Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity: Cybercrime and National Security Authoritative Reports and Resources

November 14, 2017 (R44408)

Jump to Main Text of Report

Rita Tehan, Information Research Specialist (rtehan@crs.loc.gov, 7-6739)

Summary

As online attacks grow in volume and sophistication, the United States is expanding its cybersecurity efforts. Cybercriminals continue to develop new ways to ensnare victims, whereas nation-state hackers compromise companies, government agencies, and businesses to create espionage networks and steal information. Threats come from both criminals and hostile countries, especially China, Russia, Iran, and North Korea.

Much is written on this topic, and this CRS report directs the reader to authoritative sources that address many of the most prominent issues. The annotated descriptions of these sources are listed in reverse chronological order, with an emphasis on material published in the past several years. This report includes resources and studies from government agencies (federal, state, local, and international), think tanks, academic institutions, news organizations, and other sources:

- **Table 1**—cybercrime, data breaches and security, including hacking, real-time attack maps, and statistics (such as economic estimates)
- **Table 2**—national security, cyber espionage, and cyberwar, including Stuxnet, China, and the Dark Web
- **Table 3**—cloud computing, the Internet of Things (IoT), smart cites, and FedRAMP

The following reports comprise a series of authoritative reports and resources on these additional cybersecurity topics:

- CRS Report R44405, *Cybersecurity: Overview Reports and Links to Government, News, and Related Resources*, by Rita Tehan.
- CRS Report R44406, *Cybersecurity: Education, Training, and R&D Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R44408, *Cybersecurity: Cybercrime and National Security Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R44410, *Cybersecurity: Critical Infrastructure Authoritative Reports and Resources*, by Rita Tehan.

Contents

- Introduction

Tables

- Table 1. Cybercrime, Data Breaches, and Data Security
- Table 2. National Security, Cyber Espionage, and Cyberwar
- Table 3. Cloud Computing, "The Internet of Things," Smart Cities, and FedRAMP

- CRS Report R44417, *Cybersecurity: State, Local, and International Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R44427, *Cybersecurity: Federal Government Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.
- CRS Report R43310, *Cybersecurity: Data, Statistics, and Glossaries*, by Rita Tehan.

Introduction

As online attacks grow in volume and sophistication, the United States is expanding its cybersecurity efforts. Cybercriminals continue to develop new ways to ensnare victims, whereas nation-state hackers compromise companies, government agencies, and businesses to create espionage networks and steal information. Threats come from both criminals and hostile countries, especially China, Russia, Iran, and North Korea.

Much is written on this topic, and this CRS report directs the reader to authoritative sources that address many of the most prominent issues. The annotated descriptions of these sources are listed in reverse chronological order, with an emphasis on material published in the past several years. This report includes resources and studies from government agencies (federal, state, local, and international), think tanks, academic institutions, news organizations, and other sources:

- **Table 1**—cybercrime, data breaches and security, including hacking, real-time attack maps, and statistics (such as economic estimates)
- **Table 2**—national security, cyber espionage, and cyberwar, including Stuxnet, China, and the Dark Web
- **Table 3**—cloud computing, the Internet of Things (IoT), and FedRAMP

Table 1. Cybercrime, Data Breaches, and Data Security
(include data breaches[1], hacking, real-time attack maps, statistics)

Title	Source	Date	Notes
The Cyberfeed	Anubis Networks	Continuously Updated	This site provides real-time threat inte worldwide.
Digital Attack Map	Arbor Networks	Continuously Updated	The map is powered by data fed from customers worldwide who have agre network traffic and attack statistics. T global activity levels in observed atta it collected anonymously, and does n identifying information about the atta involved in any particular attack.
Cyber Incident Timeline	Center for Strategic & International Studies (CSIS)	Continuously Updated	The CSIS's Strategic Technologies p interactive "Cyber Incident Timeline" successful attacks on government ag and high tech companies, and intern crimes with losses of more than $1 m 2006. It includes news reports and vi incidents.
Summary of U.S. State Data Breach Notification Statutes	Davis Wright Tremaine LLP	Continuously Updated	Click on any of the states to see a ful their data breach notification statute.
DataBreaches.net	Dissent (pseudonym)	Continuously Updated	This site is a combination of news ag investigative reporting, and comment breaches and data breach laws. Can breaches by sector.
ThreatExchange	Facebook	Continuously Updated	ThreatExchange is a set of applicatio interfaces, or APIs, that let disparate trade information about the latest onli

			atop the Facebook Platform—a repos standard set of tools for coding applic worldwide social network—ThreatExc by Facebook and a handful of other c including Tumblr, Pinterest, Twitter, a Access to the service is strictly contro [Facebook] hopes to include more co goes on.
Federal Trade Commission List of Settled Data Security Cases	Federal Trade Commission (FTC)	Continuously Updated	The FTC's Legal Resources website compilation of laws, cases, reports, a user can filter the FTC's legal docum (case) and topic (data security), resul 55 data security cases from 2000 to 2 chronological order. Clicking the case more details, such as the case citatio press releases, and pertinent legal do
Threat Intelligence Database	Fidelis Barncat	Continuously Updated	The database includes more than 10(with configuration settings extracted f samples gathered during Fidelis' incic investigations and other intelligence g operations over the past decade. The sample includes a large number of co elements, including those controlling the malware on the host and others r command-and-control traffic. Barncat hundreds of new configuration record Barncat is available for use by CERTs organizations, government entities, IS large commercial enterprises. Access users must request access and meet
IdentityTheft.gov	FTC	Continuously Updated	The one-stop website is integrated wi consumer complaint system, allowing who are victims of identity theft to rap complaint with the FTC and then get guide to recovery that helps streamlin steps involved. The upgraded site, wl and tablet accessible, offers an array tools that enables identity theft victim documents they need to alert police, bureaus, and the Internal Revenue S among others.
HHS Breach Portal: Breaches Affecting 500 or More Individuals	Health and Human Services (HHS)	Continuously Updated	As required by Section 13402(e)(4) o Act, P.L. 111-5 HHS must post a list c unsecured protected health informatio or more individuals. These breaches more accessible format that allows us and sort the posted breaches. Additio includes brief summaries of the brea Office for Civil Rights (OCR) has inve closed, as well as the names of priva providers who have reported breache protected health information.
Combatting Cyber Crime	Homeland Security	Continuously Updated	DHS works with other federal agencie high-impact criminal investigations to defeat cyber criminals, prioritize the r training of technical experts, develop methods, and broadly share cyber re practices and tools. Criminal investig network security experts with deep u the technologies malicious actors are specific vulnerabilities they are target effectively respond to and investigate
HoneyMap	Honeynet Project	Continuously	The HoneyMap displays malicious at

		Updated	happen. Each red dot represents an a computer. Yellow dots represent "hon systems set up to record incoming at box on the bottom gives the location The Honeynet Project is an internatio nonprofit security research organizati investigating the latest attacks and de source security tools to improve Inter
Data Breaches	Identity Theft Resource Center	Continuously Updated	The report presents detailed informat exposure events along with running t specific year. Breaches are broken do categories: business, financial/credit/ educational, governmental/military, a medical/healthcare.
Regional Threat Assessment: Infection Rates and Threat Trends by Location	Microsoft Security Intelligence Report (SIR)	Continuously Updated	The report provides data on infection websites, and threat trends by region worldwide. (Note: Select "All Regions country or region to view threat asses
No More Ransom	National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Center, Kaspersky Lab and Intel Security	Continuously Updated	The online portal offers a one-stop sh ransomware infections.
ThreatWatch	NextGov	Continuously Updated	ThreatWatch is a snapshot of the dat hitting organizations and individuals, daily basis. It is not an authoritative li many compromises are never reporte discovered. The information is based published by outside news organizati researchers.
No More Ransom	National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Center, Kaspersky Lab and Intel Security	Continuously Updated	The online portal offers a one-stop sh ransomware infections.
Information about OPM Cybersecurity Incidents	Office of Personnel Management (OPM)	Continuously Updated	In April 2015, OPM discovered that th data of 4.2 million current and former government employees had been sto such as full name, birth date, home a Social Security numbers was affecte investigating this incident, in early Ju discovered that additional informatio compromised, including background records of current, former, and prosp employees and contractors.
Chronology of Data Breaches, Security Breaches 2005 to the Present	Privacy Rights Clearinghouse (PRC)	Continuously Updated	The listed (U.S.-only) data breaches reported because the personal inform compromised includes data elements identity thieves, such as Social Secu account numbers, and driver's licens list is not a comprehensive compilati data. Most of the information is obtai verifiable media stories, government state Attorneys General, such as the breach website), or blog posts with in pertinent to the breach in question.
Criminal Underground Economy Series	Trend Micro	Continuously	A review of various cybercrime marke

		Updated	world.
Global Botnet Map	Trend Micro	Continuously Updated	Trend Micro continuously monitors m activities to identify command-and-co servers and help increase protection attacks. The real-time map indicates C&C servers and victimized compute that have been discovered in the prev
The Equifax Data Breach: What to Do	FTC	September 8, 2017	FTC information on what to do after t breach, including information how to s freeze and/or fraud alert.
Data Integrity: Recovering from Ransomware and Other Destructive Events (DRAFT)	NIST	September 6, 2017	Data integrity incidents, such as rans destructive malware, malicious inside even honest mistakes, can compromi information, including emails, employ financial records, and customer data.
The FDIC's Processes for Responding to Breaches of Personally Identifiable Information	FDIC Inspector General	September 2017	An FDIC audit found that protocols fo a data breach aren't being followed, e agency has faced dozens of security past two years. The audit stemmed fr data breaches at the FDIC over nearl from January 2015 to December 201 agency has confirmed or suspects th compromised 54 times within that tim Office of Inspector General selected breaches to evaluate for the audit. (5
The CERT Guide to Coordinated Vulnerability Disclosure	Carnegie Mellon	August 2017	This document is intended to serve a those who want to initiate, develop, o own CVD capability. In it, the reader w overview of key principles underlying process, a survey of CVD stakeholde roles, and a description of CVD proce well as advice concerning operationa and problems that may arise in the pr and related services. (121 pages)
Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display	GAO	July 27, 2017	GAO was asked to review federal gov to reduce the collection and use of SS examines (1) what governmentwide i been undertaken to assist agencies i their unnecessary use of SSNs and (which agencies have developed and to eliminate the unnecessary use and SSNs and have identified challenges those efforts.
Highlights of a Forum: Combating Synthetic Identity Fraud	GAO	July 26, 2017	According to experts, synthetic identi has grown significantly in the last five resulted in losses exceeding hundred dollars to the financial industry in 201 component of synthetic identities is S principal identifier in the credit reporti convened and moderated a diverse p experts on February 15, 2017, to disc criminals create synthetic identities; t the fraud; and issues related to preve detecting SIF and prosecuting crimina
Counting the Cost: Cyber Exposure Decoded	Lloyd's of London	July 10, 2017	Lloyd's Class of Business team estim global cyber market is worth between $3.5 billion. Despite this growth, insur understanding of cyber liability and ri is an evolving process as experience of cyber-attacks grows. (56 pages)
2017 Cost of Data Breach Study: Global	Ponemon and IBM	June 28, 2017	According to the report, the average t

Overview			breach for the 419 companies partici research study decreased from $4.00 million. The average cost for each los record containing sensitive and confid information also significantly decreas 2016 to $141 in this year's study. How the decline in the overall cost, compa year's study are having larger breach
2016 Internet Crime Report	Internet Crime Complaint Center's (IC3)	June 21, 2017	IC3 is a joint project of the National W Crime Center and the FBI. In 2016, IC total of 298,728 complaints with repor excess of $1.3 billion. This past year, crime types reported by victims were and nondelivery, personal data breac scams. (28 pages)
Stateless Attribution: Toward International Accountability in Cyberspace	RAND	June 2017	This report reviews the state of cyber examines alternative options for prod standardized and transparent attribut overcome concerns about credibility. exploratory work considers the value independent, global organization who consists of investigating and publicly cyber attacks. (64 pages)
Worldwide DDoS Attacks & Cyber Insights Research Report	Neustar	May 2, 2017	Public and private organizations glob slower at detecting and responding to denial of service (DDoS) attacks as th larger and more complex, new resear than half of organizations surveyed in reported taking three hours or more t attack on their websites in the past ye percent said that they take at least th respond to such an attack. (52 pages
Data Breach Digest: Perspective is Reality	Verizon	April 26, 2017	In the Data Breach Digest, we share most interesting cases—anonymized you can learn from the lessons of oth cybercrime case studies cover the mo prevalent threats you face—from part sophisticated malware. We set out th can take to better defend your organi respond quickly if you are a victim of pages)
Data Breach Investigative Report (registration required)	Verizon	April 27, 2017	The latest report examined 42,068 in 1,935 breaches from 84 countries, dr collective data of 65 organizations. C accounts for 21% of breaches, still fa 73% hat are financially motivated. Bre heavily concentrated in three sectors health care, and public sector. (76 pa
2017 Internet Security Threat Report (registration required)	Symantec	April 26, 2017	Cyberattackers are seeking bigger fir targeting massive dollar amounts, an tripling their asking price via ransomw to 2016. In 2015, ransomware deman $294, but that jumped to $1,077 in 20 probable cause is that victims are pay 34% paid the ransom, and in the Unit did. (77 pages)
The Cyber-Value Connection: Revealing the link between cyber vulnerability	CGI/Oxford Economics	April 2017	The report looks at the reduction in c that arises from a cyber breach, vivid how a severe incident leads to a decl price. To ensure rigor and independe commissioned Oxford Economics to c econometric model using a "differenc

			technique to isolate the damage caus value by a cyber breach from other m market.(28 pages)
Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud	GAO	March 30, 2017	GAO was asked to examine issues re theft services and their usefulness. T examines, among other objectives, (1 benefits and limitations of identity the (2) factors that affect government anc decisionmaking about them. GAO rev studies, laws, regulations, and federa contracts, and interviewed federal ag consumer groups, industry stakehold providers selected because they wer participants. (70 pages)
Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits	RAND	March 13, 2017	This report provides findings from rea vulnerability and exploit data that cou conventional proxy examples and exp complement current efforts to create deciding whether to disclose or retain zero-day vulnerabilities and exploits, policy debates regarding stockpiling a disclosure, and add extra context for the implications and resulting liability data breaches for U.S. consumers, co insurers, and for the civil justice syste pages)
IBM X-Force Threat Intelligence Index 2017: The Year of the Mega-Breach	IBM	March 2017	In 2016, more than 4 billion records w worldwide, exceeding the combined t two previous years, according to a re Security. The leaked documents com credit cards, passwords, and persona information, but the report also notes cybercriminal strategies, finding a nu significant breaches were related to u data such as email archives, busines intellectual property, and source code
The Web of Vulnerabilities: Hunters, Hackers, Spies, and Criminals	*Christian Science Monitor's* Passcode team and Northwestern University's Medill School of Journalism	February 10, 2017	In a joint multimedia project between *Science Monitor's* Passcode team an University's Medill School of Journalis the growing arms race to discover so vulnerabilities and what it means for r and everyone's digital privacy and sa
2017 Identity Fraud: Securing the Connected Life (press release)	Javelin Strategy & Research	February 2017	The study revealed that the number c victims increased by 16% (rising to 1 consumers) in the last year, a record Javelin Strategy & Research began tr fraud in 2003. The study found that d of the industry, fraudsters successfull two million more victims this year wit fraudsters took rising by nearly $1 bill billion. (6 pages)
In 2017, The Insider Threat Epidemic Begins	Institute for Critical Infrastructure Technology	February 2017	The report offers a comprehensive ar Insider Threat Epidemic, including re Characterizing Insider Threats (the in cyber "kill chain," non-malicious insid malicious insider threats) (2) The Insi Debate (3) Policies, Procedures, and Combat Insider Threats (4) Non-Tech (5) Technical Controls. (52 pages)
Risk and Anxiety: A Theory of Data Breach Harms	Texas Law Review	December 14, 2016	The essay examines why courts have dealing with harms caused by data b difficulty largely stems from the fact th

			harms are intangible, risk-oriented, ar report explores how existing legal fou support the recognition of such harm. how courts can assess risk and anxie and coherent way.
Verisign Distributed Denial of Service Trends Report	Verisign	December 2016	Provides a view into attack statistics a trends during the third quarter of 201 attacks peaked over 1 Gbps' 82% inc size year over year; 59% of attacks u attack types. (12 pages)
Department Releases Intake and Charging Policy for Computer Crime Matters	Department of Justice	October 25, 2016	In the course of litigation, DOJ releas under which it chooses whether to bri under the Computer Fraud and Abus forth in the memorandum, prosecutor a number of factors to ensure that ch brought only in cases that serve a su interest.
Data Breach Response: A Guide for Businesses	Federal Trade Commission (FTC)	October 25, 2016	The guidance document provides a b help identify the general legal covera types of data and point businesses to legal standards. It also includes a mo for individuals whose Social Security have been breached. (16 pages)
IoT Devices as Proxies for Cybercrime	Krebs on Security	October 13, 2016	The post looks at how crooks are usi devices as proxies to hide their true l they engage in a variety of other type cybercriminal activity—from frequenti forums to credit card and tax refund f
Examining the Costs and Causes of Cyber Incidents	RAND	October 10, 2016	Researchers found that the typical co was about $200,000 and that most cy companies less than 0.4% of their an The $200,000 cost was roughly equiv typical company's annual information (15 pages)
From the Trenches: Current Status of Security and Risk in the Financial Sector	SANS Institute	October 6, 2016	According to a recent SANS survey, s financial services firms report ransom attack threat, followed by phishing (5 previously held the top spot. More tha financial firms say they've lost anywh $100,000 to $500,000 due to ransom
2016 Internet Organised Crime Threat Assessment (IOCTA)	Europol	September 28, 2016	The IOCTA reports a continuing and i acceleration of the security trends ob previous assessments. The additiona volume, scope, and financial damage the asymmetric risk that characterize has reached such a level that in som cybercrime may have surpassed trad terms of reporting. (72 pages)
The Rising Face of Cyber Crime: Ransomware	BitSight	September 21, 2016	Ransomware attacks on government around the world have tripled in the p Government entities are second mos targeted by ransomware attacks, follo education sector. About 4% of goverr had been exposed to Nymaim, and 3 ransomware strains. Of all industries, had the second lowest security rating ransomware attack rate. (11 pages)
Ransomware Victims Urged to Report Infections to Federal Law Enforcement	FBI	September 15, 2016	The FBI is requesting victims reach o FBI office or file a complaint with the Complaint Center, at http://www.IC3.

			ransomware infection details (as deta website).
Workshop on Data Breach Aftermath and Recovery for Individuals and Institutions	National Academies Press	September 2016	In January 2016, the National Acader Sciences, Engineering, and Medicine Workshop on Data Breach Aftermath for Individuals and Institutions. Partici existing technical and policy remedia discussed possible new mechanisms protecting and helping consumers in breach. Speakers were asked to focu breach aftermath and recovery and to to remediate harms from breaches. T summarizes the presentations and di the workshop. (67 pages)
Examining the costs and causes of cyber incidents	Journal of Cybersecurity	August 25, 2016	Researchers examined a sample of r 000 cyber events that include data br incidents, privacy violations, and phis The findings suggest that public conc the increasing rates of breaches and may be excessive compared with the modest financial impact to firms that s events. Specifically, they found that th typical cyber incident is less than $20 the same as the firm's annual IT secu which represents only 0.4% of a firm's annual revenues. (15 pages)
Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications	New America	July 28, 2016	The report offers five initial policy reco to ensure that more vulnerabilities are and patched sooner: (1) The U.S. gov minimize its participation in the vulner because it is the largest buyer in a ma discourages researchers from disclos vulnerabilities to be patched; (2) The government should establish strong, procedures for government disclosure vulnerabilities it buys or discovers, wi presumption toward disclosure; (3) C establish clear rules of the road for go hacking to better protect cybersecurit liberties; (4) Government and industry bug bounty programs as an alternativ vulnerabilities market and investigate ways to foster the disclosure and pro vulnerabilities; and (5) Congress shou computer crime and copyright laws, a should modify their application of suc the legal chill on legitimate security re pages)
Second Interim Status Report on the U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project – Major IT Business Case	OPM	May 18, 2016	The report finds that funding for the tr security upgrades project remains an because of the agency's poor plannir general finds the agency still lacks a for the massive upgrade. (12 pages)
Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information	RAND Corp.	April 20, 2016	Key findings include (1) 26% of respo estimated 64 million U.S. adults, reca notification in the past 12 months; (2) notified were already aware of the bre respondents accepted offers of free c (4) only 11% of respondents stopped affected company following a breach; respondents reported no costs of the inconvenience it garnered, while, amo reporting some cost, the median cost

			(6) 77% of respondents were highly s company's post-breach response.
2016 Internet Security Threat Report | Government	Symantec	April 13, 2016	Public-sector data breaches exposed identities in 2015, but hackers were r only one-third of those compromises, new research. Negligence was behin thirds of the exposed identities throug agencies. In total, the report suggests identities were compromised acciden with 6 million by hackers.
Combatting the Ransomware Blitzkrieg: The Only Defense is a Layered Defense, Layer One: Endpoint Security	The Institute for Critical Infrastructure Technology	April 2016	The report introduces the ins and out prevalent ransomware variants as we endpoints vulnerable to ransomware SCADA/ICS, IoT, cars, cloud, servers hardware, personal computers, and t exploitable vulnerability, the human. (
2016 Data Breach Investigations Report	Verizon	April 2016	Provides analysis and statistics on w breaches. "In 93% of cases, it took at or less to compromise systems. Orga meanwhile, took weeks or more to di breach had even occurred—and it wa customers or law enforcement that s alarm, not their own security measure
A Look Inside Cybercriminal Call Centers	Krebs on Security	January 11, 2016	Crooks who make a living via identity dating scams, and other con games c trouble when presented with a phone challenge that requires them to demo of a language they do not speak fluer criminal call center, which allows sca outsource those calls to multilingual r who can be hired to close the deal.
Target Settlement Memorandum	U.S. District Court, District of Minnesota	December 2, 2015	Target Corporation has agreed to pay institutions almost $40 million to settl suit related to its massive 2013 data l proposed settlement of up to $39,357 apply to all U.S. financial institutions t payment cards put at risk as a result breach. (20 pages)
The Cyberwar is On (Special Issue)	*The Agenda* (Politico)	December 2015	The cyber issue of *The Agenda* maga include "Why Politicians can't Handle the NSA's Hunt for Hackers," "Americ Arsenal," " The Biggest Hacks (We K "Survey: What Keeps America's Com Up at Night?," The 'Electronic Pearl H Best Frenemy, Time for a Ralph Nade "The Crypto Warrior," and "America's
Fiscal Year 2015 Top Management Challenges	Office of Personnel Management (OPM), Office of Inspector General (OIG)	October 30, 2015	See Internal Challenges section (pp. discussion of challenges related to in technology, improper payments, the r process, and the procurement proces OPM's Office of Procurement Operat Federal Acquisition Regulation and th policies in awarding a $20.7 million c provide credit monitoring and ID theft Investigators turned up "significant de the process of awarding the contract Group and its subcontractor CSID. (2
With Stolen Cards, Fraudsters Shop to Drop	Krebs on Security	September 28, 2015	Fraudsters have perfected the reship criminal enterprise that allows card th service operators to essentially split t

			merchandise ordered with stolen cred cards.
Drops for Stuff: An Analysis of Reshipping Mule Scams	Federal Bureau of Investigation (FBI), University of CA Santa Barbara, Stony Brook University, Krebs on Security, University College London	September 23, 2015	In reshipping scams, cybercriminals p value or high-demand products from merchants using stolen payment instr then ship the items to a credulous citi person, who has been recruited by th under the guise of "work-from-home" then forwards the received products t cybercriminals, most of whom are loc Once the goods reach the cybercrimi then resold on the black market for a pages)
Follow the Data: Dissecting Data Breaches and Debunking Myths	Trend Micro	September 22, 2015	Trend Micro's Forward-Looking Threa (FTR) Team has taken 10 years (200 information on data breaches in the U from the Privacy Rights Clearinghous subjected it to detailed analysis to be the real story behind data breaches a (51 pages)
Timeline: Government Data Breaches	Government Executive	July 6, 2015	The timelines are based mainly on te OPM Director Catherine Archuleta ar assistant secretary for Cybersecurity Communications at DHS, supplemen information from news reports.
2015 Cost of Data Breach Study: Global Analysis	Ponemon Institute and IBM	May 27, 2015	The average cost of a breach was up 2014, with U.S. firms paying almost $ than the global average. In the Unitec breach costs organizations on averag (the highest of the 10 nations analyze million in 2013. Globally, the cost of a 15% this year to $3.5 million. The Un likewise had the highest cost per reco $201, up from $188 last year. The co terms of size of breaches recorded: U averaged 29,087 records compromise (Free registration required to downloa
Meet 'Tox': Ransomware for the Rest of Us	McAfee Labs	May 23, 2015	The packaging of malware and malwa kits for cybercrime "consumers" has b running trend. Various turnkey kits tha access plus botnet plus stealth functi anywhere. Ransomware, though very not yet appeared in force in easy-to-c However, Tox is now available free.
2014 Internet Crime Report	Internet Crime Complaint Center (IC3)	May 19, 2015	IC3, a joint project of the National Wh Center and the FBI, received 269,422 year consisting of a wide array of sca victims across all demographic group victims of Internet crimes in the Unite more than $800 million. On average, 22,000 complaints were received eac pages)
Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data	Ponemon Institute	May 2015	A rise in cyberattacks against doctors costing the U.S. health-care system $ as organized criminals who once targ and financial firms increasingly go aft records. Criminal attacks are up 125% five years ago lost laptops was the le The study also found most organizati unprepared to address new threats a adequate resources to protect patien

Best Practices for Victim Response and Reporting of Cyber Incidents	Department of Justice (DOJ)	April 29, 2015	DOJ issued new guidance for busine practices for handling cyber incidents is broken down into what companies should not do—before, during, and a The recommendations include devel response plan, testing it, identifying h data and risk management priorities, with law enforcement and response f (15 pages)
2014 Global Threat Intel Report	CrowdStrike	February 6, 2015	The report summarizes CrowdStrike's scrutiny of more than 50 groups of cy actors, including 29 different state-sp nationalist adversaries. Key findings financial malware changed the threat point of sale malware became increa The report also profiles a number of sophisticated adversaries from China (Free registration required.)
Unique in the Shopping Mall: on the Reidentifiability of Credit Card Metadata	*Science Magazine*	January 30, 2015	Massachusetts Institute of Technolog scientists showed they can identify a more than 90% accuracy by looking a purchases; three if the price is includ after companies "*anonymized*" the tra records, saying they wiped away nam personal details. (5 pages)
Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Threat	FBI	January 20, 2015	Ransomware scams involve a type o infects computers and restricts users files or threatens the permanent dest information unless a ransom—anywh hundreds to thousands of dollars—is offers information on the FBI's and fe international, and private-sector partn steps to neutralize some of the more ransomware scams through law enfo against major botnets.
Exploit This: Evaluating the Exploit Skills of Malware Groups	Sophos Labs Hungary	January 2015	Researchers evaluated the malware persistent threat (APT) campaigns of that all leveraged a particular exploit- attack against a specific version of M The report found that none of the gro modify the attack enough to infect oth Office, even though several versions theoretically vulnerable to the same t Despite the aura of skill and complex surround APTs, they are much less s than they are given credit for. (26 pag
The Cost of Malware Containment	Ponemon Institute	January 2015	A survey of more than 600 U.S. IT se practitioners found that in a typical w organizations receive an average of malware alerts; only 19% are deeme worthy of action. Compounding the p respondents believe their prevention of malware infections in a typical wee registration required.)
Addressing the Cybersecurity Malicious Insider Threat	Schluderberg, Larry (Utica College Master's Thesis)	January 2015	"The purpose of this research was to constitutes Malicious Insider (MI) thr how they initiate attacks, the extent t activity can be modeled or predicted, risk mitigation strategies. The results addressing the Malicious Insider thre than just a technical issue. Dealing e the threat involves managing the dyn between employees, their work envir

			work associates, the systems with wh interact, and organizational policies a (80 pages)
The Underground Hacker Markets are Booming with Counterfeit Documents, Premiere Credit Cards, Hacker Tutorials, and 1000% Satisfaction Guarantees	Dell Secure Works	December 2014	Researchers examined dozens of und hacker markets and found that busine Prices have gone down for many iten offerings have expanded. According t "Underground hackers are monetizing data they can steal or buy and are co services so other scammers can succ out online and in-person fraud." (16 p
What Happens When You Swipe Your Card?	*60 Minutes*	November 30, 2014	From the script for the segment "Swip "Sophisticated cyberthieves steal you information. Common criminals buy it shopping sprees—racking up billions fraudulent purchases. The cost of the calculated into the price of every item computer crooks swipe your card nur up paying the price. 2014 is becomin 'year of the data breach.'"
Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation	Heritage Foundation	October 27, 2014	A list of federal government cybersec and failures, most of which occurred 2014. The list is part of a continuing s by Heritage that serves as a long-terr open-source data about federal cyber breaches dating back to 2004.
2014 Cost of Cybercrime Global Report	Hewlett-Packard Enterprise Security and the Ponemon Institute	October 8, 2014	This 2014 global study of U.S.-based which spanned seven nations, found course of a year, the average cost of climbed by more than 9% to $12.7 mi companies in the United States, up fr in the 2013 study. The average time t cyberattack is also rising, climbing to days in 2013. (30 pages) (Email regis required.)
The Deep Web (Special Issue)	*The Kernel*	September 28, 2014	A special issue devoted to the Deep Road, black markets, etc.
How Consumers Foot the Bill for Data Breaches (infographic)	NextGov.com	August 7, 2014	More than 600 data breaches occurre alone, with an average organizationa than $5 million. But in the end, it is th who are often picking up the tab, fron costs to credit card reissue fees.
Is Ransomware Poised for Growth?	Symantec	July 14, 2014	Ransomware usually masquerades a "wheel clamp" for the victim's comput pretending to be from the local law er might suggest the victim had been us computer for illicit purposes and clain his or her computer the victim would fine—often between $100 and $500. Ransomware escalated in 2013, with (sixfold) increase in attacks between end of the year.
iDATA: Improving Defences Against Targeted Attack	Centre for the Protection of National Infrastructure (UK)	July 2014	The iDATA program consists of a nun aimed at addressing threats posed by and state-sponsored actors. iDATA ha several outputs for the cybersecurity document provides a description of th program and a summary of the repor
Cyber Risks: The Growing Threat	Insurance Information Institute	June 27, 2014	Although cyber risks and cybersecuri acknowledged to be serious threats, companies today still do not purchase

			insurance. Insurers have developed s insurance policies to help businesses protect themselves from the cyber thr intelligence suggests that the types o cyber coverage being offered by insu expanding in response to this fast-gro need. (27 pages)
Hackers Wanted: An Examination of the Cybersecurity Labor Market	RAND Corporation	June 24, 2014	RAND examined the current status o market for cybersecurity professional emphasis on their being employed to United States. This effort was in thre review of the literature; second, inter managers and educators of cybersec professionals, supplemented by repo an examination of the economic litera markets. RAND also disaggregated t definition of *cybersecurity professiona* skills differentiation as relevant to this pages)
Big Data and Innovation, Setting The Record Straight: De-identification Does Work	Information Technology and Innovation Foundation and the Information and Privacy Commissioner, Ontario, Canada	June 16, 2014	The paper examines a select group c are often referenced in support of the identified data sets are at risk of re-id individuals through linkages with othe It examines the ways in which the aca referenced has been misconstrued a primary reason for the popularity of th misconceptions is not factual inaccura within the literature but rather a tende of commentators to overstate or exag of re-identification. (13 pages)
Net Losses: Estimating the Global Cost of Cybercrime	Center for Strategic and International Studies and McAfee	June 2014	The report explores the economic im cybercrime, including estimation, regi IP theft, opportunity and recovery cos future of cybercrime. (24 pages)
2014 U.S. State of Cybercrime Survey	Pricewaterhouse Coopers, *CSO Magazine*, the CERT Division of the Software Engineering Institute at Carnegie Mellon University, and the U.S. Secret Service	May 29, 2014	The cybersecurity programs of U.S. c not rival the persistence, tactical skill technological prowess of their potent adversaries. This year, three out of fo respondents to the survey had detect event in the past 12 months, and mo (34%) said the number of security inc had increased over the previous year
Privileged User Abuse and The Insider Threat	Ponemon Institute and Raytheon	May 21, 2014	The report looks at what companies a and the vulnerabilities that need to be policies and technologies. One proble the difficulty in actually knowing if an an insider is truly a threat. Sixty-nine respondents say they do not have en information from security tools to mak assessment, and 56% say security to many false positives. (32 pages) (Re registration to access.)
Online Advertising and Hidden Hazards to Consumer Security and Data Privacy	Senate Permanent Subcommittee on Investigations	May 15, 2014	The report found consumers could ex themselves to malware just by visitin website. It noted that the complexity made it possible for both advertisers websites to defer responsibility and th safeguards failed to protect against o The report also warned that current p create enough incentives for "online a participants" to take preventive meas

Sharing Cyberthreat Information Under 18 USC §2702(a)(3)	Department of Justice (DOJ)	May 9, 2014	DOJ issued guidance for Internet ser assuage legal concerns about inform The white paper interprets the Stored Communications Act, (18 U.S.C. §27 which prohibits providers from volunta customer information to governmenta white paper says the law does not pr from divulging data in the aggregate, specific details about identifiable cust pages)
The Target Breach, by the Numbers	Krebs on Security	May 6, 2014	A synthesis of numbers associated w data breach of December 19, 2013 (e records stolen, estimated dollar cost and community banks, and the amou Target estimates it will spend upgradi terminals to support Chip-and-PIN en
The Rising Strategic Risks of Cyberattacks	McKinsey and Company	May 2014	The authors suggest that companies with their capabilities in cyber risk ma highly visible breaches occur with inc regularity, most technology executive are losing ground to attackers. Organ and small lack the facts to make effe and traditional "protect the perimeter" strategies are proving insufficient.
Big Data: Seizing Opportunities, Preserving Values	White House	May 2014	Findings include a set of consumer p recommendations, such as national d legislation, and a fresh call for baseli privacy legislation first recommended pages)
Russian Underground Revisited	Trend Micro	April 28, 2014	The price of malicious software—des online bank fraud, identity theft, and d cybercrimes—is falling dramatically i Russian-language criminal markets i Falling prices are a result not of decli rather of an increasingly sophisticate The report outlines the products and sold and their prices. (25 pages)
Federal Agencies Need to Enhance Responses to Data Breaches	Government Accountability Office (GAO)	April 2, 2014	Major federal agencies continue to fa fully implementing all components of information security programs, which securing agency systems and the info contain—including personally identifia (PII). (19 pages)
A "Kill Chain" Analysis of the 2013 Target Data Breach	Senate Commerce Committee	March 26, 2014	The report analyzes what has been r about the Target data breach, using t *chain* framework, an analytical tool in Lockheed Martin security researchers widely used today by information sec professionals in both the public and p The analysis suggests that Target mi of opportunities along the kill chain to attackers and prevent the massive da pages)
Markets for Cybercrime Tools and Stolen Data	RAND Corporation National Security Research Division and Juniper Networks	March 25, 2014	The report, part of a multiphase study security environment, describes the f characteristics of the criminal activitie markets and how they have grown in state to explain how their existence c information security environment. (83
Merchant and Financial Trade Associations Announce Cybersecurity	Retail Industry Leaders Association	February 13, 2014	Trade associations representing the r financial services industries announc

Partnership			cybersecurity partnership. The partne on exploring paths to increased inforr better card security technology, and r trust of customers. Discussion regard partnership was initiated by the Retai Leaders Association and the Financia Roundtable.
FTC Statement Marking the FTC's 50th Data Security Settlement	Federal Trade Commission (FTC)	January 31, 2014	The FTC announced its 50th data sec What started in 2002 with a single ca established FTC Act precedent to the security has grown into an enforceme has helped to increase consumer pro encouraged companies to make safe consumer data a priority. (2 pages)
Worst Practices Guide to Insider Threats: Lessons from Past Mistakes	American Academy of Arts and Sciences	January 2014	The report presents a *worst practices* serious past mistakes regarding insid Although each situation is unique, an problems are relatively rare, the incid issues that exist in many contexts an security manager should consider. Co organizational practices—such as pri production over security, failure to sh across subunits, inadequate rules or waiving of rules, exaggerated faith in and excessive focus on external threa seen in many past failures to protect threats. (32 pages)
ENISA Threat Landscape 2013—Overview of Current and Emerging Cyber-Threats	European Union Agency for Network and Information Security (ENISA)	December 11, 2013	The report is a comprehensive compi 15 cyber threats assessed in the 201 period. ENISA has collected more tha regarding cyber threats, risks, and thr pages)
Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent	GAO	December 9, 2013	GAO recommends that "to improve th and effectiveness of government wide response programs, the Director of C update its guidance on federal agenc to a PII-related data breach to include on notifying affected individuals base determination of the level of risk; (2) d determining whether to offer assistan credit monitoring to affected individua revised reporting requirements for PII breaches to US-CERT [Computer Em Response Team], including time fram reflect the needs of individual agencie government as a whole and consolida incidents that pose limited risk." (67 p
Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences	Brookings Institution	December 2013	Economic espionage has existed at le industrial revolution, but the scope of enabled competitive data theft may b unprecedented. The authors present believe is the first economic framewo understand the long-run impact of co theft on an economy by taking into ac mechanisms and pathways by which victims. (18 pages)
Illicit Cyber Activity Involving Fraud	Carnegie Mellon University Software Engineering Institute	August 8, 2013	Technical and behavioral patterns we from 80 fraud cases—67 insider and that occurred between 2005 and the cases were used to develop insights indicators to help private industry, gov law enforcement more effectively pre detect, investigate, and manage mali

			activity within the banking and financ pages)
The Economic Impact of Cybercrime and Cyber Espionage	Center for Strategic and International Studies (CSIS)	July 22, 2013	According to CSIS, losses to the Unit country in which data is most accessi $100 billion annually. The cost of cyb cyber espionage to the global econor multiple of this, likely measured in hu billions of dollars. (20 pages)
Cyber-Crime, Securities Markets, and Systemic Risk	World Federation of Exchanges and the International Organization of Securities Commissions	July 16, 2013	The report explores the nature and ex cybercrime in securities markets and systemic risk aspects of this threat. It results of a survey to the world's exch experiences with cybercrime, cyberse and perceptions of the risk. (59 pages
Remaking American Security: Supply Chain Vulnerabilities and National Security Risks Across the U.S. Defense Industrial Base	Alliance for American Manufacturing	May 2013	Reportedly because the supply chain makes sense for U.S. officials to coop nations to ward off cyberattacks. Incr international cooperation to secure th global IT system is a valuable long-te (355 pages)
Comprehensive Study on Cybercrime	United Nations Office on Drugs and Crime	February 2013	The study examined the problem of c the perspective of governments, the p academia, and international organiza its results in eight chapters, covering connectivity and cybercrime; (2) the g cybercrime picture; (3) cybercrime leg frameworks; (4) criminalization of cyb enforcement and cybercrime investig electronic evidence and criminal justi international cooperation in criminal r cybercrime; and (8) cybercrime preve pages)
Does Cybercrime Really Cost $1 Trillion?	ProPublica	August 1, 2012	In a news release to announce its 20 *Unsecured Economies: Protecting Vi* computer security firm McAfee estima global cost for cybercrime. The numb appear in the report itself. This estima even by the three independent resea Purdue University whom McAfee cred analyzing the raw data from which th derived. An examination by ProPublic new grounds to question the data and to generate these numbers, which Mc Symantec say they stand behind.
Proactive Policy Measures by Internet Service Providers against Botnets	Organization for Economic Co-operation and Development (OECD)	May 7, 2012	The report analyzes initiatives in a nu countries through which end-users ar Internet service providers (ISPs) whe computers are identified as being cor malicious software and encouraged t mitigate the problem. (25 pages)
Developing State Solutions to Business Identity Theft: Assistance, Prevention and Detection Efforts by Secretary of State Offices	National Association of Secretaries of State (NASS)	January 2012	The white paper is the result of efforts member NASS Business Identity The develop policy guidelines and recomr state leaders dealing with identity frau involving public business records. (23
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines	SANS Institute	October 3, 2011	The 20 security measures are intend agencies' limited resources on pluggi common attack vectors. (77 pages)
Revealed: Operation Shady RAT: an Investigation Of Targeted Intrusions Into 70+ Global Companies, Governments,	McAfee	August 2, 2011	A cyber-espionage operation lasting penetrated 72 government and other most of them in the United States, an

and Non-Profit Organizations During the Last 5 Years			everything from military secrets to inc according to technology security com (See page 4 for the types of compron page 5 for the geographic distribution country of origin, pages 7-9 for the ty and pages 10-13 for the number of in 2007-2010). (14 pages)
The Role of Internet Service Providers in Botnet Mitigation: an Empirical Analysis Based on Spam Data	Organisation for Economic Co-operation and Development (OECD)	November 12, 2010	The working paper considers whethe critical control points for botnet mitiga number of infected machines varies a why. (31 pages)
Untangling Attribution: Moving to Accountability in Cyberspace (Testimony)	Council on Foreign Relations	July 15, 2010	Robert K. Knake's testimony before tl Committee on Science and Technolo attack attribution in preventing cybera attribution technologies can affect the privacy of Internet users. (14 pages)
Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities	National Research Council	2009	The report explores important charac cyberattacks. It describes the current and domestic legal structure as it mig cyberattacks and considers analogies domains of conflict to develop relevar pages)

Source: Highlights compiled by CRS from the reports.

Notes: Page counts are for documents; other cited resources are webpages.

Table 2. National Security, Cyber Espionage, and Cyberwar

(includes Stuxnet, Dark Web/Darknet)

Title	Source	Date	Notes
Cybersecurity Legislation	International Telecommunications Union	Continuously Updated	An integral and challenging co national cybersecurity strategy of regionally and internationally appropriate legislation against information and communicatio (ICTs) for criminal or other purp
Cyberthreat: Real-Time Map	Kaspersky Labs	Continuously Updated	Kaspersky Labs has launched cyber threat map that lets view cybersecurity incidents as they the world in real time. The inte includes malicious objects dete access and on-demand scans, antivirus detections, and objec vulnerability and intrusion dete subsystems.
Cyberwarfare	RAND	Continuously Updated	Explore RAND reports on cybe product type (research, blog, n event, etc.) or author. Featurec the top of the page.
Too Connected To Fail: How Attackers Can Disrupt the Global Internet, Why It Matters, And What We Can Do About It	Belfer Center for Science and International Affairs (Harvard)	May 2017	This paper examines attacks o infrastructure through a lens of and nation state conflict. Most focused on the ability of non-st these tools to exact ransom or mischief. While these are real examination of these attacks' a nation state conflict has been r pages)

Cyber Compellence: Applying Coercion in the Information Age	Marine Corps University and Northeastern University, presented at the Annual International Studies Association Meeting, Baltimore, Maryland	April 25, 2017	The paper reviews how state a cyber instruments to coerce ac between 2000 to 2014 differen cyber disruption, espionage, ar Cyber disruption and espionag to achieve their goals of gather and signaling through harassm result in an observable behavic the target in the near-term. On occasion, usually associated w cyberspace, does cyber coerci form of degradation, result in c idea of quick victory in the cybe remains elusive. (27 pages)
Bad Bots: The Weaponization of Social Media	College of William and Mary; Project on International Peace and Security	April 2017	In the next several years, hosti state actors will accelerate thei media bots to undermine demc terrorists, disrupt markets, and source intelligence collection. T conducts an alternative futures order to help policymakers ider mitigate the threats of social m worst-case and most-likely sce technological stalemate betwe detection leads to a false sens in social media information, wh breakthroughs in bot technolog disruptions until bot-detection t advances. (23 pages)
Strategic Aspects of Cyberattack, Attribution, and Blame	Proceedings of the National Academy of Sciences	March 14, 2017	Attribution of cyberattacks has technical components. A forma incorporates both elements anc conditions under which it is rati an attack and when it is better publicly. The model applies to a conflicts and provides guidanc policymakers about which para estimated to make a sound dec attribution and blame. It also d surprising conclusions about th asymmetric technical attributio (12 pages)
Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits	RAND	March 13, 2017	The report provides findings fro zero-day vulnerability and expl could augment conventional pr and expert opinion, complemer to create a framework for decic disclose or retain a cache of ze vulnerabilities and exploits, info policy debates regarding stock vulnerability disclosure, and ac for those examining the implica resulting liability of attacks and for U.S. consumers, companie for the civil justice system broa
Snapshot: Turning Back DDoS Attacks	DHS Science and Technology, Homeland Security Advanced Research Projects Agency's Cyber Security Division (CSD)	February 16, 2017	CSD's Distributed Denial of Se (DDoSD) project is spearheadi pronged approach to shift the a network infrastructure defende two primary focuses are on inc deployment of best practices to scale growth and defending ne one Tbps attack through devel collaboration tools that can be

			medium-size organizations. A t project addresses other types o service attacks, such as those Next Generation 911 emergenc systems.
Task Force on Cyber Deterrence	Defense Science Board	February 2017	The U.S. military lacks the cybe defend against potential attack financial systems, telecommun systems, and other elements o infrastructure launched by Rus Furthermore, the U.S. military's IT makes it vulnerable to attack diminish its capabilities to resp attacks. The task force recomm Pentagon develop a second-st that is cyber-resilient. (44 page
The Enemy Has a Voice: Understanding Threats to Inform Smart Investment in Cyber Defense	New America	February 2017	The report discusses the gene cyber threat intelligence (CTI) a powerful concept can reduce "o dominant" nature of cybersecu various types of such informati outlines challenges with cyber intelligence going forward and ideas that can help lead to imp such information across a varie organizations. (16 pages)
Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Threat Preparedness	MITRE Corp.	February 2017	Cyber Prep 2.0 focuses on adv and corresponding elements o strategy and includes material conventional cyber threats. Cy be used in standalone fashion, used to complement and exten other, more detailed framework [National Institute of Standards Technology] Cybersecurity Fra threat models.
The U.S. Government and Zero-Day Vulnerabilities: from Pre-Heartbleed to Shadow Brokers	Columbia Univ. Journal of International Affairs	November 2016	Government agencies currently days they discover to an intera Vulnerability Equities Process N National Security Council. The examines questions such as ho criminals and foreign adversari discover the vulnerability and h damage they could do if they d balancing that with what value might provide to U.S. intelligen pages)
Department Releases Intake and Charging Policy for Computer Crime Matters	Department of Justice	October 25, 2016	"In the course of recent litigatio department yesterday shared t which we choose whether to br under the Computer Fraud and set forth in the memorandum, p consider a number of factors in that charges are brought only i serve a substantial federal inte
Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats (Project Report)	GWU Center for Cyber & Homeland Security	October 2016	The report places the current c larger strategic context and the role of private-sector active def addressing such threats. With t report proposes a framework th most prevalent active defense places them along a spectrum and impact, indicating where c

			with the government becomes responsible private action. (86
Brief History of Law Enforcement Hacking in the United States	New America Foundation	September 2016	Understanding the history of go hacking is important in order to people in the ongoing policy di paper focuses on a selection o historical cases, with the under due to the secret nature of gov investigations, only a fraction c that has taken place is known. highlights major trends in inves and will hopefully foster more i these practices by policymaker (20 pages)
Predicting Cyber Attacks: A Study of the Successes and Failures of the Intelligence Community	Small Wars Journal	July 7, 2016	The article focuses on identifyi successes and failures of analy Intelligence Community (IC) to cyberattacks against the Unite research goal is to break down of a good cyber defensive forc to clearly identify those failures and their effects on the operati IC in cyberspace. (11 pages)
Tech for Jihad: Dissecting Jihadist's Digital Toolbox	Flashpoint	July 2016	The report attempts to catalog noteworthy digital tools in comr jihadists, and when they starte (13 pages)
Cyber Conflict: Prevention, Stability and Control	Carnegie Cyber Policy Initiative	July 2016	Only a few years ago, there we norms globally accepted by go cybersecurity or cyber conflict. States, which had long pushed had publicly announced very fe States and a few other allies co laws of armed conflict (otherwi International Humanitarian Lav Convention") applied to cybers this has changed with tremend much so that 2015 was called Global Cyber Norms. (10 page
Combatting the Ransomware Blitzkrieg: The Only Defense is a Layered Defense, Layer One: Endpoint Security	The Institute for Critical Infrastructure Technology	April, 2016	The brief contains an analysis endpoint security; vulnerable e personal computers, servers, r specialize hardware, and clouc potentially vulnerable endpoint IoT devices, cars); endpoint se selecting an endpoint security pages)
Know Your Enemies 2.0: The Encyclopedia of the Most Prominent Hactivists, Nation State, and Mercenary Hackers	*Information for Critical Infrastructure Technologies (ICIT)*	February 2016	The report covers threat group particular ranking system, but l players categorized by geograp malware, tool kits, exploit techr foot prints, and targets are cov encyclopedia. (81 pages)
Operationalizing Cybersecurity Due Diligence: A Transatlantic Comparative Case Study	*South Carolina Law Review*	January 12, 2016	"Although much work has beer applying the law of warfare to c less attention has been paid to cyber peace applicable below t threshold. Among the most imp unanswered questions is what due diligence obligations are to and to the private sector, as we obligations should be translate

			this article, we analyze how bo States and the European Unio operationalizing the concept of due diligence, and then move a menu of options presented to Parliament in November 2015 further refine and apply this co pages)
ISIS's OPSEC Manual Reveals How It Handles Cybersecurity	*Wired*	November 19, 2015	From the article, "So what exa attackers doing for OPSEC? It has a 34-page guide to operat which offers some clues. [R]es the Combating Terrorism Cent Point's military academy uncov and other related documents fr and chat rooms."
2015 Annual Report to Congress	U.S.-China Economic Commission	November 17, 2015	Reportedly China causes incre the U.S. economy and security deliberate policies targeting the (1) coordinated, government-b information from a wide variety commercial enterprises and (2 restrictions on content, standa commercial opportunities for U Hackers working for the Chine or with the government's supp encouragement—have infiltrat networks of U.S. government a contractors, and private comp personal information and trade Chapter 1, Section 4: Comme Espionage and Barriers to Dig China.) (631 pages)
Cyber Defense: An International View	U.S. Army War College Strategic Studies Institute	September 2015	The paper provides an overvie different national approaches t those of Norway, Estonia, Ger Sweden. It also provides a gui with the relevant governmental organizations in each of these compares and contrasts the ad drawbacks of each national ap pages)
Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box	Woodrow Wilson International Center for Scholars	August 1, 2015	"This policy brief outlines what and Darknet are, how they are why we should care about the policymakers, the continuing g Deep Web in general and the a expansion of the Darknet in pa new policy challenges. The res challenges may have profound civil liberties, national security, economy." (20 pages)
Cyber-Enabled Economic Warfare: An Evolving Challenge	Hudson Institute	August 2015	This monograph is divided into one dissecting the U.S.'s use o economic warfare; two providi cyber-enabled economic warfa to the United States by state a actors; two offering case studi cyber-enabled economic warfa sectors, financial services and infrastructure; and a concludin reviews key takeaways and ne pages)

Russian Underground 2.0	Trend Micro (Forward Looking Threat Team)	July 28, 2015	The Russian underground is a ecosystem that covers all aspe cybercriminal business activitie increasingly professional unde infrastructure for the sale of ma and services. There is increasi professionalization of the crime allows cheaper prices to domir thereby make it easy and very anyone without significant skill is needed to conduct criminal c pages)
Below the Surface: Exploring the Deep Web	Trend Micro	June 22, 2015	The research paper offers a loc duality of the Deep Web—how protect anonymity can be used freely, away from censorship a enforcement, or be used to exp criminal pursuits. It also briefly Deep Web's impact, and offers how it could evolve over the ne pages)
Cybersecurity: Jihadism and the Internet	European Parliament Think Tank	May 18, 2015	"Since the beginning of the cor March 2011, the numbers of Eu supporting or joining the ranks have been growing steadily, ar as high as 4,000 individuals. A the possible avenues for radica multiplying and the risks of dor increasing. The proliferation of messaging online and their reli networks suggest that the Inter increasingly a tool for promotin ideology, collecting funds, and ranks." (2 pages)
APT30 and the Mechanics of a Long-Running Cyber-Espionage Operation: How a Cyber Threat Group Exploited Governments and Commercial Entities Across Southeast Asia and India for Over a Decade	FireEye	April 2015	Reportedly a Chinese governm team has used the same basic spy on Southeast Asian and In for a decade, demonstrating th cyber defenses protecting gove information across broad swatl According to Fireeye, the fact t APT30, has been able to use t set of malware tools against go networks since at least 2005 su targets remained unaware for r decade they were being spied incapable of countering the thr
Worldwide Threat Assessment of the U.S. Intelligence Community	Director of National Intelligence	February 26, 2015	Cybersecurity is the first threat annual review of worldwide thr United States. Despite ever-im defenses, the diverse possibilit hacking intrusions, supply chai insert compromised hardware malevolent activities by human hold nearly all ICT systems at r come. Moreover, the risk calcu some private-sector entities rep adequately account for foreign the systemic interdependencie different critical infrastructure s pages)
The Impact of the Dark Web on Internet Governance and Cyber Security	Global Commission on Internet Governance	February 2015	The Dark Web is a part of the I has been intentionally hidden a

			inaccessible through standard The Deep Web has the potenti increasingly high number of ma and activities. To formulate cor strategies and policies for gove Internet, it is important to consi its farthest reaches—the Deep importantly, the Dark Web. The to provide a broader understan Web and its impact on people's pages)
Attributing Cyber Attacks	Thomas Rid and Ben Buchanan, *Journal of Strategic Studies*	December 23, 2014	The authors introduce the Q M to explain, guide, and improve attribution. Matching an offend is an exercise in minimizing un three levels: (1) tactically, attrib well as a science; (2) operation is a nuanced process, not a bla problem; and (3) strategically, a function of what is at stake poli Successful attribution requires on all levels, careful managem leadership, stress-testing, pruc communication, and recognizir challenges. (36 pages)
Operation Cleaver	Cylance	December 2, 2014	A sophisticated hacking group has probed and infiltrated targe United States and 15 other nat past two years in a series of cy dubbed "Operation Cleaver." T group has evolved faster than a Iranian campaign, according to which calls Iran "the new China concern that the group's survei operations could evolve into so destructive attacks. (86 pages)
Legal Issues Related to Cyber	*NATO Legal Gazette*	December 2014	The *NATO Legal Gazette* conta organized articles usually writte civilian legal personnel working the governments of NATO and Its purpose is to share articles for the large NATO legal comm connect legal professionals of t not a formal NATO document.
The National Intelligence Strategy of the United States of America 2014	Office of the Director of National Intelligence	September 18, 2014	Cyber intelligence is one of fou topical missions" the intelligenc must accomplish. Both state an actors use digital technologies goals, such as fomenting insta achieving economic and militar They do so "often faster than c understand the security implica mitigate potential risks." To bec effective in the cyber arena, the community reportedly must imp correctly attribute attacks. (24 p
Today's Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of the 9/11 Commission Report	The Annenberg Public Policy Center and the Bipartisan Policy Center	July 22, 2014	Members of the panel that stud attacks urge Congress to enac legislation, the White House to the consequences of potential Americans, and leaders to wor define what constitutes an onlin another country. (48 pages)

Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies	Center for a New American Security	July 2014	The report examines existing i technology security weaknesse nine specific recommendations government and others to cope insecurities. (64 pages)
M Trends: Beyond the Breach: 2014 Threat Report	Mandiant	April 2014	Cyber-threat actors are expand computer network exploitation of objectives, from the econom Threat actors are not only inter the corporate "crown jewels" b looking for ways to publicize th physical destruction, and influe decisionmakers. Private organ increasingly become collateral political conflicts. Reportedly w solution in sight, the ability to d respond to attacks has never b important. (28 pages)
Emerging Cyber Threats Report 2014	Georgia Institute of Technology	January 2014	Brief compilation of academic r losing control of cloud data, ins connected devices, attackers a mobile ecosystems, the high c against cyberattacks, and adva information manipulation. (16 p
Cybersecurity and Cyberwar: What Everyone Needs to Know	Brookings Institution	January 2014	Authors Peter W. Singer and A look at cybersecurity issues fac military, government, business individuals and examine what h these entities try to balance se freedom of speech and the ide Internet. (306 pages)
W32.Duqu: The Precursor to the Next Stuxnet	Symantec	November 14, 2013	On October 14, 2011, a resear strong international connection Symantec to a sample that app similar to Stuxnet, the malware havoc in Iran's nuclear centrifu lab named the threat *Duqu* bec files with the file name prefix *D* lab provided Symantec with sa from computer systems located well as a detailed report with in including analysis comparing th to Stuxnet.
To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve	The Langner Group	November 2013	The report summarizes the mo comprehensive research on th malware so far. It combines res reverse engineering the attack intelligence on the design of th and background information on uranium enrichment process. I attack vectors of the two differe contained in the malware and p analysis of the bigger and muc payload that was designed to d centrifuge rotors by overpressu
Strategies for Resolving the Cyber Attribution Challenge	Air University, Maxwell Air Force Base	May 2013	Private-sector reports have pro possible to determine the geog of threat actors to varying degr these assumptions, nation-stat individuals, should be held culp malicious actions and other cyb originate in or transit informatio their borders or that are owned

			registered corporate entities. T on other appealing arguments responsibility in cyberspace. (1
Role of Counterterrorism Law in Shaping 'ad Bellum' Norms for Cyber Warfare	International Law Studies (U.S. Naval War College)	April 1, 2013	"To date there has been little a the possibility that internationa and counterterrorism law in pa should develop a subset of cyb counterterrorism law to respon inevitability of cyberattacks by use of cyber weapons by gove terrorists, and to supplement e international law governing cyb the intrusions do not meet the thresholds." (42 pages)
The Tallinn Manual on the International Law Applicable to Cyber Warfare	Cambridge University Press/ NATO Cooperative Cyber Defence Center of Excellence	March 5, 2013	The Tallinn Manual identifies th law applicable to cyber warfare "black-letter rules" governing s extensive commentary accomp which sets forth the rule's basis customary law, explains how th experts interpreted applicable r cyber context, and outlines any within the group as to the rule's (Note: The manual is not an of publication but rather an expre of a group of independent expe in their personal capacities.) (3
Cyberterrorism: A Survey of Researchers	Swansea University	March 2013	The report provides an overvie from a project designed to cap understandings of cyberterroris research community. The proje June 2012 and November 201 employed a questionnaire that to more than 600 researchers, other experts. A total of 118 res received from individuals worki countries across six continents
National Level Exercise 2012: Quick Look Report	Federal Emergency Management Agency (FEMA)	March 2013	National Level Exercise (NLE) series of exercise events that e ability of the United States to e coordinated response to a seri cyber incidents. The NLE 2012 on examining four major theme implementation of the draft Nat Incident Response Plan (NCIR among governmental entities, i sharing, and decision making.
Responding to Cyber Attacks and the Applicability of Existing International Law	Army War College	January 2013	The paper identifies how the U should respond to the threat of operations against essential go private networks. First, it exam applicability of established inte cyber operations. Next, it prop for categorizing cyber operatio spectrum synchronized with es international law. Then, it discu already taken by the United St critical government and private concludes with additional steps States should take to respond cyber operations. (34 pages)
Crisis and Escalation in Cyberspace	RAND Corporation	December 2012	The report considers how the A integrate kinetic and nonkinetic

			Central to this process was car consideration of how escalation risks should be treated, which, demanded a broader considera entire crisis-management spec crises can be managed by taki reduce the incentives for other into crisis, controlling the narra understanding the stability para crises, and trying to manage es conflicts arise from crises. (200
Cyberattacks Among Rivals: 2001-2011 (from the article, "The Fog of Cyberwar" by Brandon Variano and Ryan Maness	*Foreign Affairs*	November 21, 2012	A chart showing cyberattacks b victim, 2001-2011. (Subscriptio
Proactive Defense for Evolving Cyber Threats	Sandia National Labs	November 2012	The project applied rigorous pr based analytics to two central a complementary aspects of the problem—attack strategies of t and vulnerabilities of the defen and used the results to develop grounded, practically implemen methodology for designing pro defense systems. (98 pages)
Safeguarding Cyber-Security, Fighting in Cyberspace	International Relations and Security Network (ISN)	October 22, 2012	Looks at the militarization of cy source of global tension and m that cyber warfare is already a feature of many leading states' calculations, followed by its op case that the threat posed by c capabilities is woefully oversta
Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World	Symantec Research Labs	October 16, 2012	The paper describes a method automatically identifying zero-c field-gathered data that records and malicious binaries are dow million real hosts around the w this data set for malicious files known vulnerabilities indicates appeared on the Internet befor corresponding vulnerabilities w (12 pages)
Federal Support for and Involvement in State and Local Fusion Centers	Senate Permanent Subcommittee on Investigations	October 3, 2012	A two-year bipartisan investiga U.S. Department of Homeland to engage state and local intell centers" have not yielded signi information to support federal c intelligence efforts. In Section V Centers Have Been Unable to Contribute to Federal Countert Part G, "Fusion Centers May H Not Aided, Federal Counterter the report discusses the Nover Russian "cyberattack" in Illinoi
Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States	*First Monday*	July 2, 2012	The essay argues that current tendencies within U.S. cyber w unproductive and even potenti argues that the war metaphor a deterrence analogy are neither inevitable and that abandoning open up new possibilities for th productively about the full spec cybersecurity challenges, inclu unrealized possibility of cyberw

Nodes and Codes: The Reality of Cyber Warfare	U.S. Army School of Advanced Military Studies, Command and General Staff	May 17, 2012	Explores the reality of cyber wa the story of Stuxnet. Three cas evaluate cyber policy, discours procurement in the United Stat China before and after Stuxnet similar, yet unique, realities of ((62 pages)
United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?	Triangle Institute for Security Studies	March 2012	The incongruence between na counterterrorism (CT) cyber po strategy degrades the abilities professionals to interdict transn from within cyberspace. To opt CT assets and to stymie the gr posed by terrorists' ever-expan cyberspace, national decision- modify current policies to effici national CT strategies, albeit w framework of existing CT cybe statutes. (34 pages)
A Cyberworm that Knows No Boundaries	RAND Corporation	December 21, 2011	Stuxnet-like worms pose a seri to infrastructure and computer not connected to the Internet. D against such attacks is an incre prospect. (55 pages)
Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934	DOD	November 2011	"When warranted, we will resp attacks in cyberspace as we w threat to our country. We reser use all necessary means - dipl informational, military< and eco defend our nation, our allies, o our interests." (14 pages)
Cyber War Will Not Take Place	*Journal of Strategic Studies*	October 5, 2011	The paper argues that cyber w taken place, is not currently tak unlikely to take place in the futu
Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011	Office of the National Counterintelligence Executive	October 2011	Because the United States is a development of new technolog player in global financial and tr foreign attempts to collect U.S. and economic information will c high level and will represent a c persistent threat to U.S. econo nature of the cyber threat will e continuing technological advan information environment. (31 p
A Four-Day Dive Into Stuxnet's Heart	*Threat Level* Blog *(Wired)*	December 27, 2010	"It is a mark of the extreme odd Stuxnet computer worm that M Windows vulnerability team lea from an obscure Belarusian se that even they had never heard
Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? A Preliminary Assessment	Institute for Science and International Security	December 22, 2010	The report indicates that comm Stuxnet code intended to incre frequency of devices targeted b exactly match several frequenc rotors in centrifuges at Iran's N enrichment plant are designed optimally or are at risk of break flying apart. (10 pages)
Stuxnet Analysis	European Network and Information Security Agency	October 7, 2010	A European Union cybersecuri that the Stuxnet malware is a g critical information infrastructur Computer systems that monito

			controlled and data acquisition infected with the worm might b to establish destructive over or conditions by running industria different frequencies.
Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy	National Research Council	October 5, 2010	Per request of the Office of the National Intelligence, the Natio Council undertook a two-phase to foster a broad, multidisciplin of strategies for deterring cybe United States and of the possil strategies for the U.S. governn pages)
Cyber Warfare: Armageddon in a Teacup?	Army Command and General Staff, Fort Leavenworth	December 11, 2009	This study examines cyber wa against Estonia in 2007, Georg Israel in 2008. According to the three cases cyber warfare did r strategic political objectives on warfare employed in the three mainly of Denial of Service atta defacement. These attacks we inconvenience to the affected r attacks were not of sufficient s sophistication, or duration to fo concession from the targeted r warfare offensive capability do defensive capability to the exte allow the achievement of a stra objective through cyber warfar possibility of strategic-level cyb remains great, but the capabilit demonstrated at this time." (10

Source: Highlights compiled by CRS from the reports.

Notes: Page counts are for documents; other cited resources are webpages.

Table 3. Cloud Computing,[2] "The Internet of Things,"[3] Smart Cities, and FedRAMP[4]

Title	Source	Date	Notes
About FedRAMP	FedRAMP.gov	Continuously Updated	The Federal Risk and Authorizatio Management Program (FedRAMF government-wide program that pr a standardized approach to secur assessment, authorization, and continuous monitoring for cloud products and services.
Internet of Things Consortium	Internet of Things Consortium	Continuously Updated	IoTC is comprised of hardware, software and analytics companies areas including home automation, wearables, connected cars, smart 3D printing, and virtual/augmente reality. On behalf of its members, IoTC is dedicated to the growth of internet of things marketplace and development of sustainable busin models. The IoTC educates techn firms, retailers, insurance compan marketers, media companies and wider business community about value of IoT.
Cyber-Physical Systems	National Science	Continuously	Cyber-physical systems (CPS) int

	Foundation (NSF)	Updated	sensing, computation, control, anc networking into physical objects a infrastructure, connecting them to Internet and to each other.
Cyber-Physical Systems	Office of Science and Technology Policy (OSTP), Networking and Information Technology Research and Development (NITRD) Program)	Continuously Updated	The CPS Senior Steering Group (is to coordinate programs, budget policy recommendations for CPS research and development (R&D) which includes identifying and integrating requirements, conduct joint program planning, and devel joint strategies.
Cyber-Physical Systems	University of California, Berkeley	Continuously Updated	"CPS are integrations of computa networking, and physical process Embedded computers and networ monitor and control the physical processes, with feedback loops w physical processes affect computa and vice versa."
Internet of Things Consortium	Technology hardware, software and analytics companies	Continuously Updated	IoTC is composed of hardware, software and analytics companies areas including home automation, wearables, connected cars, smart 3D printing, and virtual/augmente reality. On behalf of its members, IoTC is dedicated to the growth of Internet of things marketplace anc development of sustainable busin models. The IoTC educates techn firms, retailers, insurance compan marketers, media companies, anc wider business community about value of IoT.
Newly Launched 'Trusted IoT Alliance' Unites the Industry to Further a Blockchain-based Internet of Things	Medium	September 19, 2017	The mission of the Trusted IoT All is to bring companies together to develop and set the standard for a open source blockchain protocol t support IoT technology in major industries worldwide. The Alliance to fund small grants to support op source development and is review proposals from IoT and blockchai technologists.
Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD	GAO	July 27, 2017	Congress included provisions in re associated with two separate stat for GAO to assess the IoT-associa security challenges faced by DOD report (1) addresses the extent to DOD has identified and assessed security risks related to IoT device assesses the extent to which DOD developed policies and guidance to IoT devices, and (3) describes actions DOD has taken to address security risks related to IoT device pages)
Internet of Things: Communities Deploy Projects by Combining Federal Support with Other Funds and Expertise	GAO	July 26, 2017	All four of the communities that G reviewed are using federal funds i combination with other resources, financial and non-financial, to plar deploy IoT projects. For example, community used the $40 million D award to leverage, from communi

			partners, more than $100 million i additional direct and in-kind contributions, such as research or equipment contributions. Commur discussed four main challenges tc deploying IoT, including communit sectors (e.g., transportation, energ and public safety) that are siloed a proprietary systems that are not interoperable with one another. (4 pages)
The Internet of Things Connectivity Binge: What Are the Implications?	Pew Research Center	June 6, 2017	As automobiles, medical devices, TVs, manufacturing equipment an other tools and infrastructure are networked, is it likely that attacks, or ransomware concerns in the ne decade will cause significant num people to decide to disconnect, or the trend toward greater connectiv objects and people continue unab Some 1,201 responded to this nonscientific canvassing: 15% of t particular respondents said signifi numbers would disconnect and 85 chose the option that most people move more deeply into connected (94 pages)
Technology Assessment: Internet of Things: Status and implications of an increasingly connected world	GAO	May 15, 2017	GAO reviewed key reports and sc literature; convened two expert meetings with the assistance of th National Academies; and intervie officials from two agencies to obta their views on specific implications the IoT. (78 pages)
IoT, Automation, Autonomy, and Megacities in 2025	Center for Strategic & International Studies	April 26, 2017	Engineers designing and impleme internet-connected IOT devices fa daunting challenges that is creatir discomfort with what they see evo in their infrastructures. This paper their concerns to life by extrapolat from present trends to describe plausible (likely?) future crises pla out in multiple global cities within years. Much of what occurs in the scenarios is fully possible today. T paper attempts to reveal what is possible when these technologies applied to critical infrastructure applications en masse without ade security in densely populated citie the near future that are less resilie than other environments. (16 pag
The Cyber Shield Act: Is the Legislative Community Finally Listening to Cybersecurity Experts?	Institute for Critical Infrastructure Technology	April 2017	There are three main criteria to er Cyber Shield program works. Firs officials must ensure industry leac are involved in developing the rati but not leading the team. Second, program should include a substan public education component aime making consumers care enough a cybersecurity that the rankings ac change their buying decisions. Fir the rankings themselves should g beyond a mere one-star to five-sta

			ranking to incorporate more dynar data. (8 pages)
A 21st Century Cyber-Physical Systems Education	National Academy of Sciences Computer Science and Telecommunications Board	February 2017	The report describes the knowled skills required to engineer increas capable, adaptable, and trustwortl systems that integrate the cyber a physical worlds and recommends for creating the courses and progr needed to educate the engineerin workforce that builds them. (107 p
A Data Privacy Playbook	Berkman Klein Center (Harvard)	February 2017	Opening data has many importan benefits, but sharing data comes v inherent risks to individual privacy released data can reveal informat about individuals that would other not be public knowledge. The doc is takes a first step toward codifyi responsible privacy-protective approaches and processes that c be adopted by cities and other gro that are publicly releasing data. (1 pages)
Cross-Device Tracking: An FTC Staff Report	FTC	January 23, 2017	The report describes the technolo used to track consumers across n Internet-connected devices, the b and challenges associated with it, industry efforts to address those challenges. The report concludes making recommendations to indus about how to apply traditional prin like transparency, choice, and sec to this relatively new practice. (23 pages)
Rise of the Machines: the Dyn Attack Was Just a Practice Run	Institute for Critical Infrastructure Technology	December 2016	The Mirai IoT botnet has inspired renaissance in adversarial interes DDoS botnet innovation based on lack of fundamental security-by-de in the Internet and in IoT devices. report provides a comprehensive detailed analysis of this threat whi forced stakeholders to recognize t lack of security by design and the prevalence of vulnerabilities inher the foundational design of IoT dev (62 pages)
Internet of Things will demand a step-change in search solutions	IEEE Intelligent Systems	November 23, 2016	With more and more IoT devices l connected to the Internet, and sm data projects starting to be implemented, there is an urgent n develop new search solutions tha allow information from IoT source found and extracted. Although exi search engines have ever more sophisticated and effective ways c crawling through web pages and searching for textual data, the arti argues that they will not be effecti accessing the type of numerical a sensory data that IoT devices will to gather. (5 pages)
Internet of Things (IoT) Security and Privacy Recommendations	Broadband Internet Technical Advisory Group (BITAG)	November 22, 2016	BITAG believes the recommendat outlined in this report may help to dramatically improve the security

			privacy of IoT devices and minimiz costs associated with collateral da In addition, unless the IoT device —the sector of the industry that manufactures and distributes thes devices—improves device securit privacy, consumer backlash may impede the growth of the IoT marketplace and ultimately limit th promise that IoT holds. (43 pages
Strategic Principles for Securing the Internet of Things	DHS	November 15, 2016	The document explains IoT risks a provides a set of nonbinding princ and suggested best practices to b toward a responsible level of secu the devices and systems business design, manufacture, own, and op (17 pages)
Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems	NIST	November 2016	NIST formally unveiled their guide for increasing the security of Inter connected devices. The guide pro security guidelines for 30 different processes involved with managing Internet-connected devices, from supply phase to testing. (257 pag
Building Smart Communities for the Future: Proceedings of a Workshop	National Academies Press	October 2016	Summary of presentations at June 22, 2016, Government-University- Industry Research Roundtable (G meeting to explore the role of connectedness and sustainability developing smart communities; th challenges and opportunities asso with the roll-out of intelligent syste and the partnerships among governments, universities, and ind that are integral to these advance pages)
Announcing Over $80 million in New Federal Investment and a Doubling of Participating Communities in the White House Smart Cities Initiative	White House	September 26, 2016	In September 2015, the White Ho launched the Smart Cities Initiativ make it easier for cities, federal agencies, universities, and the pri sector to work together to researc develop, deploy, and testbed new technologies that can help make c cities more inhabitable, cleaner, a more equitable. This year, to kick Smart Cities Week, the Administra expanding this initiative, with over million in new federal investments doubling of the number of particip cities and communities, exceeding total.
Demystifying the Internet of Things	(Information Technology Laboratory) ITL Bulletin	September 2016	NIST SP800-183 offers an underl and foundational science for IoT– based technologies on the realiza that IoT involves sensing, comput communication, and actuation. It presents a common vocabulary to a better understanding of IoT and communication between those pa discussing IoT. (4 pages)
Increasing the Potential of IoT through Security and Transparency	NTIA	August 2, 2016	NTIA is planning to launch a new multistakeholder process to suppo better consumer understanding of

			products that support security upg They have used this approach to make progress on issues such as cybersecurity vulnerability disclos and to provide more transparency data collected by mobile apps. Gi the burgeoning consumer adoptio IoT, the time seems ripe to bring stakeholders together to help driv some guidelines to encourage the growth of IoT.
Network of 'Things'	NIST	July 28, 2016	The publication provides a basic r aimed at helping researchers bett understand IoT and its security challenges. (30 pages)
How Is the Federal Government Using the Internet of Things?	Center for Data Innovation	July 25, 2016	The federal government faces a n of challenges that have slowed th adoption of IoT in the public secto First, there is a lack of strategic leadership at the federal level abo how to make use of IoT. Second, agencies do not always have worl with the necessary technical skills effectively use data generated by Third, federal agencies do not hav sufficient funding to modernize the infrastructure and begin implemer IoT pilot projects. Fourth, even wh funding exists, federal procureme policies often make it difficult for agencies to quickly and easily ado technology. Finally, risks and unce —about privacy, security, interoperability, and return on investment—delay federal adoptio potential federal users wait for the technology to mature and others t adopt first. (30 pages)
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	FTC Bureau of Consumer Protection and Office of Policy Planning	June 2, 2016	FTC staff comment on NTIA's Re for Comment on the Internet of Th The comment highlights lessons l from the FTC's law enforcement, consumer and business educatio policy activities relating to these is It then addresses the benefits and of IoT, highlights some best practi recommendations for industry, discusses the role of government fostering innovation in IoT product services, and sets forth some considerations for NTIA in setting standards and promoting interoperability. (17 pages)
Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance	GAO	April 7, 2016	GAO was asked to examine feder agencies' use of Service Level Agreements (SLAs). GAO's objec were to (1) identify key practices i cloud computing SLAs and (2) determine the extent to which fed agencies have incorporated such practices into their SLAs. GAO an research, studies, and guidance developed by federal and private entities to establish a list of key

			practices to be included in SLAs. validated its list with the entities, including OMB, and analyzed 21 service contracts and related documents of five agencies (with largest fiscal year 2015 IT budget against the key practices to identi variances, their causes, and impa (46 pages)
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	National Telecommunications and Information Administration (NTIA)	April 6, 2016	NTIA is initiating an inquiry regard the Internet of Things (IoT) to revi current technological and policy landscape. Through this notice, N seeks broad input from all interest stakeholders—including the privat industry, researchers, academia, civil society—on the potential ben and challenges of these technolog and what role, if any, the U.S. government should play in this are After analyzing the comments, the department intends to issue a "gre paper" that identifies key issues impacting deployment of these technologies, highlights potential benefits and challenges, and iden possible roles for the federal government in fostering the advancement of IoT technologies partnership with the private sector pages)
Product Testing and Validation	Underwriters Laboratories	April 4, 2016	The UL Cybersecurity Assurance Program (CAP) certification verifie a product offers a reasonable leve protection against threats that ma result in unintended or unauthoriz access, change or disruption.... T 2900] Standard contains requirem for the vendor to design the secur controls in such a way that they demonstrably satisfy the security of the product. The Standard also describes testing and verification requirements aimed at collecting evidence that the designed securi controls are implemented.
Alternative perspectives on the Internet of Things	Brookings Institution	March 25, 2016	Brookings scholars contribute thei individual perspectives on the poli challenges and opportunities asso with IoT.
Emerging Cyber Threats Report 2016	Georgia Institute of Technology Cybersecurity Summit 2015	November 2015	"The intersection of the physical a digital world continued to deepen 2015. The adoption of network-connected devices and sensors— Internet of Things—accelerated a was expected to reach nearly 5 bi devices by the end of the year." (2 pages)
Interim Report on 21st Century Cyber-Physical Systems Education	NSF	July 2015	"CPS [also known as The Internet Things] are increasingly relied on provide the functionality and value products, systems, and infrastruct sectors including transportation, h

			care, manufacturing, and electrica power generation and distribution are smart, networked systems wit embedded sensors, computer processors, and actuators that se and interact with the physical worl support real-time, guaranteed performance; and are often found critical applications." (48 pages)
Internet of Things: Mapping the Value Beyond the Hype	McKinsey Global Institute	June 2015	The paper is based upon a study more than 100 use cases of the In of Things' (IoT's) potential econon impact within next 10 years. It out who will benefit and by how much also covers the factors—both ena and barriers—that organizations fa they develop their IoT solutions. (pages)
Cloud Computing: Should Companies Do Most of Their Computing in the Cloud?	*The Economist*	May 26, 2015	Big companies have embraced th cloud more slowly than expected. are holding back because of costs others are wary of entrusting sens data to another firm's servers. Sho companies be doing most of their computing in the cloud? Represen the "Yes" viewpoint is Simon Cros founder and chief technology offic (CTO) of Bromium Inc. Represent the "No" viewpoint is Bruce Schne CTO at Resilient Systems.
Formation of the Office of Technology Research and Investigation (OTRI)	Federal Trade Commission (FTC)	March 23, 2015	The OTRI will provide expert rese investigative techniques, and furth insights to the agency on technolo issues involving all facets of the F consumer protection mission, inclu privacy, data security, connected c smart homes, algorithmic transpar emerging payment methods, big d and IoT. Like the former Mobile Technology Unit (MTU), the new o will be housed in the Bureau of Consumer Protection and is the agency's latest effort to ensure tha core consumer protection mission pace with the rapidly evolving digi economy. Kristin Cohen, the curre chief of the MTU, will lead the wor the OTRI.
Insecurity in the Internet of Things (IoT)	Symantec	March 12, 2015	Symantec analyzed 50 smart hom devices available today and found none of them enforced strong passwords, used mutual authentic or protected accounts against bru force attacks. Of the mobile apps to control the tested IoT devices, a two out of 10 did not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. The tested IoT technology also contain many common vulnerabilities. (20 pages)
FedRAMP High Baseline	General Services Administration (GSA)	February 3, 2015	GSA released a draft of security-c requirements for cloud-computer

			systems purchased by federal age for "high-impact" uses. High-impa will likely consist of health and law enforcement data, but not classifie information. Currently, cloud comp vendors seeking to sell to federal agencies must obtain security accreditation through FedRAMP. T date, FedRAMP has offered accreditations up to the moderate impact level. About 80% of federa systems are low- and moderate-impacts.
What is The Internet of Things?	O'Reilly Media	January 2015	Ubiquitous connectivity is meeting era of data. Since working with lar quantities of data became dramat cheaper and easier a few years a everything that touches software h become instrumented and optimiz Finance, advertising, retail, logisti academia, and practically every o discipline has sought to measure, model, and tweak its way to efficie Software can ingest data from ma inputs, interpret it, and then issue commands in real time. (Free registration required.) (32 pages)
FedRAMP Forward: 2 Year Priorities	General Services Administration (GSA)	December 17, 2014	The report addresses how the pro will develop over the next two yea GSA is focusing on three goals fo FedRAMP: • increased compliance and ag participation, • improved efficiencies, and • continued adaptation. (14 pa
The Internet of Things: 2014 OECD Tech Insight Forum	Organisation for Economic Co-operation and Development (OECD)	December 11, 2014	The IoT extends Internet connecti beyond traditional machines such computers, smartphones, and tab a diverse range of every-day devi that use embedded technology to interact with the environment, all v Internet. How can this collected da used? What new opportunities wil create for employment and econo growth? How can societies benefi technical developments to health, transport, safety and security, bus and public services? The OECD Technology Foresight Forum facili discussion on what policies and practices will enable or inhibit the of economies to seize the benefits IoT.
DOD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process	Department of Defense (DOD) Inspector General	December 4, 2014	Report states that the DOD chief information officer "did not develo implementation plan that assigned and responsibilities as well as associated tasks, resources and milestones," despite promises tha implementation plan would directl follow the cloud strategy's release pages)

NSTAC Report to the President on the Internet of Things	President's National Security Telecommunications Advisory Committee	November 18, 2014	The NSTAC unanimously approve recommendation that government Internet traffic could get priority transmission during emergencies. government already gets emerge priority in more traditional communications networks like the phone system through programs s as the Government Emergency Telecommunications Service (GET NSTAC now is proposing a GETS the Internet. (56 pages)
The Department of Energy's Management of Cloud Computing Activities: Audit Report	Department of Energy (DOE) Inspector General	September 1, 2014	According to the inspector genera should do a better job buying, implementing, and managing its c computing services. Programs an department-wide have independe spent more than $30 million on clo services, but the chief information officer's office could not accuratel account for the money. (20 pages
Cloud Computing: The Concept, Impacts, and the Role of Government Policy	Organization for Economic Co-operation and Development (OECD)	August 19, 2014	The report gives an overview of cl computing, it • presents the concept, the ser it provides, and deployment models; • discusses how cloud comput changes the way computing i carried out; • evaluates the impacts of clou computing (including its bene and challenges as well as its economic and environmental impacts); and • discusses the policy issues ra by cloud computing and the r of governments and other stakeholders in addressing th issues. (240 pages)
Internet of Things: the Influence of M2M Data on the Energy Industry	GigaOm Research	March 4, 2014	The report examines the drivers o machine-2-machine (M2M)-data exploitation in the smart-grid secto the oil and gas sector, as well as t risks and opportunities for buyers suppliers of the related core technologies and services. (21 pa
Software Defined Perimeter	Cloud Security Alliance	December 1, 2013	Cloud Security Alliance's software defined perimeter (SDP) initiative to make "invisible networks" acce to a wider range of government agencies and corporations. The in will foster the development of architecture for securing the IoT u the cloud to create highly secure e end networks between IP-address entities. (13 pages)
Delivering on the Promise of Big Data and the Cloud	Booz Allen Hamilton	January 9, 2013	Reference architecture does away conventional data and analytics si

			consolidating all information into a single medium designed to foster connections called a 'data lake,' w reduces complexity and creates efficiencies that improve data visualization to allow for easier ins by analysts. (7 pages)
Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators	House Judiciary Committee, Subcommittee on Intellectual Property, Competition, and the Internet	July 25, 2012	Overview and discussion of cloud computing issues. (156 pages)
Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned	Government Accountability Office (GAO)	July 11, 2012	GAO recommends that the Secre of Agriculture, Health and Human Services, Homeland Security, Sta the Treasury, and the Administrato the General Services Administrati and Small Business Administratio should direct their respective chie information officers to establish estimated costs, performance goa and plans to retire associated lega systems for each cloud-based ser as applicable. (43 pages)
Cloud Computing Strategy	DOD Chief Information Officer	July 2012	The DOD Cloud Computing Strate introduces an approach to move t department from the current state duplicative, cumbersome, and cos of application silos to an end state is agile, secure, and cost-effective to a service environment that can rapidly respond to changing missi needs. (44 pages)
A Global Reality: Governmental Access to Data in the Cloud—A Comparative Analysis of Ten International Jurisdictions	Hogan Lovells	May 23, 2012	The white paper compares the na and extent of governmental acces data in the cloud in many jurisdicti around the world. (13 pages)
Policy Challenges of Cross-Border Cloud Computing	U.S. International Trade Commission	May 2012	The report examines the main pol challenges associated with cross- cloud computing—data privacy, se and ensuring the free flow of infor —and the ways countries are addressing them through domesti policymaking, international agreem and other cooperative arrangemer (38 pages)
Cloud Computing Synopsis and Recommendations (SP 800-146)	National Institute of Standards and Technology (NIST)	May 2012	NIST's guide explains cloud technologies in plain terms to fede agencies and provides recommendations for IT decisionmakers. (81 pages)
Global Cloud Computing Scorecard a Blueprint for Economic Opportunity	Business Software Alliance	February 2, 2012	The report notes that although ma developed countries have adjuste laws and regulations to address c computing, the wide differences in rules make it difficult for companie invest in the technology. (24 page
Concept of Operations: FedRAMP	General Services Administration (GSA)	February 7, 2012	FedRAMP is implemented in phas The document describes all the se that were available at the 2012 ini

			operating capability. The concept operations is updated as the prog evolves toward sustained operatio (47 pages)
Federal Risk and Authorization Management Program (FedRAMP)	Federal Chief Information Officers Council	January 4, 2012	FedRAMP provides a standard approach to assessing and autho (A&A) cloud computing services a products.
Security Authorization of Information Systems in Cloud Computing Environments (FedRAMP)	White House/Office of Management and Budget (OMB)	December 8, 2011	FedRAMP is now required for all agencies purchasing storage, applications, and other remote se from vendors. The Administration promotes cloud computing as a m to save money and accelerate the government's adoption of new technologies. (7 pages)
U.S. Government Cloud Computing Technology Roadmap, Volume I, Release 1.0 (Draft). High-Priority Requirements to Further USG Agency Cloud Computing Adoption (SP 500-293)	National Institute of Standards and Technology (NIST)	December 1, 2011	Volume I is aimed at interested pa that wish to gain a general understanding and overview of th background, purpose, context, wo results, and next steps of the U.S. Government Cloud Computing Technology Roadmap initiative. (3 pages)
U.S. Government Cloud Computing Technology Roadmap, Volume II, Release 1.0 (Draft), Useful Information for Cloud Adopters (SP 500-293)	National Institute of Standards and Technology (NIST)	December 1, 2011	Volume II is designed as a technic reference for those actively workir strategic and tactical cloud compu initiatives including, but not limited U.S. government cloud adopters. volume integrates and summarize work completed as of 2011 and ex how these findings support the ro introduced in Volume I. (85 pages
Information Security: Additional Guidance Needed to Address Cloud Computing Concerns	GAO	October 6, 2011	Twenty-two of 24 major federal agencies reported that they were concerned or very concerned abo potential information security risks associated with cloud computing. recommended that the NIST issue guidance specific to cloud comput security. (17 pages)
Cloud Computing Reference Architecture (SP 500-292)	NIST	September 1, 2011	The special publication, which is r official U.S. government standard designed to provide guidance to s communities of practitioners and researchers. (35 pages)
Federal Cloud Computing Strategy	White House	February 8, 2011	The strategy outlines how the fede government can accelerate the sa secure adoption of cloud computi and provides agencies with a fram for migrating to the cloud. It also examines how agencies can addr challenges related to the adoption cloud computing, such as privacy, procurement, standards, and governance. (43 pages)
25-Point Implementation Plan to Reform Federal Information Technology Management	White House	December 9, 2010	The plan's goals are to reduce the number of federally run data cente from 2,100 to approximately 1,300 rectify or cancel one-third of troub projects, and require federal agen

			adopt a "cloud first" strategy in wh they will move at least one systen hosted environment within a year. pages)
Federal Guidance Needed to Address Control Issues With Implementing Cloud Computing	GAO	July 1, 2010	The report suggests that the OME director should establish mileston completing a strategy for impleme the federal cloud computing initiat assist federal agencies in identifyi uses for and information security measures to use in implementing computing. (53 pages)

Source: Highlights compiled by CRS from the reports.

Notes: Page counts are for documents; other cited resources are webpages.

Author Contact Information

Rita Tehan, Information Research Specialist (rtehan@crs.loc.gov, 7-6739)

Footnotes

[1] "A breach constitutes a 'major incident' when it involves[personally identifiable information] that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people," the [OMB] memo states. "An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a 'major incident.'" Source: Fiscal Year 2016-2017 on Federal Information Security and Privacy Management Requirements, November 4, 2016.

[2] Cloud computing is a web-based service that allows users to access anything from email to social media on a third-party computer. For example, Gmail and Yahoo are cloud-based email services that allow users to access and store emails tha are saved on each respective service's computer, rather than on the individual's computer.

[3] The "Internet of Things" (IoT) refers to networks of objects that communicate with other objects and with computers through the Internet. "Things" may include virtually any object for which remote communication, data collection, or control might be useful, such as vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, or building systems. See also CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Eric A. Fischer.

[4] The Federal Risk and Authorization Management Program (FedRAMP) was established in December 2011 to provide a government-wide standard, centralized approach to assessing and authorizing cloud computing services and products. It reached initial operational capabilities in June 2012 and became fully operational during FY2014. See also CRS Report R42887, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*, by Patricia Moloney Figliola and Eric A. Fischer.