CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Piret Pernik, Jesse Wojtkowiak, Alexander Verschoor-Kirss

National Cyber Security Organisation: UNITED STATES

Tallinn 2016

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre, NATO, any agency or any government. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

www.ccdcoe.org
publications@ccdcoe.org

Other reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in the United Kingdom

Upcoming in 2016

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Special thanks to Eve Hunter for her contribution to the substance of this report and for editorial support.

Information in this study was checked for accuracy as of December 2015.

About this study

This report is a part of a NATO CCD COE project that assembles a comprehensive overview of existing national organisational models for ensuring cyber security in NATO Nations that are Sponsoring Nations to the NATO CCD COE.

The study outlines the division of cyber security tasks and responsibilities between different agencies and describes their mandate, tasks and competences, and the coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

The result is a series of country chapters, outlining national cyber security management structures by nation.

The project contributes to awareness among NATO Allies about cyber security management in the varied national settings, thus supporting nations enhancing their own organisational structure, encouraging the spread of best practices, and contributing to the development of cooperation between different national institutions in NATO nations.

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the USA as Sponsoring Nations, and Austria and Finland as Contributing Participants. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

UNITED STATES

By Piret Pernik
Research Fellow, International Centre for Defence and Security

Jesse Wojtkowiak
Visiting Research Fellow, International Centre for Defence and Security

Alexander Verschoor-Kirss
Visiting Research Fellow, International Centre for Defence and Security

Table of Contents

1. Introduction: information society in the United States

1.1. Infrastructure availability and take-up

Despite the perception of the United States (US) as a technological and innovation powerhouse, it lags behind many other modern industrialised nations in terms of internet access and connectivity. The International Telecommunication Union ranked the US 28th in terms of the percentage of individuals using the internet in 2013, with 84% connected;[1] US polling organisations yield similar values.[2] While the vast majority of Americans have access to the internet, such connections are not necessarily of high quality: just under 20 fixed broadband subscriptions per 100 had speeds equal to or greater than 10 megabits per second in early 2014, lagging far behind countries such as South Korea (global leader at 38 per 100), France (36 per 100), United Kingdom (29 per 100) and Japan (27 per 100).[3] Speeds, however, are gradually increasing. Google had installed a high-speed fibre-optic network in three cities across the US as of late 2015, with six more planned.[4]

The US has committed itself to fostering technological innovation with strategic focus on increasing internet and broadband internet access. The US Congress directed the Federal Communications Commission (FCC) to begin developing a *National Broadband Plan* (NBP) in early 2009 in order to help with this goal. The plan, unveiled in March 2010, noted the positive effect of broadband internet access, serving as 'a foundation for economic growth, job creation, global competitiveness and a better way of life,' while acknowledging that the government could play a crucial role in accelerating the process of growing the country's telecommunications infrastructure. Among some of the goals enumerated in the NBP were that 'every American should have affordable access to robust broadband service,' and '[a]t least 100 million U.S. homes should have […] actual download speeds of at least 100 Mbps and actual upload speeds of at least 50 Mbps by 2020'.

Due to a general suspicion of federal intervention in economic enterprises in the US, the government would be limited in terms of investments and ownership of the burgeoning network. Instead, the government exerts influence over the 'broadband ecosystem' in four main ways:

> '(1) Design[ing] policies to ensure robust competition and as a result maximise consumer welfare, innovation and investment;
>
> (2) Ensur[ing] efficient allocation and management of assets [that] government controls or influences, such as spectrum, poles, and rights-of-way, to encourage network upgrades and competitive entry;
>
> (3) Reform[ing] current universal service mechanisms to support deployment of broadband and voice in high cost areas,' and;
>
> (4) Reform[ing] laws, policies and incentives to maximise the benefits of broadband in sectors [that] government influences significantly.'

[1] ITU ICT-Eye, 'United States Profile', 2013 <http://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?countryID=244>.
[2] The Pew Research Center measured 87% of adults in the US as using the internet in a January 2014 poll; the most recent measurement by the U.S. Census Bureau, undertaken in 2012, determined that 75% of individuals lived in a home with internet use, with 75% of individuals accessing the internet from some location. Susannah Fox *et al*, 'The Web at 25 in the U.S. The Overall Verdict: The internet Has Been a Plus For Society and an Especially Good Thing for Individual Users', Pew Research Center, 2014 <http://www.pewinternet.org/2014/02/25/the-web-at-25-in-the-u-s>;
U.S. Census Bureau, 'Table 4. Households with A Computer and Internet Use: 1984 to 2012', 2014 <http://www.census.gov/hhes/computer/files/2012/table4.xls>.
[3] 'The World in 2015.' International Telecommunication Union, 2015. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
[4] 'Expansion Plans.' Google Fiber. <https://fiber.google.com/newcities/>

The NBP is the main goal-setting initiative for broadband providers and its by-products include annual measurements that track the improvement of American broadband access and speeds over time.[5]

In general, internet access is viewed by American internet users as a basic commodity – almost half of Americans (46%) said that the internet would be very hard to give up.[6] Accessing internet through smartphones is becoming increasingly widespread: as of June-July 2015, more than half of adult Americans (55%) had both a mobile device (smartphone or tablet) and a traditional fixed broadband subscription, and 13% were 'smartphone-only'.[7]

A few large telecommunication companies such as Comcast, Time Warner, Verizon, and AT&T provide the majority of service and infrastructure to the American public. From February 2015, the Federal Communications Commission (FCC) had more authority to regulate these providers to ensure just treatment of customers and prevent paid prioritisation that would jeopardise net neutrality.[8]

1.2. E-government and private sector e-services

1.2.1. E-government

The issues stalling comprehensive improvements in the coverage of high-speed, low-cost broadband internet access are mirrored in the US's efforts to expand the array of government services offered electronically. In recent years, the US has been plagued by many high profile debacles regarding e-government, including the infamous technical problems and cost-over runs associated with the roll-out of 'healthcare.gov', the internet portal where consumers could register for and select healthcare plans, as well as the difficulty associated with digitising the paper records of the Department of Veterans' Affairs. Nevertheless, the US ranks 7th among the worldwide top 10 e-government leaders (after South-Korea, Australia, Singapore, France, Netherlands and Japan) and 9th among worldwide top 10 e-participation countries.[9] In a 2013 poll, 34% of US adults recently contacted a government official or spoke out in a public forum via online methods (nearly 40% did so via offline methods) and nearly 40% participated in political or civic activities over social networking sites.[10] Nevertheless, online communication with the government is often impeded by the frequent requirement that people must turn documents in physically.

Still, the US has sought to make gains in the field of e-government. The *E-Governance Act* of 2002 was enacted to enhance the management and promotion of e-government services and processes. The Act serves as the primary legislative vehicle to guide federal IT management and initiatives to make information and services available online (it also includes various cyber security requirements – see section 2.1).[11]

A decade later in 2012, the *Digital Government* Strategy renewed the vision for US e-government and set out three major goals: enabling better mobile access to government information and services; focusing government purchasing on the most advanced and secure technologies; and spurring innovation in the private

[5] To date there have been no comprehensive surveys of the programme's effectiveness. It ultimately may become difficult to untangle historically which activities in terms of broadband access were directly influenced by government action as part of the NBP – the question primarily is to what degree the NBP accelerated this process beyond what private enterprise and consumer demand might have caused on their own.
[6] 'The Web at 25 in the U.S.' (n 2).
[7] Pew Research Center, 'Home Broadband 2015', 2015 < http://www.pewinternet.org/files/2015/12/Broadband-adoption-full.pdf>.
[8] Alina Selyukh, 'U.S. Internet Providers Hit with Tougher Rules, Plan Challenges.' Reuters, 26 February 2015. <http://www.reuters.com/article/2015/02/26/us-usa-internet-neutrality-idUSKBN0LU0CA20150226>.
[9] United Nations, 'United Nations E-Government Survey 2014. E-Government for the Future We Want', New York, 2014 <http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf>.
[10] Aaron Smith, 'Civic Engagement in the Digital Age. Online And Offline Political Engagement', Pew Research Center, 2013 <http://www.pewinternet.org/2013/04/25/civic-engagement-in-the-digital-age/>.
[11] Eric A. Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions', Congressional Research Service, 2013 <https://fas.org/sgp/crs/natsec/R42114.pdf>.

sector regarding technological advancement. This strategy works to complement a number of executive orders from President Obama regarding government transparency and IT reform of federal systems.[12]

1.2.2. E-commerce and technology in the private sector

Where the US clearly leads among its peers is in the realm of e-commerce in the private sector. The rise of e-commerce in the US as a substitute for physical economic activity is remarkable; in the most recent comprehensive statistics released by the US Census Bureau for the year 2013, e-commerce manufacturing totalled $3.3 trillion, an 11.1% increase from 2012, and e-commerce formed a majority of all manufacturing shipments by 57.1 percent.[13] Revised estimates for the quarterly measures of retail e-commerce show steady increases in the range of 3-5% over the previous quarter from 2009-2014. The relative strength of US e-commerce is a potential asset for the US's e-governance ambitions: the public sector can leverage the success of technological innovators in the private sector toward further developing their own capabilities.[14]

2. Strategic national cyber security objectives

Worldwide, the US has been in the vanguard of developing cyber security policy and strategy. As early as 2003 its government issued the first national cyber security strategy;[15] the first EU countries to publish similar documents that addressed aspects of cyber security were Germany in 2005 and Sweden in 2006. The *National Strategy to Secure Cyberspace* of 2003 established three strategic objectives for national cyberspace security: preventing cyber attacks against national critical infrastructures; reducing national vulnerability to cyber attacks; and minimising damage and recovery time from cyber attacks that do occur. Five national priorities were identified for attaining these goals: securing federal computer systems and networks; developing a response system; establishing a threat and vulnerability reduction programme; initiating an awareness and training programme for cyber security; and developing a system of international cooperation.[16]

Cyber security policy in the US to date has consisted of piecemeal measures; likewise, legislation is less comprehensive and more topically-focused.[17] Over 50 statutes address various aspects of cyber security. Since no overarching framework legislation or national cyber security strategy is in place that synthesises these documents or comprehensively describes the current strategy,[18] forming a clear understanding of overall strategic objectives and priorities for enhancing cyber security is a complicated task. Most of the existing documents address national priorities from narrower cyber security areas,[19] which furthermore leads to variance in terms of priorities and structure, and also fails to specify how they link to or supersede other policy

[12] 'Digital Government. Building a 21st Century Platform to Better Serve the American People' (n **Error! Bookmark not efined.**)
[13] U.S. Census Bureau, 'E-Stats 2013: Measuring the Electronic Economy', 2015. <http://www.census.gov/econ/estats/e13-estats.pdf>.
[14] Karen Layne and Jungwoo Lee. 'Developing fully functional E-government: A four stage model.' *Government Information Quarterly* 18, 2 (2001): 122-136.
[15] The White House, 'The National Strategy to Secure Cyberspace', 2003 <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>.
[16] Ibid.
[17] Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions' (n 11). The Cyber Security Act of 2012 would have been the first real piece of legislation but was not ratified by the Senate; Andrew Couts, 'Senate Kills Cybersecurity Act of 2012', Digital Trends, 2012. <http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/>. Concern over privacy and abuses of power by U.S. government agencies heavily contributed to the bill's defeat.
[18] United States Government Accountability Office (U.S.GAO), 'High-Risk Series. An Update', 2013 <http://www.gao.gov/products/GAO-13-283>.
[19] Ibid.

documents. For the most part, these documents do not describe how they fit into the overall national cyber security strategy.[20]

Broader national security and defence strategies also outline cyber security objectives. The 2010 *National Security Strategy* was the first US national security strategy[21] to devote substantial attention to cyber threats;[22] it also represented a change in the characterisation of cyber threats by the federal government, with emphasis shifting from non-state terrorism to state-sponsored activities and from a predominantly political to an economic concern.[23] The *Quadrennial Homeland Security Review* of 2010 identified 'safeguarding and securing cyberspace' as one of the five priority homeland security missions. In order to implement the National Security Strategy and achieve the goals set out in the Quadrennial Homeland Security Review, the Department of Homeland Security's (DHS) *Blueprint for a Secure Cyber Future* of 2011 provided a plan of action which absorbed and delineated two areas: protecting critical information infrastructure, and strengthening the cyber ecosystem.[24] The subsequent *Quadrennial Homeland Security Review* of 2014 prioritised investments that support national interest and missions, including cyber, and described those cyber threats that pose a risk to national interests.[25] It clarified the responsibility of DoD to develop new and expanded full-spectrum cyberspace capabilities for the defence of homeland and for the support of military missions worldwide. DoD's Quadrennial Defence Review of 2014 listed the major roles of DoD in cyber: 'to defend the integrity of [DoD] networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyberattack on vital U.S. interests'.[26]

The current *National Security Strategy*, adopted in early 2015, acknowledges the growing danger of disruptive and even destructive cyber attacks, and communicates the US's intent to fortify the cyber security of critical infrastructure, increase investment in cyber capabilities, and 'impose costs' on malicious cyber actors. The document focuses particularly on the US's goal to promote international norms in cyberspace.[27] The priorities set out by the National Security Strategy are supported in the *National Intelligence Strategy of the United States of America* (2014), which lists as one of the four mission objectives for the intelligence community the detection and understanding cyber threats to inform and enable national security decision making, cybersecurity, and cyber effects operations. The strategy reaffirms goals such as increasing partnerships and information-sharing, as well as advancing technological capabilities.[28]

In 2011, the White House released the *International Strategy for Cyberspace*, which reflects the US's approach to engaging with international partners and communicating national priorities. The overall objective as articulated by the strategy is as follows:

> *The United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we*

[20] Ibid.
[21] The 2008 *National Defence Strategy* acknowledged the susceptibility of cyberspace to malicious operations as a strategic vulnerability, stating that 'The US […] face[s] a spectrum of challenges, including […] emerging space and cyber threats'. U.S. Department of Defense, 'National Defense Strategy', 2008. <http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf>.
[22] The White House, 'National Security Strategy', 2010 <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>.
[23] Robinson, Neil et al, 'Cyber-Security Threat Characterization: A Rapid Comparative Analysis', RAND Corporation, 2013.
[24] U.S. Department of Homeland Security, 'Blueprint for a Secure Cyber Future. The Cybersecurity Strategy for the Homeland Security Enterprise', 2011 <http://www.dhs.gov/blueprint-secure-cyber-future>.
[25] U.S. Department of Homeland Security, '2014 Quadrennial Homeland Security Review', 2014 <http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf>.
[26] U.S. Department of Defense, 'Quadrennial Defense Review 2014', 2014 <http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf>.
[27] White House, 'National Security Strategy', 2015. <https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>.
[28] Office of the Director of National Intelligence, 'The National Intelligence Strategy of the United States of America', 2014. <http://www.dni.gov/files/documents/2014_NIS_Publication.pdf>.

will build and sustain an environment in which norms of responsible behaviour guide states' actions, sustain partnerships, and support the rule of law in cyberspace.

The strategy goes on to divide this goal into diplomatic, defence, and development goals, pointing out policy priorities for the entire federal government under seven interdependent areas of activity (economy, protection of national networks, law enforcement, military, internet governance, international development, and internet freedom).[29]

The remaining part of this section will chronologically review the most relevant strategy documents and federal legislation, including legal acts issued by the Congress and executive orders by the Presidents of the US) pertaining to the 'whole-of-government' approach to ensuring cyber security. These documents address a wide range of activities: the protection of national critical infrastructure and the security of federal computer systems and networks; the designation of roles and responsibilities for federal, state, local, tribal, territorial and private sector partners; the enhancement of public-private sector partnerships; as well as cyber security aspects of international and national security, defence and counter-intelligence. For greater clarity, the overview of the evolution of these documents is divided into three sub-sections:

(1) Documents that regulate cyber security aspects of federal networks;

(2) Documents regarding critical infrastructure protection (CIP); and

(3) Military documents pertaining to cyber security aspects of national security and defence.

2.1. Cyber security of federal networks

The *Federal Information Security Management Act* (FISMA) – as part of the *E-Governance Act* of 2002 – instituted a risk management framework developed by the National Institute of Standards and Technology (NIST) to standardise cyber security processes throughout US government agencies.[30] The act established a Federal Chief Information Officer within the Office of Management and Budget (OMB), responsible for overseeing the government's use of technology both in terms of spending and strategy.[31] It clarified and strengthened NIST's responsibilities for developing security standards for federal computer systems (except for defence and intelligence systems), established a central federal incident centre, and made OMB responsible for promulgating federal cyber security standards.[32] FISMA was criticised for being inefficient in providing adequate cyber security to government IT systems;[33] many legislative proposals unsuccessfully sought reform before an amendment to FISMA was finally enacted in December 2014.[34]

[29] The White House, 'International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World', 2011. <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.
[30] The United States Congress, 'H.R.2458 – E-Government Act of 2002. 107th Congress (2001-2002)', 2002 <https://www.congress.gov/bill/107th-congress/house-bill/2458>.
[31] The statute includes within it the Federal Information Security Management Act (FISMA) and the Confidential Information Protection and Statistical Efficiency Act. Ibid.
[32] Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions' (n 11)
[33] The criticism concerns inadequate resources, a focus on procedure and reporting rather than operational security, a lack of widely accepted cyber security metrics, variations in agency interpretation of the mandates in the act, excessive focus on individual information systems as opposed to the agency's overall information architecture, and insufficient means to enforce compliance both within and across agencies. Ibid.
[34] For example, Federal Information Security Amendments Act of 2012 (H.R. 1163), which addresses FISMA reform, passed the House but was not considered by the Senate. Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions' (n 11).

The 2014 update to FISMA clarifies responsibilities for CIOs, establishes clearer reporting guidelines with an emphasis on speed, and mandates OMB to clarify policy on reporting breaches involving personal identifying information.[35]

The *National Security Presidential Directive 54* and the *Homeland Security Presidential Directive 23* were issued by President George W. Bush in January 2008. The directives authorised DHS together with OMB to set minimum operational standards for federal government civilian networks.[36] Both directives underlined the whole-of-government approach to ensuring cyber security, which was subsequently embodied in the *Comprehensive National Cybersecurity Initiative* (CNCI) set up pursuant to the directives. The CNCI's stated purpose is defending against the most immediate and the full spectrum of threats and strengthening the future cyber security environment by initiating a comprehensive approach that encompasses law enforcement, intelligence, counterintelligence, and military capabilities.[37] It has become the key element of President Barack Obama's approach to a US cyber security strategy.

The main actions of the CNCI are:[38]

- creating or enhancing shared situational awareness within federal government, and with other government agencies and the private sector;
- creating or enhancing the ability to respond quickly to prevent intrusions;
- enhancing counterintelligence capabilities;
- increasing the security of the supply chain for key information technologies;
- expanding cyber education;
- coordinating and redirecting research and development efforts; and
- developing deterrence strategies.

The CNCI has 12 sub-initiatives, among the most noteworthy are improving defence of federal systems and increasing security of classified networks; clarifying the federal role in protecting critical infrastructure; improving research coordination; and prioritising information sharing and cyber security education and awareness.[39]

In order to develop a strategic framework to ensure the CNCI is being appropriately integrated, resourced, and coordinated with Congress and the private sector, President Obama initiated the *Cyberspace Policy Review* in 2009. The review was critical of the progress of the US government as a whole,[40] identifying key shortcomings in policy, legal structures, management, coordination, and research that were listed as the greatest vulnerabilities to US comprehensive cyber security.[41] Among other things, the review suggested a stronger leadership role for the White House, as well as strengthening federal leadership and accountability for cyber security. Additionally, it laid out 10 near-term actions and 14 mid-term actions to support the overall goals of the CNCI.[42]

---

[35] Aaron Boyd, '2014 FISMA reduces paperwork, codifies management structure', Federal Times, 2014 <http://www.federaltimes.com/story/government/it/management/2014/12/16/2014-fisma-reduces-paperwork-codifies-management-structure/20482819/>.

[36] Again, they empower DHS to lead and coordinate the national cybersecurity effort to protect cyberspace and the computers connected to it.

[37] The White House, 'The Comprehensive National Cybersecurity Initiative (CNCI)' <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>.

[38] Ibid.

[39] Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions' (n 11).

[40] John Rollins *et al*, 'Congressional Research Service Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations', Congressional Research Service, 2009 <http://fas.org/sgp/crs/natsec/R40427.pdf>.

[41] 'The Comprehensive National Cybersecurity Initiative (CNCI)' (n 37).

[42] The White House, 'Cybersecurity' <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity>. The progress report of the action items is available at: The White House, National Security Council, 'Cybersecurity Progress after

Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program (2011) outlines strategic directions for DHS, the National Science Foundation, and the National Institute of Standards and Technology (NIST) with regard to research priorities to ensure reliable communications infrastructure.[43]

2.2. Protecting critical infrastructure

The US's strategic approach regarding critical infrastructure protection (CIP) focuses on public-private partnerships, while government authorities hold coordinating and prioritising responsibilities. The *Presidential Decision Directive 63 of 1998* established a structure under White House leadership to coordinate the activities of the federal government to protect critical infrastructure from cyber attack.[44] The *Homeland Security Act* of 2002 created the Department of Homeland Security (DHS) and placed it in charge of, inter alia, coordinating national efforts concerning the protection of critical infrastructure across the IT and communications sectors.[45] The majority of the responsibilities laid out in the National Strategy to Secure Cyberspace of 2003 were also added to the DHS remit.[46]

A national policy was established within *Homeland Security Presidential Directive 7* of 2003 for identifying and prioritising critical infrastructure in the physical realm and cyberspace and for protecting it from terrorist attacks.[47] The directive updated the roles and responsibilities of various agencies that were outlined in the Homeland Security Act of 2002 and other documents.[48] It also confirmed DHS's responsibility for coordinating overall critical infrastructure protection efforts and designated the department as the lead agency for IT and communications sectors to share threat information, vulnerability assessments, and development of appropriate protective action and contingency plans.[49] It further directed DHS to produce a *National Infrastructure Protection Plan* (NIPP) that outlines partnership criteria between the federal government and critical infrastructure owners and operators. The plan was adopted in 2006 and updated in 2009.[50]

Along with the National Strategy to Secure Cyberspace, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* was published in 2003. The document identifies the nation's critical infrastructure[51] and the threats that are posed to it.[52] As with the 2003 *National Strategy to Secure Cyberspace*,

---

President Obama's Address', 2010 <http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010>.

[43] Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions' (n 11).

[44] The White House, 'Presidential Decision Directive/NSC-63. Critical Infrastructure Protection', Washington, 1998, Section II <http://fas.org/irp/offdocs/pdd/pdd-63.htm>. Cited in: The White House, 'Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure', 2009 <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. The directive was later updated by the *National Strategy to Secure Cyberspace* of 2003.

[45] 'Cyberspace Policy Review' (n 44) appendix C.

[46] Ibid.

[47] U.S. Department of Homeland Security, 'Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection', 2003 <http://www.dhs.gov/homeland-security-presidential-directive-7>. The directive did not encompass the protection of federal government information systems. 'Cyberspace Policy Review' (n 44).

[48] John D. Moteff, 'Critical Infrastructures: Background, Policy, and Implementation', Congressional Research Service, 2014 <http://fas.org/sgp/crs/homesec/RL30153.pdf>.

[49] Ibid.

[50] U.S. Department of Homeland Security, 'National Infrastructure Protection Plan 2006', 2006 <https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf>. U.S. Department of Homeland Security, 'National Infrastructure Protection Plan 2009', 2009 <https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>. U.S. Government Accountability Office, 'Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience', GAO-10-296, 2010.

[51] In the US, critical infrastructure comprises of 16 sectors: chemical facilities; commercial facilities; communications; critical manufacturing; dams; Defence Industrial Base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; water and wastewater systems. The White House, Office of the Press Secretary, 'Presidential Policy Directive - Critical Infrastructure Security and Resilience/PPD-21', 2013 <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

the majority of the responsibilities in this document fall upon DHS. In 2012, the Obama administration backed legislation that would have given DHS the authority to secure critical infrastructure networks; however, the draft legislation twice failed to pass Congress.[53] As a response, Obama issued *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity* (EO 13636). This landmark document, binding for the President's term of office, complements all previous documents and orders improved information sharing between the federal government and private sector. It also establishes minimum requirements for improving security at critical infrastructures.[54]

The *Presidential Policy Directive Critical Infrastructure Security and Resilience*[55] (PPD-21), issued alongside EO 13636, made no major changes in policy, roles and responsibilities, or programmes; however, it demanded an evaluation of the existing public-private partnership model, the identification of baseline data and system requirements for efficient information exchange, and the development of a situational awareness capability.[56] It also called for an update to the *National Infrastructure Protection Plan* of 2009 (NIPP), itself a revision of the 2006 plan, culminating in the plan's third revision which was issued in 2013.[57]

In order to address the shortcomings of FISMA, EO 13636 directed the federal government to develop a voluntary cyber security framework, creating the *Framework for Improving Critical Infrastructure Cybersecurity* of 2014, which consists of guidelines, practices, and voluntary standards for the private sector to promote the protection of critical infrastructure.[58] It is designed to help organisations start a cyber security programme or improve on existing ones,[59] and provides an industry-driven risk management approach to strengthen cyber security across all critical infrastructure sectors.[60]

In addition to the listed documents, four bills pertaining to the protection of critical infrastructure were enacted in 2014:

- *Federal Information Security Modernization Act of 2014*, amending the 2002 FISMA, clarifies the role of DHS in securing federal agencies' digital information, defines that OMB is responsible for federal implementation of FISMA requirements, and puts in place reporting requirements for cyber incidents.[61]

---

[52] The White House, 'The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets', Washington, 2003 <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[53] Mark Clayton, 'Senate Cybersecurity Bill Fails, So Obama Could Take Charge', The Christian Science Monitor, 2012 <http://www.csmonitor.com/USA/Politics/2012/1116/Senate-cybersecurity-bill-fails-so-Obama-could-take-charge>.
[54] U.S. Department of Homeland Security, Office of Inspector General, 'Implementation Status of the Enhanced Cybersecurity Services Program', Washington, 2014 <http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf>.
[55] This directive replaced the Homeland Security Presidential Directive 23 signed by the president George W. Bush in January 2008. 'Presidential Policy Directive - Critical Infrastructure Security and Resilience/PPD-21' (n 51).
[56] 'Critical Infrastructures*:* Background*,* Policy, and Implementation' (n 48).
[57] U.S. Department of Homeland Security, 'National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience', 2013 <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.
[58] The framework was developed by the National Institute for Science and Technology. U.S. Department of Commerce, The National Institute of Standards and Technology (NIST), 'Framework for Improving Critical Infrastructure Cybersecurity', 2013 <http://www.nist.gov/cyberframework/index.cfm>.
[59] U.S. Chamber of Commerce, '2014 Cybersecurity Education & Framework Awareness Campaign. Improving Today. Protecting Tomorrow™', Austin, Texas, 2014 <https://www.uschamber.com/programs/national-security-emergency-preparedness/2015-cybersecurity-campaign/education-awareness >.
[60] '2014 Quadrennial Homeland Security Review', 2014 (n 25).
[61] Passed by the Senate Homeland Security and Government Affairs Committee on June 25, 2014. The United States Congress, 'Federal Information Security Modernization Act of 2014. 113th Congress (2013-2015)', 2D Session, 2014 <https://www.govtrack.us/congress/bills/113/s2521/text>.

- *The National Cybersecurity Protection Act of 2014* was signed by President Obama in December 2014. This act allows DHS to share information with the private sector, respond to cyber incidents, assist private companies and federal agencies alike, and recommend cyber security measures.[62]
- *National Cybersecurity and Critical Infrastructure Protection (NCCIP) Act of 2013* codifies the role of DHS in preventing and responding to cyber security incidents, and establishes an information sharing partnership between DHS and the owners and operators of the critical infrastructure.[63]
- *Cybersecurity Enhancement Act of 2014* gives the National Institute of Standards and Technology the authorisation and support to develop voluntary standards to reduce the risk of cyber attacks to critical infrastructure.[64]

The federal agencies have also been tasked with an evaluation of existing cyber regulations for the industries under their purview with the possibility of creating regulatory standards.[65] DHS, the Department of Commerce, and the Department of the Treasury are also reviewing incentives packages to induce private sector compliance with the *Framework for Improving Critical Infrastructure Cybersecurity*.[66]

The 'congressional watchdog', the US Government Accountability Office (GAO), has called attention to a lack of cyber security guidance by the federal government's departments and agencies for the specific critical infrastructure sectors they are responsible for. The level to which various critical infrastructure sectors are required by law or regulation to comply with specific cyber security requirements is extremely varied. Despite the blatant separation between the public and private entities and federal and state entities, the GAO observed a lack of clarity on where responsibility lies amongst these parties.[67]

The *National Response Framework* presents the guiding principles that enable a unified national response to disasters and emergencies, including cyber security incidents. It has a broad target audience including the private sector, NGOs and even individuals, although compliance is voluntary for non-governmental bodies. The document designates the roles of various organisations in crisis response and delegates smaller tasks to the heads of each department. Whereas other documents go into specifics on managing each crisis, the Framework focuses on the details of collaboration. An appendix to the Framework, the Cyber Incident Annex, clarifies the interconnectedness of the gamut of cyber-related legislation and response teams. For example, the *National Cyber Incident Response Plan* for the operational coordination and execution of the cyber security incident response capability is under the leadership of the National Cybersecurity and Communications Integration Center (NCCIC) and its subsidiary, the US-CERT.[68]

---

[62] The Senate Homeland Security and Governmental Affairs Committee passed this bill on June 25, 2014. The United States Congress, 'S. 2519 – National Cybersecurity and Communications Integration Centre Act of 2014', 2014 <https://www.cbo.gov/publication/45594>.

[63] Passed the House on 28 June 2014. The U.S. House Committee on Homeland Security, 'National Cybersecurity and Critical Infrastructure Protection Act of 2013 (NCCIP Act)', H.R. 3696, 2013 <http://homeland.house.gov/sites/homeland.house.gov/files/documents/12113_NCCIP_summary.pdf>.

[64] 'High-Risk Series. An Update' (n 18).

[65] Tony Romm, 'Cybersecurity in Slow Lane One Year after Obama Order, ' *Politico*, 2014 <http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html>.

[66] Alina Selyukh, 'U.S. to Offer Companies Broad Standards to Improve Cybersecurity,' Reuters, 2014, <http://www.reuters.com/article/2014/02/12/us-usa-cybersecurity-standards-idUSBREA1B0AL20140212>. The framework was published by the National Institute of Standards and Technology in February 2012. U.S. Department of Commerce, The National Institute of Standards and Technology (NIST), 'Framework For Improving Critical Infrastructure Cybersecurity', Version 1.0, 2014 <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

[67] 'High-Risk Series. An Update' (n 18).

[68] In 2010 DHS issued a draft plan. It describes roles, responsibilities, and actions to prepare, respond, and recover from cyber incidents. U.S. Department of Homeland Security, 'National Cyber Incident Response Plan (NCIRP)', Interim Version, 2010 <http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf>; Federal Emergency Management Agency, 'National Response Plan: Cyber Incident Annex', 2004 <http://www.fema.gov/media-library-data/20130726-1825-25045-8307/cyber_incident_annex_2004.pdf>.

2.3. Military and defence cyber strategies

The *National Military Strategy for Cyberspace Operations*, released by the Joint Chiefs of Staff in 2006, was the first overarching document describing the US military's approach to cyberspace operations. The document identified the role of the US armed forces as to secure US interests by conducting military operations in cyberspace. According to the strategy, DoD 'relies on cyberspace to achieve national military objectives in the areas of military, intelligence, and business operations.' [69]

The *National Military Strategy of the United States of America* (2011) recognised that cyberspace has emerged as a war-fighting domain in its own right and that the US 'will enhance deterrence in air, space, and cyberspace by possessing the capability to fight through a degraded environment and improving the US's ability to attribute and defeat attacks on systems or supporting infrastructure.'[70] Cyberspace also is a major presence in DoD's *Sustaining U.S. Global Leadership: Priorities for 21st Century Defence.* This document focuses primarily on abstract goals for the military such as defending networks and enhancing resiliency.[71]

The *Information Operations* (JP 3-13) of 2012 provides joint doctrine for the planning, preparation, execution, and assessment of information operations across the range of military operations.[72] From a legal perspective, the Pentagon has provided the *Department of Defence Law of War Manual* (June 2015) which includes a chapter which clarifies DoD's interpretation of applicable law including interpretations of *jus in bello* and *jus ad bellum* in cyberspace.[73]

The *Cyber Electromagnetic Activities* (FM 3-38) of the US Army, published in 2014, provides doctrinal guidance and direction for conducting cyber electromagnetic activities, as well as the tactics and procedures for planning, integrating, and synchronising them.[74] The doctrine blends Army operations in cyberspace with electronic warfare and manipulating the electromagnetic spectrum.[75] In addition to this doctrine, the *Joint Cyberspace Operations* (JP 3-12) document, signed in February 2013, addresses the uniqueness of military operations in cyberspace, clarifies cyberspace operations-related command and operational interrelationships, and incorporates operational lessons learned.[76]

Plan X, a cyber warfare programme of the Defence Advanced Research Projects Agency (DARPA), develops platforms for the DoD to plan for, conduct, and assess cyber warfare in a manner similar to kinetic warfare.[77]

DoD's current approach to cyber security is explained in the *Department of Defence Cyber Strategy* of 2015, which updated the earlier *Department of Defence Strategy for Operating in Cyberspace* of 2011.[78] The new

[69] The Joint Chiefs of Staff (JCS), 'The National Military Strategy for Cyberspace Operations (U)', Washington, 2006 <http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf>.
[70] U.S. Department of Defense, 'National Military Strategy of the United States of America 2011: Redefining America's Military Leadership', Washington, 2011 <www.defense.gov/pubs/2011-National-Military-Strategy.pdf>.
[71] U.S. Department of Defense, 'Sustaining U.S. Global Leadership: Priorities for 21st Century Defense', 2012 <http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf>.
[72] The Joint Chiefs of Staff (JCS), 'Compendium of Key Joint Doctrine Publications', 2014 <http://www.dtic.mil/doctrine/new_pubs/compendium.pdf>.
[73] U.S. Department of Defense, Office of General Counsel, 'Law of War Manual', 2015 <http://www.dod.mil/dodgc/images/law_war_manual15.pdf>.
[74] U.S. Department of Army, 'Cyber Electromagnetic Activities', No. 3-38, Washington, 2014 <http://fas.org/irp/doddir/army/fm3-38.pdf>.
[75] Jared Serbu, 'On DoD: Army Charts Overlaps between Cyber, Electronic Warfare', Federal News Radio, 2014 <http://www.federalnewsradio.com/396/3682590/Army-contemplates-new-career-branch-for-cyber-personnel>.
[76] The Joint Chiefs of Staff (JCS), Joint Publication 3-12 (R) 'Cyberspace Operations', 2013 <http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf>.
[77] The Defence Advanced Research Projects Agency (DARPA), 'Plan X' <http://www.darpa.mil/program/plan-x >.
[78] U.S. Department of Defense, 'The Department of Defense Strategy for Operating in Cyberspace 2011', 2011 <http://www.defense.gov/news/d20110714cyber.pdf>.

strategy offers more transparency in terms of DoD's own offensive and operational capabilities.[79] The plan focuses on strategic goals for DoD as an entity, as opposed to how different sectors within DoD interact.

To respond to external and insider threats, supply chain vulnerabilities and threats to DoD's operational capability, the following five strategic initiatives are advocated in the 2015 strategy:[80]

(1) 'Build and maintain ready forces and capabilities to conduct cyberspace operations';

(2) 'Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions';

(3) 'Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence';

(4) 'Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages'; and

(5) 'Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.'

3. National organisational structure for cyber security and cyber defence

The US federal government's bureaucracy is vast and complicated; the exact number of agencies, offices, boards, and commissions is unknown. All federal departments and agencies are in charge of the protection of their own ICT systems, and many have sector-specific responsibilities for critical infrastructure for which they are responsible.[81] The regulatory mandate of different departments and agencies varies; most departments have a generalised responsibility to regulate in their constituency, others have existing cyber security-specific regulations, while some do not have a clear authority to regulate cyber security. In such cases, some comply with high-level requirements, while others follow voluntary guidance.[82] Moreover, in some cases, cyber security strategy documents assign high-level roles and responsibilities to federal government entities, but leave the implementation details to the agencies' discretion. As an example, criticism has been voiced that OMB and DHS roles and responsibilities for overseeing agencies' information security programmes have not been clearly or adequately defined.[83]

3.1. Political and strategic management and coordination

While responsibilities for leading cyber policy are broadly distributed, the primary policy coordinating role is taken by the National Security Council's[84] Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) in the White House. The ICI-IPC is co-chaired by the Homeland Security Council and the Cyber Security Coordinator (CSC) at the National Security Council's Cyber Security Office.[85] The CSC leads the

[79] Zheng, Denise, '2015 DOD Cyber Strategy', Center for Strategic & International Studies, 2015 <https://csis.org/publication/2015-dod-cyber-strategy>.
[80] U.S. Department of Defense, 'The Department of Defense Cyber Strategy', 2015. <http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.
[81] Roles and responsibilities of federal departments and agencies in regards with the protection of the critical infrastructures are outlined in the Presidential Policy Directive Critical Infrastructure Security and Resilience (PPD-21) (n 51).
[82] Michael Daniel, 'Assessing Cybersecurity Regulations', The White House Blog, 2014 <http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations>.
[83] 'High-Risk Series. An Update' (n 18).
[84] The National Security Council is a forum in which Cabinet members and Security Advisors meet with the president to determine U.S. national and international policy.
[85] Until the establishment of CSC in 2009 no single individual or entity had the responsibility to coordinate federal government cybersecurity-related activities. 'Cyberspace Policy Review' (n 44).

interagency development of national cyber security strategy and policy, and oversees agencies' implementation of those policies. The CSC, acting as the principal advisor to the president of the National Security Council, reports to the council, leads consultation process in the White House, and coordinates the US cyber security-related policies and activities.[86]

In addition to the roles of the White House entities, the Department of Homeland Security (DHS) is the primary institution responsible for cyber security within US borders (even though it has very limited statutory responsibility for the protection of federal information systems).[87] The priority areas for safeguarding and securing cyberspace – one of DHS's five core tasks – are the following: strengthen the security and resilience of critical infrastructure; help federal civilian agencies in regards with cyber security procurements and promote the adoption of common risk-based policies and best practice; advance law enforcement, incident response, and reporting capabilities; and ensure a healthy cyber ecosystem.[88]

Through its National Cyber Security Division, DHS provides strategic guidance and coordinates the overall federal effort to protect the critical infrastructure.[89] Of the 22 agencies in DHS, the National Protection and Programs Directorate (NPPD), which includes the National Cybersecurity & Communications Integration Centre (NCCIC; see subsection 3.2.), has a mandate directed toward cyber security. NPPD is primarily responsible for fulfilling DHS's national, non-law enforcement cyber security missions.[90]

The Department of State (DoS) is the primary agency for communicating and coordinating the President's cyber security policy internationally. DoS deals with cyber aspects of security, economic and human rights issues and with internet freedom. The Office of the Coordinator for Cyber Issues, aptly named, coordinates cyber issues within the department. The responsibilities of the office include advising the Secretary and Deputy Secretaries of State on cyber issues, and acting as liaison to the White House, other federal departments and agencies, and the private sector.[91]

3.2. Operational cyber incident management and incident management coordination

The Department of Justice (DoJ) is largely responsible for the enforcement of laws relating to cyber security. It counters the cyber threat by investigating and prosecuting intrusion cases, gathering intelligence in support of nation state attribution, and providing legal and policy support to other departments.[92] DoJ prosecutes cybercrimes; investigates, attributes, and disrupts cybercrimes under its jurisdiction; leads domestic national

[86] Neil Robinson *et al*, 'Cyber-Security Threat Characterization: A Rapid Comparative Analysis' (n 23). CSC also works closely with the Federal Chief Information Officer (FCIO) and the Federal Chief Technology Officer (FCTO) Office of Budget and Management; and the Office of Science and Technology.

[87] Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions' (n 11). The core mission of DHS is to prevent terrorism and enhance security, secure and manage the boarders, enforce and administer immigration laws, safeguard and secure cyberspace, and ensure resilience to disasters. U.S. Department of Homeland Security, 'Our Mission', 2014 <http://www.dhs.gov/our-mission>.

[88] '2014 Quadrennial Homeland Security Review' (n 25).

[89] U.S. Department of Homeland Security, 'Identifying Critical Infrastructure', 2013 <http://www.dhs.gov/topic/critical-infrastructure-security>. DHS coordinates the national protection against, mitigation of, and recovery from cyber incidents; works to prevent and protect against risks to critical infrastructure; disseminates domestic cyber threat and vulnerability analysis across critical infrastructure sectors; secures federal civilian systems by approaching federal systems and networks as an integrated whole and by researching, developing, and rapidly deploying cyber security solutions and services at the pace that cyber threats evolve; investigates, attributes, and disrupts cybercrimes under its jurisdiction; and coordinates federal government responses to significant incidents, whether cyber or physical, affecting critical infrastructure. '2014 Quadrennial Homeland Security Review' (n 25).

[90] 'Implementation Status of the Enhanced Cybersecurity Services Program' (n 54).

[91] U.S. Department of State, 'Office of The Coordinator for Cyber Issues' <http://www.state.gov/s/cyberissues/index.htm>; POLITICO, 'Cyber Is the New Black: Cyber Coordinator Painter', 2014 <http://www.politico.com/multimedia/video/2014/07/cyber-is-the-new-black-cybersecurity-coordinator-painter-interview.html>.

[92] U.S. Department of Justice, 'Cyber Security', 2014 <http://www.justice.gov/jmd/2014factsheets/cyber-security.pdf>.

security operations regarding cyber threats, including disrupting foreign intelligence, terrorist, or other national security threats; and conducts domestic collection, analysis, and dissemination of cyber threat information.[93] In ensuring a whole-of-government approach to combating cyber threats to national security, the National Security Division of the DoJ, in partnership with other components of the department, has launched a nationwide National Security Cyber Specialist Network to better address cyber intrusions and attacks carried out by nation states or terrorist organisations.[94] The DoJ's Computer Crime and Intellectual Property Section prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.[95]

As mentioned in section 2.2, the *Homeland Security Act* of 2002 created the Department of Homeland Security (DHS) and placed it in charge of critical infrastructure protection across IT and communications sectors.[96] As part of the Office of Cybersecurity and Communications (CS&C) within the DHS agency of National Protection and Programs Directorate (NPPD), the National Cybersecurity & Communications Integration Centre (NCCIC) coordinates the cyber security aspects of critical infrastructure protection.[97] NPPD is primarily responsible for fulfilling DHS's national, non-law enforcement cyber security missions; within the NPPD, the Office of Cybersecurity and Communications (CS&C) provides crisis management, incident response, and defence capabilities for the entirety of US cyber and communication infrastructure. It is also responsible for the implementation of the Enhanced Cybersecurity Services programme.[98]

[93] '2014 Quadrennial Homeland Security Review' (n 25).
[94] U.S. Department of Justice, 'Combatting National Security Cyber Threats' <http://www.justice.gov/nsd/about-division-0>.
[95] U.S. Department of Justice, 'Computer Crime & Intellectual Property Section', 2014 <http://www.justice.gov/criminal/cybercrime/>.
[96] 'Cyberspace Policy Review' (n 44) appendix C.
[97] Cyber security assets can be found also in other directorates such as Science and Technology, and Intelligence and Analysis.
[98] 'Implementation Status of the Enhanced Cybersecurity Services Program' (n 54).

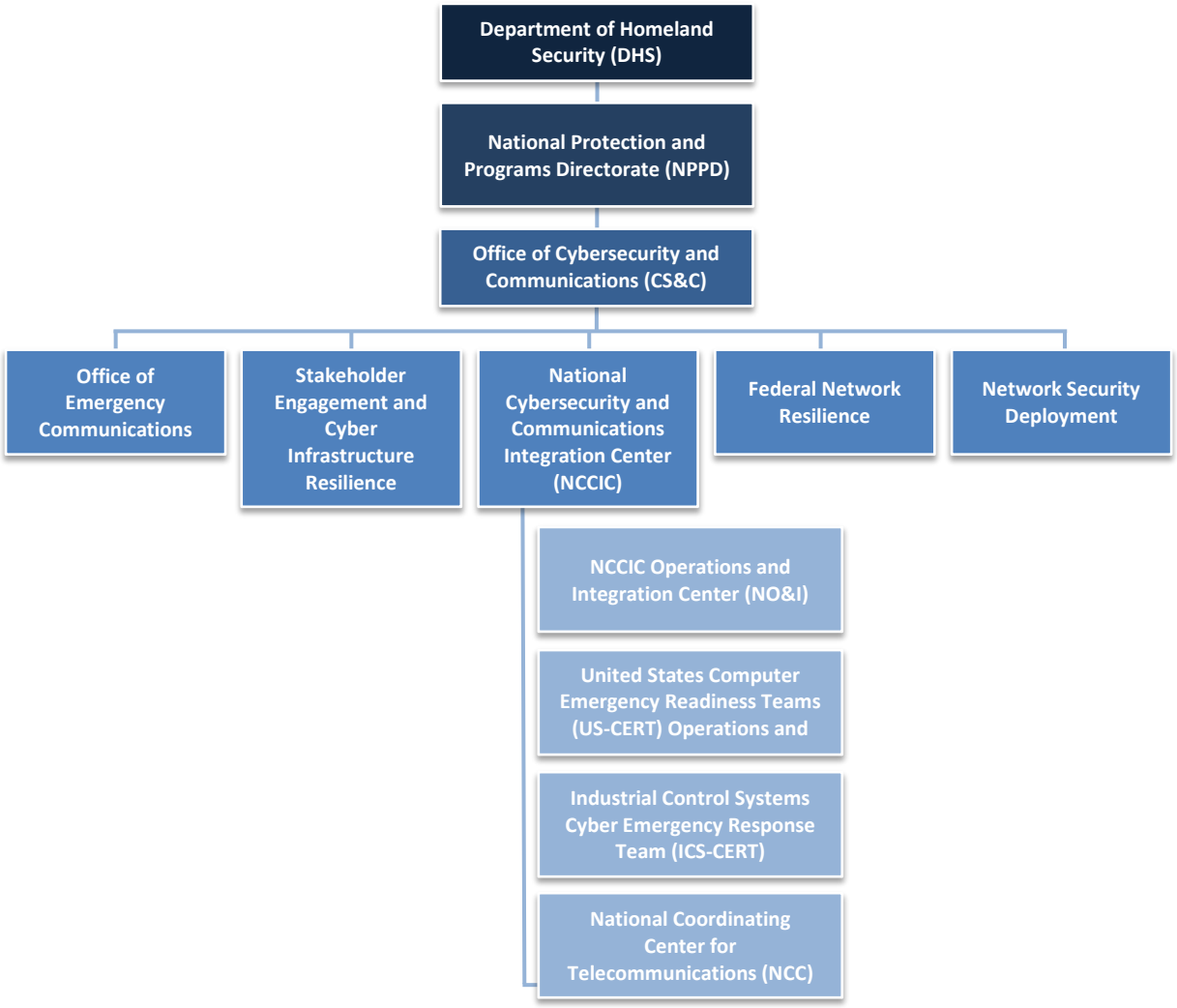

Figure 1. CS&C Organisational chart

NCCIC provides a management centre that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement.[99] Its mission emphasises cooperation and information sharing between all levels of government and the private sector. Although NCCIC works closely with critical infrastructure owners and operators, it has no authority to enforce compliance with cyber security measures in the private sector: its activities include the provision of situational awareness regarding vulnerabilities, intrusions, incidents, mitigation, and data recovery actions.[100] NCCIC pursues its mission with four branches consisting of NCCIC Operations and Integration (NO&I), the US Computer Emergency Readiness Team (US-CERT), the Industrial US Computer Emergency Readiness Team (ICS-CERT), and National Coordinating Centre for Communications (NCC).[101] These branches provide a framework for coordination and support of all federal agencies in securing their systems and aiding in any cyber security related issues as tasked by FISMA.[102]

NO&I develops operational planning, training, and exercises for the NCCIC. It manages (including planning, executing and participation) various cyber exercises at the national and international levels and within private

[99] U.S. Department of Homeland Security, 'Office of Cybersecurity and Communications', 2014 <http://www.dhs.gov/office-cybersecurity-and-communications>.
[100] Philippe VItel, 'Cyber Space and Euro-Atlantic Security', NATO Parliamentary Assembly, 2014 <http://www.nato-pa.int/shortcut.asp?FILE=3551>'.
[101] DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers (n **Error! Bookmark not defined.**).
[102] Ibid, 3.

sector, ranging from small-scale table-top exercises to large-scale operations-based exercises.[103]

US-CERT responds to cyber incidents, provides technical assistance to operators, and disseminates notifications about current and potential threats. US-CERT distributes information to the government, the private sector, and international organisations and partners. For example, it provides a web portal to share cyber-related information and news with both the public and private sectors and publishes a weekly Cyber Security Bulletin with a summary of new vulnerabilities. In addition, US-CERT has established several important collaboration groups and programmes to foster and facilitate information sharing on cyber security issues among government agencies, including: the Federal CIO Council, the Government Forum of Incident Response and Security Teams; the National Council of Information Sharing Analysis Centres; and the Software Assurance Community Resources and Information Clearinghouse.[104]

ICS-CERT reduces risk to critical infrastructure by strengthening industrial control systems security through public-private partnerships. ICS-CERT has four focus areas: situational awareness for critical infrastructure and key resources stakeholders; control systems' incident response and technical analysis; control systems' vulnerability coordination; and strengthening cyber security partnerships with government departments and agencies.[105] It produces various alerts, advisories, newsletters, and reports for critical infrastructure owners and operators.

NCC leads every aspect of telecommunication infrastructure and services repair or expansion. Coordination is accomplished via partnerships in the government and with private sector stakeholders, both nationally and internationally.[106]

3.3. Military cyber defence

3.3.1. Department of Defense

While DHS protects .gov infrastructure and civilian government networks, the Department of Defense (DoD) is tasked with safeguarding the .mil domain and the DoD's global information infrastructure from cyber attack. DoD moreover has responsibilities for gathering foreign cyber threat information, securing national security and military systems, and investigating cybercrimes under military jurisdiction.[107]

DoD's cyber activities and missions are guided by the 2015 Department of Defense Cyber Strategy (see 2.3), which considers three main 'missions' for DoD in cyber: cyber security and operational capability building for the protection of DoD networks, systems, and information; defence against cyber attacks 'of significant consequence' targeting the nation; and support to military operations and contingency plans.[108]

The operational roles and responsibilities of DoD in cyber security are realised through USCYBERCOM Joint Operations Center (see 3.3.2.), the National Security Agency/Central Security Service Center, the Defense Cyber Crime Center, and the Defense Information Systems Agency (DISA).[109] Specifically, DISA has been tasked with providing information technology and communications support to and defending military networks.

While President Obama's 2015 budget proposal projected a decline in the overall funding for DoD budget and for federal government IT in 2015, funding for cyberspace operations increased by 8.5%. This increased funding supports, among others, the prioritisation of R&D for cyberspace operations (as one of the six priority areas of

[103] U.S. Computer Emergency Readiness Team, 'National Cybersecurity and Communications Integration Center', <https://www.us-cert.gov/nccic>.
[104] U.S. Computer Emergency Readiness Team, 'About Us', <https://www.us-cert.gov/about-us>.
[105] DHS' Efforts to Coordinate The Activities of Federal Cyber Operations Centers (n **Error! Bookmark not defined.**), 6.
[106] U.S. Computer Emergency Readiness Team, 'The National Coordinating Center for Communications' <https://www.us-cert.gov/nccic/ncc-watch>.
[107] 2014 Quadrennial Homeland Security Review (n 25).
[108] Department of Defense Cyber Strategy 2015 (n 80).
[109] 2014 Quadrennial Homeland Security Review (n 25).

the DoD), including defensive and offensive cyberspace operations and the development of USCYBERCOM's Cyber Mission Forces. Other cyber-relevant priority areas were distinguished as well, such as operations providing information assurance and cyber security to the DoD networks; supporting cyberspace research and technology projects; supporting defensive cyberspace operations; recognising and augmenting personnel within the combatant commands to support the integration and coordination of cyberspace operations; and supporting ongoing investments in the DoD's larger IT budget.[110]

3.3.2. USCYBERCOM and cyber components of military services

Each military service has a cyber component that reports to the US Cyber Command (USCYBERCOM), a sub-unified command under US Strategic Command (USSTRATCOM)[111], located at Fort Meade Maryland and co-located with the headquarters of the National Security Agency (NSA). The Director of the NSA is 'dual-hatted' as the Commander of USCYBERCOM.[112]

USCYBERCOM was established in 2010 and achieved initial operational capability in the same year. Its service elements include three-star commands representing each military service: Army Cyber Command (ARCYBER), US Fleet Cyber Command 10th Fleet (FCC/C10F), US Marine Corps Forces Cyberspace (MARFORCYBER), 24th Air Force (AFCYBER), and Coast Guard Cyber Command (CGCYBER).[113]

USCYBERCOM has primary responsibility for centralised command and control of cyberspace operations, including their synchronisation, planning and execution.[114] It leads day-to-day defence and protection of DoD information networks; coordinates DoD operations providing support to military missions; directs the operations and defence of specified DoD information networks; and prepares to conduct full spectrum military cyberspace operations when directed.[115]

With each service branch defining their mission slightly differently, the USCYBERCOM ensures consistency among the cyber activities of the branches. Their overall goals remain the same: ensuring the defence of their IT infrastructure to enable superiority in command and control; and conducting electronic warfare, signal intelligence and information operations across the full spectrum of their warfare components.

The five priorities for USCYBERCOM are to build a trained and ready cyber force, put tools in place that create true situational awareness in cyberspace, create command-and-control and operational concepts to execute the mission, build a joint defensible network, and ensure the command has the right policies and authorities that allow it to execute full-spectrum operations in cyberspace.[116]

By 2016, the DoD is expected to develop a Cyber Mission Force (CMF), projected to include more than 6,000 military and civilian personnel as well as contractor support from the military departments and defence

---

[110] Dennis Murphy, 'Pentagon Budget 2015: DoD Cyberspace Operations Would Get 8.5% Boost', Jane's Defence Weekly, 2014 <http://www.janes.com/article/35427/pentagon-budget-2015-dod-cyberspace-operations-would-get-8-5-boost>; U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, 'United States Department of Defense Fiscal Year 2015 Budget Request', 2014. <http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/fy2015_Budget_Request_Overview_Book.pdf>.

[111] United States Strategic Command is one of nine DoD Combatant Commands. Personnel and leadership are selected from one of the military branches: Department of the Army, Department of the Navy, Department of the Air Force.

[112] Gallagher, Sean, 'White House: NSA and Cyber Command to stay under one boss', Arstechnica, 2013 <http://arstechnica.com/tech-policy/2013/12/white-house-nsa-and-cyber-command-to-stay-under-one-boss/>.

[113] U.S. Department of Defense, 'U.S. Cyber Command Fact Sheet', 2010, <http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf>.

[114] Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions' (n 11); The White House, 'Presidential Memorandum--Unified Command Plan 2011', Washington, 2011 <https://www.whitehouse.gov/the-press-office/2011/04/06/presidential-memorandum-unified-command-plan-2011>.

[115] 'U.S. Cyber Command Fact Sheet', 2010 (n 116).

[116] USCYBERCOM commander Adm Mike Rogers outlined these priorities during an interview at the NSA headquarters on 14 August 2014. Cheryl Pellerin, 'Rogers: Cybercom Defending Networks, Nation', U.S. Department of Defense (DoD) News, 2014 <http://www.defense.gov/news/newsarticle.aspx?id=122949>.

components.[117] The CMF will comprise four types of teams: National Mission Teams providing support in case of 'cyberattacks of significant consequence' to the nation; Cyber Protection Teams to defend DoD's priority networks and systems and to support military operations worldwide; Combat Mission Teams, which support operational plans and contingency operations; and Support Teams to provide analytic and planning support.[118] In particular, the 27 Combat Missions Teams will support the combatant commands, such as the US Central Command, Pacific Command, and European Command.[119] In order to simulate cyberspace operations and test new technologies and capabilities, a National Cyber Range will be developed.[120]

The Joint Operations Centre at Fort Meade is currently in the process of construction and is scheduled to be occupied in 2018.[121] Combatant commanders also have their own Combatant Command Joint Cyberspace Centres that receive support from USCYBERCOM; such support includes the establishment of Network Operations and Security Centres during an operation.[122]

The US Army Cyber Command (ARCYBER) will develop forces needed to support the combatant commands and DoD, integrated fully with the Joint Information Environment, and will pursue cyberspace capabilities to the lowest echelons of the Army. ARCYBER is intended to reach full operational capability by the end of 2015, and will be relocated to Fort Gordon, Georgia, to be situated together with the Army Cyber Center of Excellence[123] and a regional office of the National Security Agency.[124] The main components of ARCYBER are the Army Cyber Centre (USMA) and Army Cyber Operations and Integration Centre (ACOIC).[125]

The 24th Air Force (AFCYBER) achieved full operational capability in 2010. Its mission is 'to operate, extend, and defend its own network, defend key mission systems, and provide full spectrum cyberspace capabilities'. It executes 24/7 full spectrum cyberspace operations, and its fighting force amounts to 5,400 active duty and 11,000 reserve personnel.[126]

The 2013 Joint Information Environment White Paper spells out a plan for consolidating data centres among the branches of the military to ensure leaders have the most accurate information; placing data centres in the cloud is another plan for increasing information sharing and agility within the US military.[127]

3.4. Crisis management

In respect to domestic crisis management, DHS provides crisis management and technical assistance to other federal government entities and the private sector.[128] While crisis response coordination is centralised in the federal government, the execution is decentralised with each of the cyber incident response partners playing a legally mandated role. Public and private sector organisations are responsible for the preparedness activities and maintaining response capabilities and recovery actions. These capabilities, actions, roles and

[117] Ellen Nakashima, 'U.S. Cyberwarfare Force to Grow Significantly, Defense Secretary Says', The Washington Post, 2014 <http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html>; 'The Department of Defense Cyber Strategy' (n 80).
[118] Ibid.
[119] Warren Strobel *et al*, 'With Troops and Techies, U.S. Prepares for Cyber Warfare', Reuters, 2013 <http://www.reuters.com/article/2013/06/07/us-usa-cyberwar-idUSBRE95608D20130607>.
[120] 'The Department of Defense Strategy For Operating in Cyberspace 2011' (n 78).
[121] 'United States Department of Fiscal Year 2015 Budget Request', 2014 (n 110).
[122] 'Cyberspace Operations. Joint Publication 3-12 (R)', 2013 (n 76).
[123] The Army Cyber CoE ensures Army cyber capabilities align with Joint force requirements and capabilities. U.S. Army, 'Army Cyber Center of Excellence and Fort Gordon', <http://www.army.mil/ArmyCyberCoE>.
[124] 'On DoD: Army Charts Overlaps Between Cyber, Electronic Warfare' (n 75).
[125] 'United States Department of Defense Fiscal Year 2015 Budget Request' (n 110).
[126] U.S. Air Force, '24th Air Force Fact Sheet', 2014 <http://newpreview.afnews.af.mil/24af/library/factsheets/factsheet.asp?id=15663>.
[127] The Joint Chiefs of Staff (JCS), 'Joint Information Environment White Paper', Washington, 2013 <http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf>.
[128] The White House, 'The National Strategy to Secure Cyberspace' (n 15).

responsibilities are described in the DHS's strategic framework for operational coordination and execution, the *National Cyber Incident Response Plan* (see 2.2).[129] In addition to the DHS, key roles are played by the White House, DoD, NSA, DoJ, Federal Bureau of Investigation (FBI), DoS, sector-specific agencies (SSAs),[130] other federal and state, local, tribal and territorial governments, as well as the private and non-governmental sectors, and international partners. DHS also houses an Office for Infrastructure Protection which leads the efforts to secure critical infrastructure, particularly focusing on government cooperating with the private sector infrastructure operators.[131]

In the case of an attack on a member of the defence industrial base that supports US military operations, DoD is the designated sector-specific agency. Further, in certain cases, DoD may be instructed to take the lead from DHS and provide defence support to civil agencies.[132]

In steady state (daily operation), the DHS, through its National Cybersecurity and Communications Integration Center (NCCIC, see 3.2.), coordinates national response efforts and information sharing and provides situational awareness (including a 24/7 steady-state common operational picture) across the nation's cyberspace. NCCIC coordinates regularly with federal, state, local, tribal and territorial governments, law enforcement, the intelligence community, international computer emergency response teams (CERTs), domestic information sharing and analysis centres (ISACs),[133] and critical infrastructure partners within the private sector.[134] It works with other federal cyber centres to exchange critical information and coordinate analytical and response processes; federal law enforcement, critical infrastructure partners, and SSAs and ISACs have been incorporated into its day-to-day operations. Through US-CERT's and ICS-CERT's portals, NCCIC shares sensitive cyber security information with validated private sector, government, and international partners.[135]

As the central national point for coordination for day-to-day cyber response efforts, the NCCIC also coordinates response to significant cyber incidents. During periods of heightened threat, the NCCIC coordinates and conducts classified briefings – in conjunction with the intelligence community – with SSAs, government coordinating councils,[136] and sector coordinating councils.[137] In addition to its partners, NCCIC coordinates with DHS' other coordination centres (National Operations Centre, National Infrastructure Coordinating Centre, National Response Coordination Centre) and communicates situational awareness to the White House.[138]

The Cyber Unified Coordination Group, an interagency and inter-organisational coordination body representing the public and private sectors, ensures unity of NCCIC coordination during the steady state and facilitates rapid

[129] More detailed operational plans are at the sector and organisational levels. 'National Cyber Incident Response Plan (NCIRP)' (n 68).
[130] Federal department or agency designated with responsibility for providing institutional knowledge and specialised expertise as well as leading, facilitating, or supporting the security and resilience programmes and associated activities of its designated critical infrastructure sector. 'Presidential Policy Directive - Critical Infrastructure Security and Resilience/PPD-21' (n 51).
[131] U.S. Department of Homeland Security, National Protection and Programs Directorate, 'Office of Infrastructure Protection Strategic Plan: 2012- 2016', 2012 http://www.dhs.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf>.
[132] 'Cyberspace Operations. Joint Publication 3-12 (R)', 2013 (n 76).
[133] Operational entities formed by critical infrastructure owners and operators to gather, analyse, appropriately sanitise, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. 'Presidential Decision Directive/NSC-63. Critical Infrastructure Protection' (n 44).
[134] U.S. Department of Homeland Security, 'Supplemental Tool: Connecting to the NICC and NCCIC', <http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Connecting%20to%20the%20NICC%20and%20NCCIC_508.pdf>; 'National Cyber Incident Response Plan (NCIRP)' (n 68).
[135] Ibid.
[136] The government council for each sector, established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government. 'National Infrastructure Protection Plan (NIPP)', 2009 (n 50).
[137] The private sector organisations representing key stakeholders within each critical infrastructure sector. Adapted from: Ibid.; 'Supplemental Tool: Connecting to the NICC and NCCIC' (n 134).
[138] 'National Cyber Incident Response Plan (NCIRP)' (n 68).

response in the event of significant cyber incident.[139] However, the principal federal interagency mechanism that coordinates the preparation, response, recovery effort, and operational information sharing during 'nationally significant cyber incidents' is the National Cyber Response Coordination Group (NCRCG). It includes members from 19 federal departments and agencies which coordinate through their established relationships with state, local, tribal, and territorial governments and private sector.[140]

Both the US-CERT and the ISC-CERT are key players in crisis management. By facilitating information sharing amongst different players, they have the knowledge and pre-existing connections to assist with incident and crisis management.

3.5. Cyber intelligence

The US Intelligence Community, headed by the Director of National Intelligence[141] (DNI) is intrinsically linked to cyber due to the amount of information that flows throughout shared information technology infrastructures of the world. The Office of the Director of National Intelligence coordinates 17 agencies and organisations, many of which are under the authority of DHS and DoD.[142] DNI establishes objectives across the intelligence community, but has no direct control over the personnel of the various agencies.

The National Security Agency (NSA) is the primary cyber security agency in the national security sector, although other agencies also play significant roles. The Director of the NSA, who is also the Commander of the US Cyber Command and the Central Security Serve, reports to the Director of National Intelligence. The NSA also provides signals intelligence to various to components of the DoD.[143]

As a result of the CNCI, The Federal Bureau of Investigation (FBI) manages the National Cyber Investigative Joint Task Force (NCIJTF) which aggregates counterintelligence, counterterrorism, intelligence, and law enforcement information and activities from 19 federal agencies in order to predict and prevent cyber attacks.[144]

The Intelligence Community provides and secures the intelligence technology for the armed forces.[145]

3.6. Engagement with the private sector

In contrast to many European countries, where critical infrastructure owners and operators are legally obliged to report major cyber security incidents to a designated government authority, in the US information-sharing about vulnerability and risk assessments between the federal government and the private sector is voluntary. Similarly, primary responsibility for protection, response, and recovery from cyber attacks targeting critical

[139] Ibid.
[140] IT Law Wiki, Wikia, 'National Cyber Response Coordination Group (NCRCG)' <http://itlaw.wikia.com/wiki/National_Cyber_Response_Coordination_Group>; 'National Response Plan: Cyber Incident Annex' (n 68).
[141] This position is not a cabinet seat and though a political office, it does not carry the weight of the Secretary of Defence or the Secretary of Homeland Security.
[142] Air Force Intelligence (DoD), Army Intelligence (DoD), Central Intelligence Agency, Coast Guard Intelligence (DHS), Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation (DOJ), Marine Corps Intelligence (DoD), National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, Navy Intelligence (DoD), and the Office of the Director of National Intelligence. Office of the Director of National Intelligence, Members of the IC <http://www.dni.gov/index.php/intelligence-community/members-of-the-ic>.
[143] The Joint Chiefs of Staff (JCS), 'Joint Publication 3-12 (R) Cyberspace Operations', 2013 (n 76).
[144] U.S. Department of Justice, The Federal Bureau of Investigation (FBI), 'National Cyber Investigative Joint Task Force (NCIJTF)' <http://www.fbi.gov/about-us/investigate/cyber/ncijtf>.
[145] U.S. Coast Guard, 'United States Coast Guard Cyber Strategy', p.21, Department of Homeland Security, 2015 <https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf>; U.S. Central Intelligence Agency, 'Executive Order 12333', 1981 <https://www.cia.gov/about-cia/eo12333.html>.

infrastructure lies with the owners and operators of these assets.[146] The policy of the US government is to increase information sharing with the private sector.[147]

Much of the incident management and coordination is done in cooperation with the private sector due to the amount of infrastructure and knowledge that the private sector possesses. DHS's NCCIC is a leader in collaborating with the private sector in order to secure critical infrastructure and key resources; it particularly works with telecommunications and information infrastructures.

Each critical infrastructure sector has established its own information sharing centres. For example, in the energy sector, an information sharing and analysis centre was established in 1998, while the Cybersecurity Risk Information Sharing programme, established in 2013, provides energy sector organisations with near-real-time cyber threat information and analysis.[148] In order to overcome the reluctance of companies to report cyber incident data publicly – given potentially negative regulatory or reputational consequences – an anonymised information sharing portal that enables cyber incident trend analysis and benchmarking for critical infrastructure has been developed.[149] The portal aggregates anonymised cyber security scores from organisations and enables companies to measure their progress against their peers.[150]

The National Cyberspace Security Response System, as described in the *National Strategy to Secure Cyberspace*, is a public-private system which provides mechanisms for rapid identification, information exchange, response, and remediation to mitigate the damage caused by malicious cyberspace activity.[151]

The National Institute of Standards and Technology (NIST) under the Department of Commerce (DoC) develops cyber security standards and guidelines that are promulgated by the Office of Management and Budget (OMB). Together with the DoC, NIST manages the *National Initiative for Cybersecurity Education* (NICE) which enhances the recruitment, training, and retention of cyber security professionals, the raising of public awareness, and the promotion of cyber security education in schools.[152] The DoC also manages the contract with the Internet Corporation for Assigned Names and Numbers (ICANN), which otherwise employs a multi-stakeholder governance structure and is, as such, a key vessel for public-private cooperation and engagement.[153]

There are numerous public-private partnership initiatives. Some of the most effective are as follows:

[146] However, some critical infrastructure sectors (nuclear, maritime, etc.) must meet specific standards for assessing their vulnerabilities. 'Critical Infrastructures: Background, Policy, and Implementation' (n 48).
[147] National Strategy for Information Sharing and Safeguarding (December 2012), establishes the need for information sharing processes and sector-specific protocols with the private sector to improve information quality and timeliness. The White House, 'National Strategy for Information Sharing and Safeguarding (NSISS)', Washington, 2012 <http://nsi.ncirc.gov/documents/NSISS_2012_White_House.pdf?AspxAutoDetectCookieSupport=1>.
[148] The Electricity Sector Information Sharing and Analysis Center shares critical information with the industry on infrastructure protection, including threat indications, vulnerabilities and protective strategies. The Electricity Sector Information Sharing and Analysis Center (ES-ISAC), 'FAQ' <https://www.esisac.com/SitePages/FAQ.aspx>.
About the Cybersecurity Risk Information Sharing Program, see: Energy.gov, 'Energy Department Releases New Guidance for Strengthening Cybersecurity of the Grid's Supply Chain', 2014 <http://energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain>.
[149] U.S. Department of Homeland Security's National Protection and Programs Directorate (NPPD), 'Insurance Industry Working Session Readout Report - Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues', 2014 <http://insidecybersecurity.com/iwpfile.html?file=aug2014%2Fcs2014_0152.pdf>.
[150] The portal will be developed for the Cybersecurity Capability Maturity Model programme. Inside Cybersecurity, 'DOE: Web Portal Will Enable Cybersecurity Benchmarking' <http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/doe-web-portal-will-enable-cybersecurity-benchmarking/menu-id-1075.html>.
[151] White House, 'The National Strategy to Secure Cyberspace' (n 15).
[152] 'Cybersecurity Progress After President Obama's Address' (n 42).
[153] U.S. Department of Commerce, National Telecommunication and Information Administration (NTIA), 'FY 2015 Budget as Presented to Congress', 2014 <www.ntia.doc.gov/files/ntia/publications/ntia2015cjfinal.pdf>.

- The public-private partnership framework, National Infrastructure Protection Plan (NIPP), outlines how the federal government and critical infrastructure owners and operators can work together to manage risks and achieve security and resilience.[154]
- Both DHS and the DoD have in place public-private partnership arrangements, including the National Cyber Security Partnership.
- Partnerships between DHS, DoD and Defence Industrial Base (DIB) aims to increase the protection of sensitive information. The DIB *Cybersecurity and Information Assurance Program*, established in 2012 by DoD and DHS, was created to enhance the resiliency of Defence Industrial Base critical infrastructure companies through increased cyber threat information sharing.[155]
- A voluntary information sharing initiative (established in 2012 as the Joint Cybersecurity Services Program, expanded in 2013) initiated by DHS, the Enhanced Cybersecurity Services (ECS) programme, with an aim to share unclassified and classified indicators of malicious cyber activity with critical infrastructure sector participants. Sector-specific agencies and government furnished information providers supply the cyber threat indicators and technical information to the programme. The effectiveness of the programme has been questioned because the enrolment to the programme has been slow – as of March 2014, only three sectors (Defence Industrial Base, energy, and communication services) from the 16 critical infrastructure sectors were receiving its services.[156]

Another noteworthy example of private-public collaboration is *Einstein*, the DHS's intrusion detection system designed to detect malicious traffic targeting federal government civilian networks, which is delivered through commercial technology and with participation from commercial service providers. The programme provides an automated process for collecting, correlating, analysing, and sharing computer security information across the federal government in order to enhance cyber security analysis, situational awareness, and security response.[157] Currently the programme is in its third phase (Einstein 3) and provides an intrusion prevention system that is able to automatically detect and respond to cyber threats before harm is done, thus preventing malicious traffic from harming federal government civilian networks.[158]

Enhancing public-private partnerships is a core component of the US's efforts to secure itself in cyberspace; nonetheless, many challenges for improving the effectiveness of public-private information sharing still remain.[159]

[154] U.S. Department of Homeland Security, 'National Infrastructure Protection Plan. NIPP Cover NIPP 2013 Partnering for Critical Infrastructure Security and Resilience', 2015 <http://www.dhs.gov/national-infrastructure-protection-plan>.
[155] The DIB comprises the public and private organisations and corporations that support DOD through the provision of defence technologies, weapons systems, policy and strategy development, and personnel. 'The Department of Defense Strategy for Operating in Cyberspace 2011' (n 78).
[156] 'Implementation Status of the Enhanced Cybersecurity Services Program' (n 54).
[157] U.S. Department of Homeland Security, 'Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A)', DHS/PIA/NPPD-027, 2013 <http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf>.
[158] 'The Comprehensive National Cybersecurity Initiative (CNCI)' (n 37).
[159] 'High-Risk Series. An Update' (n 18).

References

Clayton, Mark, 'Senate Cybersecurity Bill Fails, So Obama Could Take Charge', The Christian Science Monitor, 2012 <http://www.csmonitor.com/USA/Politics/2012/1116/Senate-cybersecurity-bill-fails-so-Obama-could-take-charge>.

Couts, Andrew, 'Senate Kills Cybersecurity Act of 2012', Digital Trends, 2012 <http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/>.

Daniel, Michael, 'Assessing Cybersecurity Regulations', The White House Blog, 2014 <http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations>.

Energy.gov, 'Energy Department Releases New Guidance for Strengthening Cybersecurity of the Grid's Supply Chain', 2014 <http://energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain>.

Executive Office of the President of the United States, 'Digital Government. Building a 21st Century Platform to Better Serve the American People', 2012 <http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html>.

Fischer, Eric A., 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions', Congressional Research Service, 2013 <https://fas.org/sgp/crs/natsec/R42114.pdf>.

Fox, Susannah et al, 'The Web at 25 In the U.S. The Overall Verdict: The Internet has been a Plus for Society and an Especially Good Thing for Individual Users', Pew Research Center, 2014 <http://www.pewinternet.org/2014/02/25/the-web-at-25-in-the-u-s>.

Gallagher, Sean, 'White House: NSA and Cyber Command to stay under one boss', Arstechnica, 2013 <http://arstechnica.com/tech-policy/2013/12/white-house-nsa-and-cyber-command-to-stay-under-one-boss/>.

Google Fiber, 'Expansion Plans', 2015 <https://fiber.google.com/newcities/>

Horrigan, John B. and Duggan, Maeve, 'Home Broadband 2015', Pew Research Center, 2015 < http://www.pewinternet.org/files/2015/12/Broadband-adoption-full.pdf>.

Inside Cybersecurity, 'DOE: Web Portal Will Enable Cybersecurity Benchmarking' <http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/doe-web-portal-will-enable-cybersecurity-benchmarking/menu-id-1075.html>.

IT Law Wiki, Wikia, 'National Cyber Response Coordination Group (NCRCG)' <http://itlaw.wikia.com/wiki/National_Cyber_Response_Coordination_Group>.

ITU ICT-Eye, 'United States Profile', 2013 <http://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?countryID=244>.

Layne, Karen, and Jungwoo Lee. 'Developing fully functional E-government: A four stage model.' *Government Information Quarterly* 18, 2 (2001): 122-136

Moteff, John D., 'Critical Infrastructures: Background, Policy, and Implementation', Congressional Research Service, 2014 <http://fas.org/sgp/crs/homesec/RL30153.pdf>.

Murphy, Dennis, 'Pentagon Budget 2015: DoD Cyberspace Operations Would Get 8.5% Boost', Jane's Defence Weekly, 2014 <http://www.janes.com/article/35427/pentagon-budget-2015-dod-cyberspace-operations-would-get-8-5-boost>.

Nakashima, Ellen, 'U.S. Cyberwarfare Force To Grow Significantly, Defense Secretary Says', The Washington Post, 2014 <http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html>.

National Response Plan: Cyber Incident Annex', Federal Emergency Management Agency, 2004 <http://www.fema.gov/media-library-data/20130726-1825-25045-8307/cyber_incident_annex_2004.pdf>.

Office of the Director of National Intelligence, 'The National Intelligence Strategy of the United States of America', 2014. <http://www.dni.gov/files/documents/2014_NIS_Publication.pdf>.

Office of the Director of National Intelligence, Members of the IC <http://www.dni.gov/index.php/intelligence-community/members-of-the-ic>

Pellerin, Cheryl, 'Rogers: Cybercom Defending Networks, Nation', U.S. Department of Defense (DoD) News, 2014 <http://www.defense.gov/news/newsarticle.aspx?id=122949>.

POLITICO, 'Cyber Is the New Black: Cyber Coordinator Painter', 2014 <http://www.politico.com/multimedia/video/2014/07/cyber-is-the-new-black-cybersecurity-coordinator-painter-interview.html>.

Robinson, Neil et al, 'Cyber-Security Threat Characterization: A Rapid Comparative Analysis', RAND Corporation, 2013 <http://www.rand.org/pubs/research_reports/RR235.html>.

Rollins, John et al, 'Congressional Research Service Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations', Congressional Research Service, 2009 <http://fas.org/sgp/crs/natsec/R40427.pdf>.

Romm, Tony, 'Cybersecurity in Slow Lane One Year after Obama Order, ' Politico, 2014 <http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html>.

Selyukh, Alina, 'U.S. to Offer Companies Broad Standards to Improve Cybersecurity,' Reuters, 2014, <http://www.reuters.com/article/2014/02/12/us-usa-cybersecurity-standards-idUSBREA1B0AL20140212>.

Selyukh, Alina. 'U.S. Internet Providers Hit with Tougher Rules, Plan Challenges.' Reuters, 2015 <http://www.reuters.com/article/2015/02/26/us-usa-internet-neutrality-idUSKBN0LU0CA20150226>.

Serbu, Jared, 'On DoD: Army Charts Overlaps between Cyber, Electronic Warfare', Federal News Radio, 2014 <http://www.federalnewsradio.com/396/3682590/Army-contemplates-new-career-branch-for-cyber-personnel>.

Smith, Aaron, 'Civic Engagement in the Digital Age. Online and Offline Political Engagement', Pew Research Center, 2013 <http://www.pewInternet.org/2013/04/25/civic-engagement-in-the-digital-age/>.

Strobel, Warren et al, 'With Troops and Techies, U.S. Prepares for Cyber Warfare', Reuters, 2013 <http://www.reuters.com/article/2013/06/07/us-usa-cyberwar-idUSBRE95608D20130607>.

The Defence Advanced Research Projects Agency (DARPA), 'Plan X' <http://www.darpa.mil/Our_Work/I2O/Programs/Plan_X.aspx>.

The Electricity Sector Information Sharing and Analysis Center (ES-ISAC), 'FAQ' <https://www.esisac.com/SitePages/FAQ.aspx>.

The Joint Chiefs of Staff (JCS), 'Compendium of Key Joint Doctrine Publications', 2014 <http://www.dtic.mil/doctrine/new_pubs/compendium.pdf>.

The Joint Chiefs of Staff (JCS), 'Joint Information Environment White Paper', Washington, DC, 2013 <http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf>.

The Joint Chiefs of Staff (JCS), 'Joint Publication 3-12 (R) Cyberspace Operations', 2013 <http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf>.

The Joint Chiefs of Staff (JCS), 'The National Military Strategy for Cyberspace Operations (U)', Washington, 2006 <http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf>.

The United States Congress, 'H.R.2458 – E-Government Act of 2002. 107th Congress (2001-2002)', 2002 <https://www.congress.gov/bill/107th-congress/house-bill/2458>.

U.S. Air Force, '24th Air Force Fact Sheet', 2014 <http://newpreview.afnews.af.mil/24af/library/factsheets/factsheet.asp?id=15663>.

U.S. Army War College, Department of Military Strategy, Planning, and Operations & Center for Strategic Leadership, 'Information Operations Primer: Fundamentals of Information Operations', AY12 Edition, Carlisle, 2011 <www.au.af.mil/au/awc/awcgate/army-usawc/info_ops_primer.pdf>.

U.S. Army, 'Army Cyber Center of Excellence and Fort Gordon', <http://www.army.mil/ArmyCyberCoE>.

U.S. Census Bureau, 'E-Stats 2013: Measuring the Electronic Economy', 2015. <http://www.census.gov/econ/estats/e13-estats.pdf>.

U.S. Census Bureau, 'Table 4. Households with a Computer and Internet Use: 1984 To 2012', 2014 <http://www.census.gov/hhes/computer/files/2012/table4.xls>.

U.S. Central Intelligence Agency, 'Executive Order 12333', 1981 <https://www.cia.gov/about-cia/eo12333.html>.

U.S. Chamber of Commerce, '2014 Cybersecurity Education & Framework Awareness Campaign. Improving Today. Protecting Tomorrow™', Austin, Texas, 2014 <https://www.uschamber.com/programs/national-security-emergency-preparedness/2015-cybersecurity-campaign/education-awareness >.

U.S. Coast Guard, 'United States Coast guard Cyber Strategy', Washington, DC: Department of Homeland Security, 2015 <https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf>.

U.S. Computer Emergency Readiness Team, 'About Us', <https://www.us-cert.gov/about-us>.

U.S. Computer Emergency Readiness Team, 'National Cybersecurity and Communications Integration Center', <https://www.us-cert.gov/nccic>.

U.S. Computer Emergency Readiness Team, 'The National Coordinating Center for Communications' <https://www.us-cert.gov/nccic/ncc-watch>.

U.S. Congress, 'Federal Information Security Modernization Act of 2014. 113th Congress (2013-2015)', 2D Session, 2014 <https://www.govtrack.us/congress/bills/113/s2521/text>.

U.S. Congress, 'S. 2519 – National Cybersecurity and Communications Integration Centre Act of 2014', 2014 <https://www.cbo.gov/publication/45594>.

U.S. Department of Army, 'Cyber Electromagnetic Activities', No. 3-38, Washington, 2014 <http://fas.org/irp/doddir/army/fm3-38.pdf>.

U.S. Department of Commerce, National Telecommunication and Information Administration (NTIA), 'FY 2015 Budget as Presented to Congress', 2014 <www.ntia.doc.gov/files/ntia/publications/ntia2015cjfinal.pdf>.

U.S. Department of Commerce, The National Institute of Standards and Technology (NIST), 'Framework for Improving Critical Infrastructure Cybersecurity', 2013 <http://www.nist.gov/cyberframework/index.cfm>.

U.S. Department of Commerce, The National Institute of Standards and Technology (NIST), 'Framework For Improving Critical Infrastructure Cybersecurity', Version 1.0, 2014 <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

U.S. Department of Defense, 'National Defense Strategy', 2008 <http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf>.

U.S. Department of Defense, 'National Military Strategy of The United States of America 2011: Redefining America's Military Leadership', Washington, 2011 <www.defense.gov/pubs/2011-National-Military-Strategy.pdf>.

U.S. Department of Defense, 'Quadrennial Defense Review 2014', 2014 <http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf>.

U.S. Department of Defense, 'Sustaining U.S. Global Leadership: Priorities for 21st Century Defense', 2012 <http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf>.

U.S. Department of Defense, 'The Department of Defense Strategy for Operating in Cyberspace 2011', 2011 <http://www.defense.gov/news/d20110714cyber.pdf>.

U.S. Department of Defense, 'The Department of Defense Strategy for Operating in Cyberspace 2015', 2015. <http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

U.S. Department of Defense, 'U.S. Cyber Command Fact Sheet', 2010, <http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf>.

U.S. Department of Defense, Office of General Counsel, 'Law of War Manual', 2015 <http://www.dod.mil/dodgc/images/law_war_manual15.pdf>.

U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, 'United States Department of Defense Fiscal Year 2015 Budget Request', 2014 <http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/fy2015_Budget_Request_Overview_Book.pdf>.

U.S. Department of Homeland Security, '2014 Quadrennial Homeland Security Review', 2014 <http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf>.

U.S. Department of Homeland Security, 'Blueprint for a Secure Cyber Future. The Cybersecurity Strategy for the Homeland Security Enterprise', 2011 <http://www.dhs.gov/blueprint-secure-cyber-future>.

U.S. Department of Homeland Security, 'Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection', 2003 <http://www.dhs.gov/homeland-security-presidential-directive-7>.

U.S. Department of Homeland Security, 'Identifying Critical Infrastructure', 2013 <http://www.dhs.gov/topic/critical-infrastructure-security>.

U.S. Department of Homeland Security, 'National Cyber Incident Response Plan (NCIRP)', Interim Version, 2010 <http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf>.

U.S. Department of Homeland Security, 'National Infrastructure Protection Plan 2006', 2006 <https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf>.

U.S. Department of Homeland Security, 'National Infrastructure Protection Plan 2009', 2009 <https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>.

U.S. Department of Homeland Security, 'National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience', 2013 <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

U.S. Department of Homeland Security, 'National Infrastructure Protection Plan. NIPP Cover NIPP 2013 Partnering for Critical Infrastructure Security and Resilience', 2015 <http://www.dhs.gov/national-infrastructure-protection-plan>.

U.S. Department of Homeland Security, 'National Infrastructure Protection Plan (NIPP): Partnering to Enhance and Resiliency', 2009 <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>.

U.S. Department of Homeland Security, 'Office of Cybersecurity and Communications', 2014 <http://www.dhs.gov/office-cybersecurity-and-communications>.

U.S. Department of Homeland Security, 'Our Mission', 2014 <http://www.dhs.gov/our-mission>.

U.S. Department of Homeland Security, 'Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A)', DHS/PIA/NPPD-027, 2013 <http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf>.

U.S. Department of Homeland Security, 'Supplemental Tool: Connecting to the NICC and NCCIC', <http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Connecting%20to%20the%20NICC%20and%20NCCIC_508.pdf>.

U.S. Department of Homeland Security, National Protection and Programs Directorate, 'Office of Infrastructure Protection Strategic Plan: 2012- 2016', 2012 http://www.dhs.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf>.

U.S. Department of Homeland Security, Office of Inspector General, 'DHS' Efforts To Coordinate The Activities of Federal Cyber Operations Centers', Washington, 2013 <http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf>.

U.S. Department of Homeland Security, Office of Inspector General, 'Implementation Status of The Enhanced Cybersecurity Services Program', Washington, 2014 <http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf>.

U.S. Department of Homeland Security's National Protection and Programs Directorate (NPPD), 'Insurance Industry Working Session Readout Report - Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues', 2014 <http://insidecybersecurity.com/iwpfile.html?file=aug2014%2Fcs2014_0152.pdf>.

U.S. Department of Justice, 'Combatting National Security Cyber Threats' <http://www.justice.gov/nsd/about-division-0>.

U.S. Department of Justice, 'Computer Crime & Intellectual Property Section', 2014 <http://www.justice.gov/criminal/cybercrime/>.

U.S. Department of Justice, 'Cyber Security', 2014 <http://www.justice.gov/jmd/2014factsheets/cyber-security.pdf>.

U.S. Department of Justice, The Federal Bureau of Investigation (FBI), 'National Cyber Investigative Joint Task Force (NCIJTF)' <http://www.fbi.gov/about-us/investigate/cyber/ncijtf>.

U.S. Department of State, 'Office Of The Coordinator For Cyber Issues' <http://www.state.gov/s/cyberissues/index.htm>.

U.S. Government Accountability Office, 'Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience', GAO-10-296, 2010.

U.S. House Committee on Homeland Security, 'National Cybersecurity and Critical Infrastructure Protection Act of 2013 (NCCIP Act)', H.R. 3696, 2013 <http://homeland.house.gov/sites/homeland.house.gov/files/documents/12113_NCCIP_summary.pdf>.

United Nations, 'United Nations E-Government Survey 2014. E-Government for the Future We Want', New York, 2014 <http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf>.

United States Congress, 'Federal Information Security Modernization Act of 2014. 113th Congress (2013-2015)', 2D Session, 2014 <https://www.govtrack.us/congress/bills/113/s2521/text>.

United States Congress, 'S. 2519 – National Cybersecurity and Communications Integration Centre Act of 2014', 2014 <https://www.cbo.gov/publication/45594>.

United States Government Accountability Office (U.S. GAO), 'High-Risk Series. An Update', 2013 <http://www.gao.gov/products/GAO-13-283>.

US CERT, National Cybersecurity and Communications Integration Center, <https://www.us-cert.gov/nccic>.

Vitel, Philippe, 'Cyber Space and Euro-Atlantic Security', NATO Parliamentary Assembly, 2014 <http://www.nato-pa.int/shortcut.asp?FILE=3551>.

White House, 'Cybersecurity' <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity>.

White House, 'Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure', 2009 <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

White House, 'International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World', 2011 <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

White House, 'National Security Strategy', 2010 <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>.

White House, 'National Security Strategy', 2015 <https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>.

White House, 'National Strategy for Information Sharing and Safeguarding (NSISS)', Washington, 2012 <http://nsi.ncirc.gov/documents/NSISS_2012_White_House.pdf?AspxAutoDetectCookieSupport=1>.

White House, 'National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy', Washington, 2011 <https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf>.

White House, 'Presidential Decision Directive/NSC-63. Critical Infrastructure Protection', Washington, 1998, Section II <http://fas.org/irp/offdocs/pdd/pdd-63.htm>.

White House, 'Presidential Memorandum--Unified Command Plan 2011', Washington, 2011 <https://www.whitehouse.gov/the-press-office/2011/04/06/presidential-memorandum-unified-command-plan-2011>.

White House, 'The Comprehensive National Cybersecurity Initiative (CNCI)' <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>.

White House, 'The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets', Washington, 2003 <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

White House, 'The National Strategy to Secure Cyberspace', Washington, 2003 <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>.

White House, National Security Council, 'Cybersecurity Progress after President Obama's Address', 2010 <http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010>.

White House, Office of the Press Secretary, 'Presidential Policy Directive - Critical Infrastructure Security and Resilience/PPD-21', 2013 <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

Zheng, Denise, '2015 DOD Cyber Strategy', Center for Strategic & International Studies, 2015 <https://csis.org/publication/2015-dod-cyber-strategy>.