of faith by their customers. A fourth challenge is the free-rider problem, with many participants in information-sharing schemes absorbing more information than they contribute, and with many participants treating information-sharing as marketing opportunities for their own security solutions.[4]

Legislation has fallen short for these reasons as well as the challenges of operating in a highly polarized partisan environment. The last major cyber legislation dates to 2002. Congress came close to passing comprehensive cyber security legislation in 2012 and 2013.[5] Efforts failed in 2012 because business balked at the prescriptive nature of proposed legislation, while the 2013 proposed legislation was overcome by political maneuvering leading up to the closing of the U.S. Government. Congress did pass the National Cybersecurity Protection Act,[6] Federal Information Security Modernization Act,[7] and Department of Homeland Security Cybersecurity Workforce Recruitment and Retention Act[8] in December 2014, which address various aspects of cyber security in the United States. Congress is currently working on comprehensive cyber legislation designed to address indemnity and liability with the goal of passing the legislation in the summer of 2015.

At the level of implementing the national-level policies and strategies, the boundaries between the various Federal agencies have also evolved. Today, the Department of Homeland Security (DHS), Department of Justice, and Department of Defense (DOD) share prominence but play discrete roles in countering the cyber threat.

Department of Homeland Security

DHS coordinates the national protection, prevention, and mitigation of and recovery from cyber incidents; disseminates domestic cyber threat and vulnerability analysis; protects critical infrastructure; secures Federal civilian systems (the dot.gov domain); and investigates cyber crimes under its jurisdiction.

The DHS vision is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards.[9] One of the five core missions of DHS is to safeguard and secure cyberspace, which involves the following components:

- strengthen the security and resilience of critical infrastructure
- secure the Federal civilian government information technology enterprise
- advance law enforcement, incident response, and reporting capabilities
- strengthen the (cyber) ecosystem.[10]

Subject matter expert assigned to Navy Information Assurance and Cyber Security Program Office demonstrates tactical key loader cryptographic key fill device (U.S. Navy/Rick Naystatt)

DHS essentially sees itself as facilitating the cyber neighborhood watch for the United States.[11] The core division of DHS that addresses cyber threats is the National Protection and Programs Directorate (NPPD), whose primary goal is to reduce the risks of homeland threats and make the physical and digital infrastructure of the U.S. Government more resilient and secure.[12] Within the NPPD, the most prominent cyber security offices are the Office of Cybersecurity and Communication (CS&C), Office of Infrastructure Protection, and Office of Cyber and Infrastructure Analysis. Outside of the NPPD, cyber security operations also take place within U.S. Immigrations and Custom Enforcement and the U.S. Secret Service.

CS&C works to prevent or minimize disruptions to critical information networks to protect the public, economy, and government services. It also leads efforts to protect the Federal dot.gov domain of civilian government networks and collaborate with the private sector—the dot.com domain—to increase the security of critical networks.[13] CS&C carries out its mission through its five divisions:

- The Office of Emergency Communications
- The National Cybersecurity and Communications Integration Center
- Stakeholder Engagement and Cyber Infrastructure Resilience
- Federal Network Resilience
- Network Security Deployment.

The CS&C Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division is the primary DHS point of engagement and coordination for national security/emergency preparedness (NS/EP) communications and cybersecurity initiatives for both government and industry partners, and is the Executive Secretariat for the Joint Program Office for the NS/EP Communications Executive Committee. CS&C relies on SECIR to streamline coordination and engagement with external partners, while leveraging capabilities and significant subject matter expertise to meet stakeholder requirements.[14]

The National Cybersecurity and Communications Integration Center (NCCIC) serves as a focal point for coordinating cyber security information-sharing with the private sector; provides technical assistance, onsite analysis, mitigation support, and assessment assistance to cyber attack victims, as well as situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact

critical infrastructure; and coordinates the national response to significant cyber incidents affecting critical infrastructure.[15] Under the National Infrastructure Protection Plan framework, the collaborative activity of the NCCIC blends together the interdependent missions of the National Coordinating Center for Telecommunications, U.S. Computer Emergency Readiness Team (US-CERT), DHS Office of Intelligence and Analysis, and National Cyber Security Center.[16] The NCCIC mission is to reduce the likelihood and severity of incidents against the Nation's critical technology and communications networks[17] and to build capacity and resilience in other organizations[18] through its four branches: the NCCIC Operations and Integration, US-CERT, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and National Coordination Center for Communications (NCC).

US-CERT provides a single accountable focal point to improve the Nation's cyber security posture, coordinate cyber information-sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans.[19] Additionally, US-CERT collaborates with Federal agencies; the private sector; the research community; academia; state, local, and tribal governments; and international partners. Through coordination with various national security incident centers in responding to potential security events and threats on both classified and unclassified networks, US-CERT disseminates cyber security information to the public.[20]

ICS-CERT operates cyber security operations centers that focus on responding to and analyzing control systems–related incidents; conducting vulnerability, malware, and digital media analysis; providing onsite incident response services; providing situational awareness in the form of actionable intelligence; coordinating the responsible disclosure of vulnerabilities and associated mitigations; and sharing and coordinating vulnerability information and threat analysis through information products and alerts.[21]

The NCC continuously monitors national and international incidents and events that may impact emergency communications. NCC works with both US-CERT and ICS-CERT to monitor and resolve issues impacting cyber and communications during an emergency.[22]

The Office of Infrastructure Protection leads the coordinated national effort to reduce risk to critical U.S. infrastructure and to help respond and quickly recover in case of terrorist attacks, natural disasters, or other emergencies. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators, as well as state, local, tribal, and territorial partners understand and address risks.[23] The office is the sector-specific agency for six of the critical infrastructure sectors: chemical, commercial facilities, critical manufacturing, dams, emergency services, and nuclear,

The Office of Cyber and Infrastructure Analysis implements PPD 21, which calls for integrated analysis of critical infrastructure, and Executive Order 13636, which identifies critical infrastructure where cyber incidents could have catastrophic impacts to public health and safety, the economy, and national security. The mission is to support efforts to protect the Nation's critical infrastructure by providing analytic support to DHS leadership, operational components, and field personnel during steady-state operations and crises on emerging threats and incidents; assessing and informing national risk management strategies on the likelihood and consequence of emerging and future risks; and developing and enhancing capabilities to support crisis actions by identifying and prioritizing infrastructure through the use of analytic tools and modeling capabilities.[24]

Homeland Security Investigations (HSI) operates the Cyber Crime Center (C3), which is responsible for providing domestic and international training and the support, coordination, and deconfliction of cyber investigations related to online economic crime, digital theft of export-controlled data, digital theft of intellectual property, and online child exploitation investigations. This state-of-the-art center offers cyber crime support and training to Federal, state, local, and international law enforcement agencies.[25] The most important sector of the C3 in dealing with cyber security is the Cyber Crimes Unit, which provides the management and oversight of the agency's cyber-related investigations by focusing on the transnational criminal organizations that use cyber capabilities to further their capital enterprise. This unit provides training, investigative support, and guidance to HSI field offices in emerging cyber technologies as well as subject matter expertise in cyber-related investigations related to identity and benefit document fraud, money-laundering, financial fraud, commercial fraud, counterproliferation investigations, narcotics-trafficking, and illegal exports.[26]

The Secret Service leads a network of electronic crimes task forces to bring together Federal, state, and local law enforcement, prosecutors, private industry, and academia for the common purpose of preventing, detecting, mitigating, and investigating various forms of malicious cyber activity. The Secret Service also runs the National Computer Forensics Institute, a training center dedicated to providing state and local law enforcement and legal and judicial professionals a free, comprehensive education on current cyber crime trends, investigative, methods, and prosecutorial and judicial challenges.[27]

Department of Justice

The Department of Justice investigates, attributes, disrupts, and prosecutes cyber crimes; has the lead for domestic national security operations; conducts domestic collection, analysis, and dissemination of cyber threat intelligence; supports the national protection, prevention, mitigation of, and recovery from cyber incidents; and coordinates cyber threat investigations.

Justice developed its 2014–2018 strategy to include priorities and programs that address the President's priorities.[28] Its number one goal is to "prevent terrorism and promote the nation's security consistent with the rule of law," and it aligns cyber efforts under that goal. It intends to combat cyber-based

threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors.[29] Its cyber strategy involves an all-tools approach including both investigation and prosecution, with a focus on the disruption of the threat.[30]

The Federal Bureau of investigation (FBI) leads the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud by gathering and sharing information and intelligence with public- and private-sector partners worldwide.[31] It has developed a number of initiatives to perform these missions. Internally, the headquarters now contains the Cyber Division to bring together various FBI cyber initiatives and missions and has placed cyber task forces in all 56 field offices to focus exclusively on cyber security threats and synchronize domestic cyber threat investigations in the local community.[32]

The Cyber Action Team (CAT) is the FBI Cyber Division's investigative rapid response team that can be on scene within 48 hours. The CAT mission is to deploy globally at the direction of FBI Cyber Division to bring in-depth cyber intrusion expertise and specialized investigative skills to initiatives, cases, and emergencies deemed critical and significant. When deployed, CAT objectives are to provide support to the local field office to make the case move as quickly and effectively as possible and to provide detailed intrusion analysis using a blend of FBI investigative techniques.

Today, the National Cyber Investigative Joint Task Force (NCIJTF) is the focal point for government agencies to coordinate, integrate, and share information related to domestic cyber threat investigations. The FBI is the executive agent for the joint task force and partners with the National Security Agency (NSA), Central Intelligence Agency, Secret Service, DHS, and United States Cyber Command (USCYBERCOM). Its five mission areas include coordinating whole-of-government campaigns against known cyber threats, exploiting valuable cyber data, analyzing and reporting on that data, applying traditional financial investigative approaches to the cyber domain, and maintaining an around-the-clock cyber incident management watch. Because task force members represent many state, Federal, and international jurisdictions, collaboration at the NCIJTF is critical to ensuring that all legal means and resources available are used to track, attribute, and take action against these cyber threats and to ultimately place international cyber criminals behind bars and off our global networks.

Other examples of cyber collaboration fostered by the FBI are:

- InfraGard, an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.
- The National Cyber-Forensics and Training Alliance, which has become an international model for bringing together law enforcement, private industry, and academia to share information to stop emerging cyber threats and mitigate existing ones.[33]
- The Strategic Alliance Cyber Crime Working Group, started at FBI headquarters in September 2006, which consists of cyber law enforcement bodies from Australia, Canada, New Zealand, the United Kingdom, and the United States.[34]

The Justice Department's National Security Division and Criminal Division each concentrates on its own cyber issues. The division deals with cyber-based threats to the national security.[35] It created the National Security Cyber Specialist network that is a new tool in the government's cyber toolkit and a critical part of the department's efforts to better address cyber intrusions and attacks carried out by nation-states or terrorist organizations.[36]

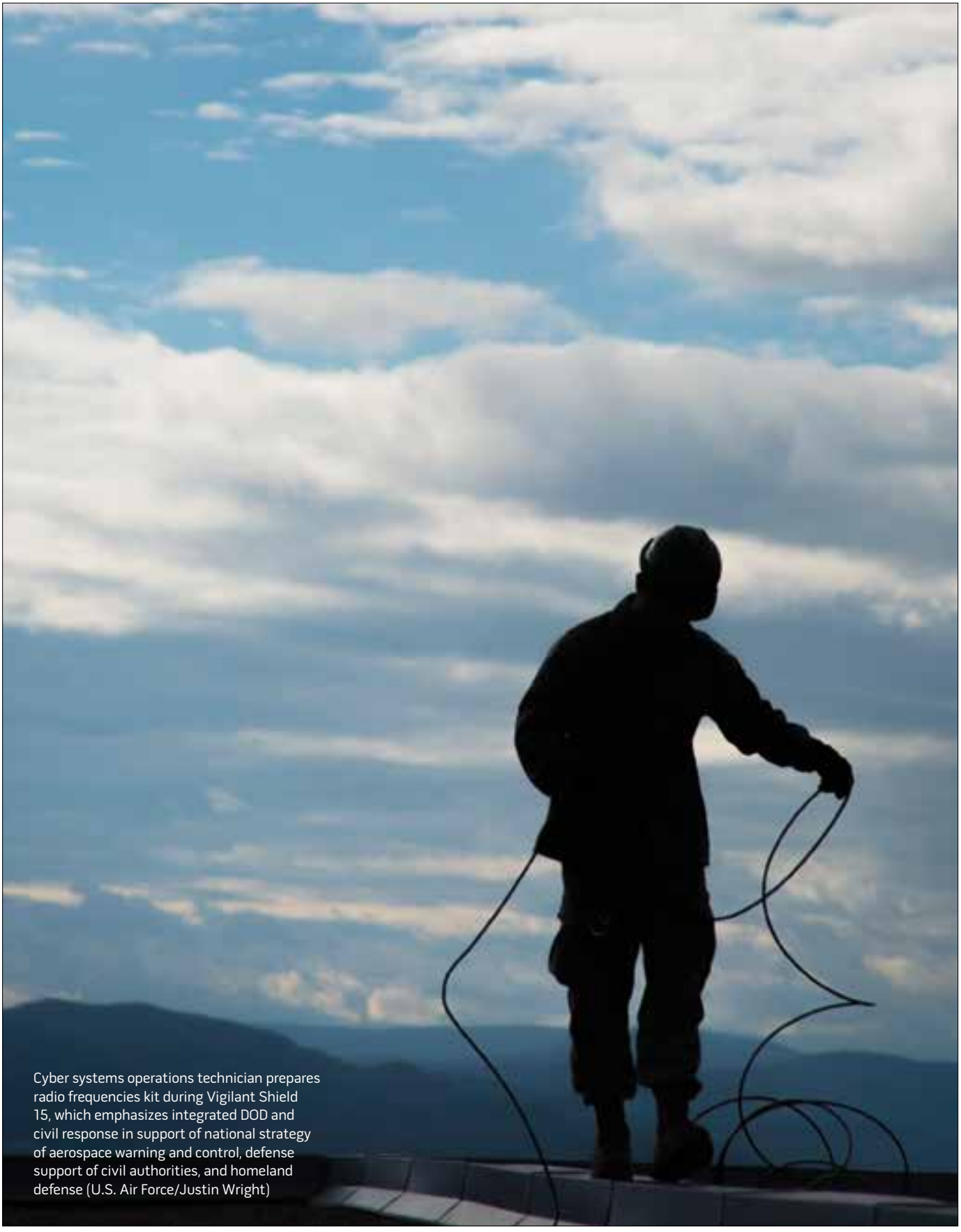
The Criminal Division contains the Computer Crime and Intellectual Property Section (CCIPS), which implements Justice's national strategies in combating computer and intellectual property crimes worldwide. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. In pursuing all these goals, CCIPS attorneys regularly run complex investigations; resolve unique legal and investigative issues raised by emerging computer and telecommunications technologies; litigate cases; provide litigation support to other prosecutors; train Federal, state, and local law enforcement personnel; comment on and propose legislation; and initiate and participate in international efforts to combat computer and intellectual property crime.[37]

The Offices of the U.S. Attorneys is the last major part of Justice that works cyber issues. One of their 10 priority areas is cyber crime.[38] Their three areas of concentration are Internet stalking, computer hacking, intellectual property rights and forensics. They also assist the National Computer Forensics Institute.

Department of Defense

The DOD mission is to secure the Nation's freedom of action in cyberspace and help mitigate risks to national security resulting from America's growing dependence on cyberspace. Specific mission sets include directing, securing, and defending DOD Information Network (DODIN) operations (including the dot.mil domain); maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; and providing support to civil authorities and international partners.[39]

DOD articulates its cyber policy through the *DOD Strategy for Operating in Cyberspace*, dated July 2011, and Joint Publication 3-12, *Cyberspace Operations*, dated February 5, 2013. DOD's operations are designed to achieve and maintain *cyberspace superiority*, defined as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary."[40] DOD organizations are allowed



Cyber systems operations technician prepares radio frequencies kit during Vigilant Shield 15, which emphasizes integrated DOD and civil response in support of national strategy of aerospace warning and control, defense support of civil authorities, and homeland defense (U.S. Air Force/Justin Wright)

to perform defensive cyber operations; however, full-spectrum cyber operations (including offensive cyber operations) are approved by the President and directed by the Secretary of Defense.[41]

Combatant Commands (CCMDs) provide operations instructions and command and control to the Armed Forces and have a significant impact on how they are organized, trained, and resourced—areas over which Congress has constitutional authority.[42] CCMDs share cyber information largely through USCYBERCOM and their own joint cyber centers, but various personnel also meet periodically to share information in collaboration sessions.[43]

The National Security Agency is the Nation's cryptologic organization that coordinates, directs, and performs highly specialized activities to protect U.S. information systems and to produce foreign signals intelligence information. It supports military customers, national policymakers, and the counterterrorism and counterintelligence communities, as well as key international allies. The NSA also shares information about software vulnerabilities with vendors and users in any commercial product or system (not just software) used by the United States and its allies, with an emphasis on risk mitigation and defense.[44]

The Defense Information Systems Agency (DISA) provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. They are overall responsible for DODIN. Each Service also has its own equivalent to DISA that operates its part of DODIN.

The Defense Cyber Crime Center delivers superior digital forensics and multimedia laboratory services, cyber technical training, research, development, testing and evaluation, and cyber analysis capabilities supporting cyber counterintelligence and counterterrorism, criminal investigations, intrusion forensics, law enforcement, the Intelligence Community, critical infrastructure partners, and information operations for DOD.[45]

USCYBERCOM was formed in 2010 by consolidating two U.S. Strategic Command (USSTRATCOM) subordinate organizations: the Joint Functional Component Command–Network Warfare and Joint Task Force–Global Network Operations.[46] It is a subunified command under USSTRATCOM. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified DODIN. It also prepares, when directed, to conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure U.S./allied freedom of action in cyberspace and deny the same to adversaries.[47]

USCYBERCOM's main instrument of power consists of the Cyber National Mission Force, which conducts cyberspace operations to disrupt and deny adversary attacks against national critical infrastructure. It is the U.S. military's first joint tactical command with a dedicated mission focused on cyberspace operations. It plans to create 133 cyber mission teams by the end of fiscal year 2016, which will consist of National Mission Teams, which perform full-spectrum cyber operations; National Support Teams, which provide direct support to the National Missions Teams; and National Cyber Protection Teams, which protect whomever they are assigned to.

Combat Mission Forces are similar to the National Mission Teams but rather than serving at the national level, they conduct cyberspace operations to achieve combatant commanders' objectives and are geographically and functionally aligned under one of four Joint Force Headquarters–Cyber (JFHQ-C) in direct support of geographic and functional CCMDs:

- JFHQ-C Washington supports U.S. Special Operations Command, U.S. Pacific Command, and U.S. Southern Command.
- JFHQ-C Georgia supports U.S. Central Command, U.S. Africa Command, and U.S. Northern Command.
- JFHQ-C Texas supports U.S. European Command, USSTRATCOM, and U.S. Transportation Command.[48]
- JFHQ-DODIN defends DOD information networks at USCYBERCOM.[49]

The Services and Cyber. The Service chiefs will provide cyber operations capabilities for deployment/support to CCMDs as directed by the Secretary of Defense and remain responsible for compliance with USSTRATCOM's direction for operation and defense of the DODIN.[50] In addition to the joint strategy and doctrine, each Service also has its own doctrine to deal with cyber issues:

- The Army publishes Field Manual 3-38, *Cyber Electromagnetic Activities*, and is currently developing a new Cyber Branch and Military Occupational Specialty to facilitate the development of its cyber workforce.
- The Navy has a set of approaches including the *Department of the Navy Cybersecurity/Information Assurance Workforce Management, Oversight and Compliance*; the *Navy Information Dominance Corps Human Capital Strategy 2012–2017*; *Navy Cyber Power 2020*; the *U.S. Navy Information Dominance Roadmap 2013–2028*; and the *Navy Strategy for Achieving Information Dominance 2013–2017*. The Service created the Information Dominance Corps, a unified body that produces precise, timely warfighting decisions[51] by bringing together the intelligence, information professional, information warfare, meteorology and oceanography communities, and members of the space cadre.
- The Marine Corps has Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations*. The Service recognizes five types of cyber operations: network operations, defensive and offensive cyber operations, computer network exploitation, and information assurance.
- The Air Force codified its cyber doctrine in Air Force Doctrine Document 3-12, *Cyberspace Operations*, published in 2010 and updated in 2011.[52]

It has also created its own cyber branch by carving out part of the Air Force communications community.

Each of the Services also has its own cyber organizations. Under their Title 10 role as force providers to the combatant commanders, the Services recruit, train, educate, and retain the military cyber force. These are U.S. Army Cyber Command/2nd U.S. Army, U.S. Fleet Cyber Command/U.S. 10th Fleet, 24th Air Force, and U.S. Marine Corps Forces Cyber Command.[53]

Service-Specific Structure. U.S. Army Cyber Command or 2nd U.S. Army is the single information technology provider for all network communications and is responsible for the Army section of the DODIN.[54] The U.S. Intelligence and Security Command conducts intelligence, security, and information operations for military commanders and national decisionmakers.[55] The command is also responsible for the Joint Forces Headquarters Cyber in Georgia.

U.S. Fleet Cyber Command (FCC) and 10th Fleet compose combined headquarters at Fort Meade, Maryland. FCC is the staff organization to organize forces, and 10th Fleet is the operational staff that provides command and control.[56] FCC has a mission set similar to the other Services: direct cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; organize and direct cryptologic operations worldwide and support information operations and space planning and operations, as directed; execute cyber missions as directed; direct, operate, maintain, secure, and defend the Navy's portion of the DODIN; deliver integrated cyber, information operations, cryptologic, and space capabilities; deliver global cyber network operational requirements; assess cyber readiness; and manage, man, train, and equip functions associated with Navy Component Commander and Service Cryptologic Commander responsibilities.[57] The mission of 10th Fleet is to serve as the Numbered Fleet for Fleet Cyber Command and exercise operational control of assigned forces and to coordinate with other naval, coalition, and joint task forces to execute the full spectrum of cyber, electronic warfare, information operations, and signal intelligence capabilities and missions across the cyber, electromagnetic, and space domains.[58]

Marine Corps Forces Cyber Command has two subordinate elements: the Marine Corps Network Operations and Security Center and L Company of the Marine Corps Support Battalion.[59] It has also been innovative in its deployment of cyber forces, with the Marine Air-Ground Task Force Cyberspace and Electronic Warfare Coordination Cell being embedded into the Marine Expeditionary Unit onboard ships where it provides support directly to deployed forces.

Air Forces Cyber or the 24th Air Force is self-described as an "Operational war-fighting organization that executes full spectrum cyberspace operations to ensure friendly forces maintain a warfighting advantage."[60] It has several subordinate elements:

- 624th Operations Center serves as the cyber operations center for the Air Force.
- 67th Cyberspace Wing operates the Air Force Information Network, which is the Air Force section of DODIN.
- 688th Cyberspace Wing delivers proven information operations engineering and infrastructure capabilities.
- 5th Combat Communications Group delivers expeditionary communications, information systems, engineering and installation, air traffic control, and weather services to the President, Secretary of Defense, and combatant commanders.[61]

Conclusion

The United States both benefits from and is challenged by a wide variety of Federal Government actors in the cyber realm. The benefit comes from pursuing multiple responses simultaneously, leading to agility and greater defense in-depth. However, this same approach is far more expensive and may lead to confusion with private-sector stakeholders and an increased level of competition for limited skilled resources. The abundance of Federal Government actors was not a planned response. Many of these organizations were created as the result of bottom-up initiatives from within the various departments seeking to respond to an emerging, ill-defined threat area. Executive branch decision memoranda, policy statements, and strategies are beginning to bring some organization to the interdepartmental effort; however, a statutory blueprint (with corresponding budgetary guidance) has yet to be approved by Congress. Whether it is wise to prune the Federal Government's response to the cyber threat is a policy decision yet to be made, but the current state of affairs clearly requires a map to understand its full scale and scope. This article has looked at the structure that exists in 2015. No doubt the structure, roles, and missions will continue to change as the cyber realm itself matures. **JFQ**

Notes

[1] Interview with Brigadier General Greg Touhill, USAF (Ret.), Deputy Assistant Secretary of Homeland Security, Cyber Security Operations Program, March 27, 2015.

[2] *National Security Strategy* (Washington, DC: The White House, February 2015), 12–13, available at <www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>.

[3] "Cybersecurity," The White House, March 18, 2015, available at <www.whitehouse.gov/issues/foreign-policy/cybersecurity>.

[4] Testimony of Steven R. Chabinsky before the U.S. Senate Committee on Homeland Security and Governmental Affairs, "Strengthening Public-Private Partnerships to Reduce Cyber Risks to our Nation's Critical Infrastructure," Washington, DC, March 26, 2014.

[5] The authors would like to thank Thomas Wingfield, Esq., for providing his thoughts on cyber legislation.

[6] "S.2519—National Cybersecurity Protection Act of 2014," U.S. Congress, December, 18, 2014, available at <www.congress.gov/113/bills/s2519/BILLS-113s2519enr.pdf>.

[7] "S.2521—Federal Information Security Modernization Act of 2014," U.S. Congress, December 18, 2014, available at <www.congress.gov/113/bills/s2521/BILLS-

113s2521enr.pdf>.

[8] "S.2354—DHS Cybersecurity Workforce and Recruitment and Retention Act of 2014," U.S. Congress, July 14, 2014, available at <www.congress.gov/113/bills/s2354/BILLS-113s2354rs.pdf>.

[9] "Our Mission," Department of Homeland Security (DHS), available at <www.dhs.gov/our-mission>.

[10] "The 2014 Quadrennial Homeland Security Review," DHS, June 18, 2014, 78, available at <www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>.

[11] Touhill interview.

[12] Touhill interview; and "NPPD at a Glance," DHS, available at <www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-071614.pdf>.

[13] Touhill interview; and "Office of Cybersecurity and Communications," DHS, available at <www.dhs.gov/office-cybersecurity-and-communications>.

[14] "Stakeholder Engagement and Cyber Infrastructure Resilience," DHS, available at <www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience>.

[15] "The 2014 Quadrennial Homeland Security Review."

[16] "Cybersecurity: DHS's Role, Federal Efforts, and National Policy," U.S. Government Printing Office (GPO), June 16, 2010, 12, available at <www.gpo.gov/fdsys/pkg/CHRG-111hhrg64697/pdf/CHRG-111hhrg64697.pdf>.

[17] "National Cybersecurity Communications Integration Center," DHS, available at <www.dhs.gov/about-national-cybersecurity-communications-integration-center>.

[18] Touhill interview.

[19] "About Us," U.S. Computer Emergency Response Team, available at <www.us-cert.gov/about-us>.

[20] "Cybersecurity: DHS's Role, Federal Efforts, and National Policy," GPO, June 16, 2010, 15, available at <www.gpo.gov/fdsys/pkg/CHRG-111hhrg64697/pdf/CHRG-111hhrg64697.pdf>.

[21] "About the Industrial Control Systems Cyber Emergency Response Team," Industrial Control Systems Cyber Emergency Response Team, available at <https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team>.

[22] "National Coordinating Center for Communications," DHS, available at <www.dhs.gov/national-coordinating-center-communications#>.

[23] "Office of Infrastructure Protection Strategic Plan: 2012–2016," DHS, available at <www.dhs.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf>.

[24] "Office of Cyber and Infrastructure Analysis," DHS, available at <www.dhs.gov/office-cyber-infrastructure-analysis>.

[25] "Cyber Crimes Center," U.S. Immigration and Customs Enforcement, available at <www.ice.gov/cyber-crimes>.

[26] Ibid.

[27] "About," National Computer Forensics Institute, available at <www.ncfi.usss.gov/ncfi/pages/about.jsf>.

[28] "Strategic Plan Fiscal Years 2014–2018," U.S. Department of Justice (DOJ), available at <www.justice.gov/about/strategic-plan-fiscal-years-2014-2018>.

[29] Ibid., 10.

[30] Ibid., 19.

[31] "Cyber Crime," Federal Bureau of Investigation (FBI), available at <www.fbi.gov/about-us/investigate/cyber>.

[32] "Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity," FBI, available at <www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1>.

[33] "The NCFTA: Combating Force to Fight Cyber Crime," FBI, September 16, 2011, available at <www.fbi.gov/news/stories/2011/september/cyber_091611>.

[34] "Cyber Solidarity: Five Nations, One Mission," FBI, March 18, 2008, available at <www.fbi.gov/news/stories/2008/march/cybergroup_031708>.

[35] "Combatting National Security Cyber Threats," DOJ, available at <www.justice.gov/nsd/about-division-0>.

[36] "New Network Takes Aim at Cyber Threats to National Security," DOJ, November 14, 2012, available at <www.justice.gov/opa/blog/new-network-takes-aim-cyber-threats-national-security>.

[37] "Computer Crime and Intellectual Property Section," DOJ, available at <www.justice.gov/criminal/cybercrime/>.

[38] "Cyber Crime," Offices of the U.S. Attorneys, available at <www.justice.gov/usao/priority-areas/cyber-crime>.

[39] Vice Admiral Michael S. Rogers, USN, Nominee for Commander, U.S. Cyber Command, Congressional Testimony, March 11, 2014.

[40] Joint Publication (JP) 3-12(R), *Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, February 5, 2013), GL-4, available at <www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf>.

[41] Rogers Congressional Testimony, March 11, 2014.

[42] Andrew Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," R42077 (Washington, DC: Congressional Research Service, January 3, 2013), available at <http://fas.org/sgp/crs/natsec/R42077.pdf>.

[43] Rita Boland, "Command's Cybersecurity Crosses Domains, Directorates," *Signal*, June 1, 2013, available at <www.afcea.org/content/?q=command%E2%80%99s-cybersecurity%E2%80%A8-crosses-domains-directorates>.

[44] Rogers Congressional Testimony, March 11, 2014.

[45] "Mission," Defense Cyber Crime Center, available at <www.dc3.mil/index/mission>.

[46] U.S. Cyber Command's Web site is available at <www.jtfgno.mil>.

[47] "Mission Statement," U.S. Cyber Command, available at <www.jtfgno.mil/default.aspx>.

[48] "Advance Questions for Vice Admiral Michael S. Rogers," Senate Armed Services Committee, March 11, 2014, available at <http://fas.org:8080/irp/congress/2014_hr/031114rogers-q.pdf>.

[49] "Statement of Admiral Michael S. Rogers," Senate Armed Services Committee, March 19, 2015, available at <http://fas.org:8080/irp/congress/2015_hr/031915rogers.pdf>.

[50] JP 3-12(R), ix.

[51] "Navy Information Dominance Corps Human Capital Strategy 2012–2017," U.S. Navy, iv, available at <www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf>.

[52] Air Force Doctrine Document 3-12, *Cyberspace Operations*, U.S. Air Force, July 15, 2010 (updated November 30, 2011).

[53] "DOD Strategy for Operating in Cyberspace," DOD, July 2011, available at <www.defense.gov/news/d20110714cyber.pdf>.

[54] "NETCOM," U.S. Army Cyber Command, available at <www.arcyber.army.mil/org-netcom.html>; and <www.army.mil/info/organization/unitsandcommands/commandstructure/netcom/>.

[55] "INSCOM," U.S. Army Cyber Command, available at <www.arcyber.army.mil/org-inscom.html>; and <www.inscom.army.mil/>.

[56] Email from CAPT Stephanie Keck, Division Director, Information Dominance Corps and Foreign Area Officer Assignments, Navy Personnel Command.

[57] "U.S. Fleet Cyber Command Mission and Vision," U.S. Fleet Cyber Command, available at <www.fcc.navy.mil/>.

[58] "U.S. Tenth Fleet Mission," U.S. Fleet Cyber Command, available at <www.fcc.navy.mil/>.

[59] Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations* (Washington, DC: Department of the Navy, Headquarters U.S. Marine Corps, August 9, 2011), 2-17 and 2-18.

[60] "24th Air Force Fact Sheet," *24th Air Force*, available at <http://newpreview.afnews.af.mil/24af/library/factsheets/factsheet.asp?id=15663>.

[61] "24th Air Force Units," *24th Air Force*, available at <www.24af.af.mil/units/index.asp>.