CRS Reports & Analysis

Cybersecurity: Overview Reports and Links to Government, News, and Related Resources
March 2, 2016 (R44405)
Jump to Main Text of Report
Rita Tehan, Information Research Specialist (rtehan@crs.loc.gov, 7-6739)
View Acknowledgments

Related Author

- Rita Tehan

Contents

- Introduction

Tables

- Table 1. Cybersecurity Overview
- Table 2. Congressional and Government Agencies Resources
- Table 3. International Organizations Resources
- Table 4. News Publications Resources
- Table 5. Other Associations and Institutions Resources

Summary

Much is written on the topic of cybersecurity. This CRS report and those listed below direct the reader to authoritative sources that address many of the most prominent issues. Included in the reports are resources and studies from government agencies (federal, state, local, and international), think tanks, academic institutions, news organizations, and other sources.

This report is intended to serve as a starting point for congressional staff assigned to cover cybersecurity issues. It includes annotated descriptions of reports, websites, or external resources:

- **Table 1**—cybersecurity overview
- **Table 2**—congressional and government resources
- **Table 3**—international organizations resources
- **Table 4** —news resources
- **Table 5**—other associations and institutions resources

The following CRS reports comprise a series that compiles authoritative reports and resources on these cybersecurity topics:

- CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan
- CRS Report R43310, *Cybersecurity: Data, Statistics, and Glossaries*, by Rita Tehan

For access to additional CRS reports and other resources, see the *Cybersecurity Issue Page* at http://www.crs.gov.

Introduction

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**—cybersecurity overview
- **Table 2**—congressional and government resources
- **Table 3**—international organizations resources
- **Table 4**—news resources
- **Table 5**—other associations and institutions resources

Table 1. Cybersecurity Overview

(reports offer an overview of single or multiple cybersecurity issues)

Title	Source	Date	Notes
Cybersecurity Collection	The National Academies Press	Continuously Updated	The prevention of cyberattacks on a nation's important computer and communications system and networks is a problem that looms large. To best prevent such attacks, this collection explains the importance of increasing the usability of security technologies, recommends strategies for future research aimed at countering cyberattacks, and considers how information technology systems can be used to not only maximize protection against attacks but also respond to threats.
Cyber Policy	Homeland Security Digital Library	Continuously Updated	A database of reports and documents grouped by audits and investigations, CRS reports, DOD reports, executive branch, hearings, international perspective, research and analysis, theses, and websites.
The Defender's Dilemma: Charting a Course Toward Cybersecurity	RAND Corp.	December 2015	This report, the second in a multiphase study on the future of cybersecurity, reveals perspectives and perceptions from chief information security officers; examines the development of network defense measures—and the countermeasures that attackers create to subvert those measures; and explores the role of software vulnerabilities and inherent weaknesses. Among the report's findings were that cybersecurity experts are at least as focused on preserving their organizations' reputations as protecting actual property. Researchers also found that organizational size and software quality play significant roles in the

			strategies that defenders may adopt. (162 pages)
Cybersecurity Dilemmas: Technology, Policy, and Incentives: Summary of Discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum	National Academy of Sciences (NAS)	October 2015	The forum examined a broad range of topics, including cybersecurity and international relations, privacy, rational cybersecurity, and accelerating progress in cybersecurity. The report summarizes the presentations and discussions from this forum. (32 pages)
Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance	Pardee Center for International Futures	August 28, 2015	The report analyzes the current economic impact of information communication technology (ICT) and examines potential futures through 2030. The research also considers the costs of adverse cyber events and the costs of efforts to prevent such events. (135 pages)
Net of Insecurity: A Disaster Foretold - And Ignored (Part 3)	*Washington Post*	June 22, 2015	The May 19, 1998 testimony (before the Senate Governmental Affairs Committee) "from L0pht, as the hacker group called itself, was among the most audacious of a rising chorus of warnings delivered in the 1990s as the Internet was exploding in popularity, well on its way to becoming a potent global force for communication, commerce and criminality.... "
Net of Insecurity: The Long Life of a Quick Fix (Part. 2)	*Washington Post*	May 31, 2015	"A key protocol created as a short-term solution in 1989 is designed to automatically trust users, a flaw that leaves the network ripe for attack."
Net of Insecurity: A Flaw in the Design (Part 1)	*Washington Post*	May 30, 2015	"Even as scientists spent years developing the Internet, few imagined how popular and essential it would become. Fewer still imagined that eventually it would be available for almost anybody to use, or to misuse."
Cyber Threat Information Sharing: Recommendations for Congress and the Administration	Center for Strategic and International Studies (CSIS)	March 10, 2015	The success of the President's executive order promoting cyberthreat information sharing depends on legislation passing Congress. The report recommends that legislation should not be one-size-fits-all; have a minimal role for government; build on existing information sharing; streamline mechanisms to share information; add value for all parties participating; protect information shared from FOIA requests, litigation, or regulatory enforcement; and protect organizations from civil and

			criminal liability for monitoring and sharing on cyberthreats if done in good faith. (18 pages)
The Emergence of Cybersecurity Law	Indiana University Maurer School of Law	February 2015	The paper examines cyberlaw as a growing field of legal practice and the roles that lawyers play in helping companies respond to cybersecurity threats. Drawing on interviews with lawyers, consultants, and academics knowledgeable in the intersection of law and cybersecurity, as well as a survey of lawyers working in general counsel's offices, the study examines the broader context of cybersecurity, the current legal framework for data security and related issues, and the ways in which lawyers learn about and involve themselves in cybersecurity issues. (31 pages)
OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy	The *RUSI Journal*	November 4, 2014	The article argues that cyber is "hyped out." Overstating the threat does have benefits (for some); it also comes with significant costs. The benefits are short-lived and easy to spot, whereas the costs are long-term and harder to understand—and they are piling up fast and high. Indeed, the costs are so high that the debate inches toward a turning point for all parties involved. The authors list 13 reasons why cybersecurity hype is counterproductive. (8 pages)
Power Relationships in the United States Federal Government and its Effect on Cybersecurity Policy	*Journal of Information System Security*	October 2014	The paper explores the power relationships that affected the decisions made by the executive, legislative, and judicial branches of government. It also describes how these power relationships changed as a result of the emerging reality of cyber security. (18 pages)
Ten Strategies of a World-Class Cybersecurity Operations Center	MITRE Corporation	October 2014	Reportedly, all too often, cybersecurity operations centers (CSOCs) are set up and operate with a focus on technology without adequately addressing people and process issues. The main premise of this book is that a more balanced approach would be more effective. The book describes the 10 strategies of effective CSOCs—regardless of their size, offered capabilities, or type of constituency served cost. (346 pages)
Policies for Enhancing U.S. Leadership in Cyberspace	National Science Foundation (NSF)	August 20, 2014	The project focuses on three areas in which U.S. policy could provide additional leadership in cyberspace—publication of

			zero-day exploits; labeling of neutral infrastructure, such as networks associated with hospitals or religious sites, and shared norms to protect neutral cyberspaces; and sustainment of Internet interoperability, which allows Internet users on different networks to communicate directly without interference. The findings may benefit national security by giving policymakers a way of assessing the costs and benefits of publishing exploits or patches.
Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies	Center for New American Security	July 2014	For key systems, the paper recommends sacrificing some Internet benefits to ensure security. "Methods for pursuing this strategy include stripping down systems so they do less but have fewer vulnerabilities, and integrating humans and other out-of-band (i.e., non-cyber) factors so the nation is not solely dependent on digital systems," as well as "making investments for graceful degradation." (64 pages)
At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues	National Academies Press	May 13, 2014	The report is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, the book may be a resource for policymakers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace. (102 pages)
Immediate Opportunities for Strengthening the Nation's Cybersecurity	President's Council of Advisors on Science and Technology (PCAST)	November 2013	The report recommends the government phase out insecure, outdated operating systems, such as Windows XP, implement better encryption technology, and encourage automatic security updates, among other changes. PCAST also recommends, for regulated industries, that the government help create cybersecurity best practices and audit the adoption of these practices. For independent agencies, the report suggests that PCAST should write new rules that require businesses to report their cyber improvements. (31 pages)
Defending an Open, Global, Secure, and Resilient Internet	Council on Foreign Relations	June 2013	The task force recommends that the United States develop a digital policy framework based on four pillars, the last of which is

			that U.S.-based industry work rapidly to establish an industry-led approach to counter current and future cyberattacks. (127 pages)
Measuring What Matters: Reducing Risk by Rethinking How We Evaluate Cybersecurity	Safegov.org, in coordination with the National Academy of Public Administration	March 2013	The report recommends that rather than periodically auditing whether an agency's systems meet the standards enumerated in the Federal Information Security Management Act (FISMA; P.L. 107-296 (Title X), and P.L. 107-347 (Title III)) at a static moment in time, agencies and their inspectors general should keep running scorecards of "cyber risk indicators" based on continual inspector general assessments of a federal organization's cyber vulnerabilities. (39 pages)
SEI [Software Engineering Institute] Emerging Technology Center: Cyber Intelligence Tradecraft Project	Carnegie Mellon University	January 2013	The report addresses the endemic problem of functional cyber intelligence analysts not effectively communicating with nontechnical audiences. It also notes organizations' reluctance to share information within their own entities, industries, and across economic sectors. (23 pages)
The National Cyber Security Framework Manual	NATO Cooperative Cyber Defense Center of Excellence	December 11, 2012	The report provides detailed background information and in-depth theoretical frameworks to help the reader understand the various facets of national cybersecurity, according to different levels of public policy formulation. The four levels of government—political, strategic, operational, and tactical/technical—each have their own perspectives on national cybersecurity, and each is addressed in individual sections within the manual. (253 pages)
20 Critical Security Controls for Effective Cyber Defense	CSIS	November 2012	The top 20 security controls from a public-private consortium. Members of the consortium include the National Security Agency (NSA), U.S. Computer Emergency Readiness Team, Department of Defense (DOD) Joint Task Force-Global Network Operations, Department of Energy Nuclear Laboratories, Department of State, and DOD Cyber Crime Center plus commercial forensics experts in the banking and critical infrastructure communities. (89 pages)
Mission Critical: A Public-Private	Business Roundtable	October 11, 2011	The report suggests that "[p]ublic policy

Strategy for Effective Cybersecurity			solutions must recognize the absolute importance of leveraging policy foundations that support effective global risk management, in contrast to 'check-the-box' compliance approaches that can undermine security and cooperation." The document concludes with specific policy proposals and activity commitments. (28 pages)
A Review of Frequently Used Cyber Analogies	National Security Cyberspace Institute	July 22, 2011	"The current cybersecurity crisis can be described several ways with numerous metaphors. Many compare the current crisis with the lawlessness to that of the Wild West and the outdated tactics and race to security with the Cold War. When treated as a distressed ecosystem, the work of both national and international agencies to eradicate many infectious diseases serves as a model as how poor health can be corrected with proper resources and execution. Before these issues are discussed, what cyberspace actually is must be identified." (7 pages)
America's Cyber Future: Security and Prosperity in the Information Age	Center for a New American Security	May 31, 2011	To help U.S. policymakers address the growing danger of cyber insecurity, the two-volume report features chapters on cybersecurity strategy, policy, and technology by some of the world's leading experts on international relations, national security, and information technology. (296 pages)
Resilience of the Internet Interconnection Ecosystem	European Network and Information Security Agency (ENISA)	April 11, 2011	The study consists of several parts. Part I provides a summary and recommendations. Part II (State of the Art Review) offers a detailed description of the Internet's routing mechanisms and an analysis of their robustness at the technical, economic, and policy levels. Part III (Report on the Consultation) reports and summarizes the results of consultation with a broad range of stakeholders. Part IV includes the bibliography and appendices. (238 pages)
Cybersecurity Two Years Later	CSIS	January 2011	The Commission on Cybersecurity for the 44th Presidency's reviews what progress has been made and what still need to be done, stemming from its 2008 report citing 25 recommendations for change. (22 pages)

Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop	National Research Council (NRC)	September 21, 2010	The report discusses computer system security and privacy, their relationship to usability, and research at their intersection. It is drawn from remarks made at the NRC's July 2009 *Workshop on Usability, Security and Privacy of Computer Systems* as well as reports from the NRC's Computer Science and Telecommunications Board on security and privacy. (70 pages)
National Security Threats in Cyberspace	Joint Workshop of the National Security Threats in Cyberspace and the National Strategy Forum	September 15, 2009	The two-day workshop brought together more than two dozen experts with diverse backgrounds, including physicists; telecommunications executives; Silicon Valley entrepreneurs; federal law enforcement, military, homeland security, and intelligence officials; congressional staffers; and civil liberties advocates. Participants engaged in an open-ended discussion of cyber policy as it relates to national security. (37 pages)

Source: Highlights compiled by the Congressional Research Service (CRS) from the sources.

Note: Page counts are given for documents; other cited resources are web pages.

Table 2. Congressional and Government Agencies Resources

Name	Source	Notes
Integrated Intelligence Center (IIC)	Center for Internet Security	Serves as a resource for state, local, tribal, and territorial government partners to engage in a collaborative information sharing and analysis environment on cybersecurity issues. Through this initiative, the IIC provides fusion centers, homeland security advisors, and law enforcement entities with access to a broad range of cybersecurity products, reflecting input from many sources.
Computer Security Resource Center	National Institute of Standards and Technology (NIST)	Links to NIST resources, publications, and computer security groups.
Cyber Domain Security and Operations	Department of Defense (DOD)	Links to press releases, fact sheets, speeches, announcements, and videos.
Cyber Strategy	DOD	The purpose of this strategy is to guide the development of DOD's cyber forces and strengthen its cyber defense and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DOD's three primary cyber missions.

Congressional Cybersecurity Caucus	Congressional Cybersecurity Caucus	Provides statistics, news on congressional cyberspace actions, and links to other information websites. The caucus is led by Representatives Jim Langevin and Mike McCaul.
Cybersecurity	White House National Security Council	Links to White House policy statements, key documents, videos, and blog posts.
Cybersecurity	National Telecommunications and Information Administration (NTIA) of U.S. Department of Commerce (DOC)	DOC's Internet Policy Task Force is conducting a comprehensive review of the nexus between cybersecurity challenges in the commercial sector and innovation in the Internet economy.
Cybersecurity and Information Systems	National Academy of Sciences (NAS) Trustworthiness Computer Science and Telecommunications Board	A list of independent and informed reports on cybersecurity and public policy.
Cyberspace Policy Review	White House	Document repository (news, federal, trade association, think tank reports, congressional hearings, etc.) posted to WhiteHouse.gov.
Getting Started for State, Local, Tribal, and Territorial (SLTT) Governments	United States Computer Emergency Readiness Team (U.S. CERT)	The resources are available to state, local, tribal, and territorial governments. These resources have been aligned to the five Cybersecurity Framework function areas. The page will be updated as additional resources—from DHS, other federal agencies, and the private sector—are identified.
Office of Cybersecurity and Communications (CS&C)	Department of Homeland Security (DHS)	CS&C is responsible for enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector ".com" domain to increase the security of critical networks. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.
President's National Security Telecommunications Advisory Committee (NSTAC)	DHS	NSTAC's goal is to develop recommendations to the President to assure vital telecommunications links through any event or crisis and to help the U.S. government maintain a reliable, secure, and resilient national communications posture.
U.S. Cyber-Consequences Unit	U.S. Cyber-Consequences Unit (U.S.-CCU)	U.S.-CCU, a nonprofit 501c(3) research institute, provides assessments of the strategic and economic

		consequences of possible cyberattacks and cyber-assisted physical attacks. It also investigates the likelihood of such attacks and examines the cost-effectiveness of possible counter-measures.

Source: Highlights compiled by CRS from the reports.

Table 3. International Organizations Resources

(international governments, associations, and think tanks)

Name	Source	Notes
Center for Internet Security (Australia)	Australian Communications and Media Authority	The Australian Internet Security Initiative (AISI) is an anti-botnet initiative that collects data on botnets in collaboration with Internet service providers and two industry codes of practice.
Cybercrime	Council of Europe	Links to the Convention on Cybercrime treaty, standards, news, and related information.
Cybersecurity Gateway	International Telecommunications Union (ITU)	ITU's Cybersecurity Gateway aims to be a collaborative platform, providing and sharing information between partners in civil society, private sector, governmental, and international organizations working in different areas of cybersecurity.
Cybercrime Legislation - Country Profiles	Council of Europe	These profiles have been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation.
ENISA: Securing Europe's Information Society	European Network and Information Security Agency (ENISA)	ENISA informs businesses and citizens in the European Union about cybersecurity threats, vulnerabilities, and attacks. (Requires free registration to access.)
International Cyber Security Protection Alliance (ICSPA)	ICSPA	A global nonprofit organization that aims to channel funding, expertise, and assistance directly to law enforcement cybercrime units around the world.
NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) (Tallin, Estonia)	North Atlantic Treaty Organization (NATO)	The center is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Hungary, Italy, the Slovak Republic, and Spain as sponsoring nations to enhance NATO's cyberdefense capability.

NCI Agency Cyber Security	NATO	The NCI Agency Cyber Security Service Line is responsible for the full lifecycle of NATO Cyber Security activities, designing, implementing and operating: Scientific and technical expertise, Supporting Acquisition, Maintenance and Sustainment, and Conducting Operations and Incident Management.

Source: Highlights compiled by CRS from the reports.

Table 4. News Publications Resources

(articles from news organizations)

Publication Name	Source	Notes
Computer Security (Cybersecurity)	*New York Times*	News about computer security (cybersecurity), including commentary and archival articles.
Cybersecurity	*NextGov.com*	The latest developments in protecting critical networks and digital information.
Cyberwarfare and Cybersecurity	*Benton Foundation*	Information on the use of computers and the Internet in conducting warfare in cyberspace.
Homeland Security	*Congressional Quarterly* (CQ)	News and analysis centered on homeland security issues, both within *CQ on Defense* and among the CQ's broader coverage of policy and legislation.
Cybersecurity	*The Hill*	Cybersecurity news stories, video and regulations.
Cybersecurity	*Homeland Security News Wire*	Analysis and coverage of cybersecurity news.

Table 5. Other Associations and Institutions Resources

(academic institutions, think tanks, trade associations and other non-governmental sources)

Name	Notes
Council on Cybersecurity	The council, based in the Washington, DC, area, is the successor organization to the National Board of Information Security Examiners (NBISE), founded in the United States in 2010 to identify and strengthen the skills needed to improve the performance of the cybersecurity workforce. The council will also be home to the U.S. Cyber Challenge, formerly a program of NBISE, which works with the cybersecurity community to bring accessible, compelling programs that motivate students and professionals to pursue education, development, and career opportunities in cybersecurity.

Cyber Aces Foundation	According to the Foundation, it offers challenging and realistic cybersecurity competitions, training camps, and educational initiatives through which high school and college students and young professionals develop the practical skills needed to excel as cybersecurity practitioners.
Cybersecurity from the Center for Strategic and International Studies (CSIS)	Links to experts, programs, publications, and multimedia. CSIS is a bipartisan, nonprofit organization whose affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change.
Cybersecurity Initiative	In partnership with the Hewlett Foundation, the Cybersecurity Initiative will build (1) a network of Cyber Fellows to write and contribute new thinking to the policy debate, (2) an International Cyber Network to write and comment on cybersecurity issues from a range of vantage points, and (3) a series of media partnerships to connect the above networks into and push forward wider public discourse. These include New America's relationship with Slate Magazine and its Future Tense blog, a cybersecurity focused podcast co-hosted with Christian Science Monitor, its "Future of War" programming with Defense One/The Atlantic.
Cyber Corps: Scholarship For Service (SFS)	SFS is designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. The program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning.
Cyber Policy	A featured collection of the Homeland Security Digital Library. Groups resources by audits and investigations, CRS reports, DOD reports, executive branch, hearings, international perspective, research and analysis, theses, and websites.
Cyber Security Policy and Research Institute (GWU)	The Cyber Security Policy and Research Institute (CSPRI) is a center for George Washington University and the Washington area to promote technical research and policy analysis of issues that have a significant computer security and information assurance component. CSPRI is the home for major information assurance and cybersecurity scholarship programs funded by the Department of Homeland Security and the National Science Foundation.
Digital and Cyberspace Policy Program, Council on Foreign Relations (CFR)	CFR experts investigate the impact of information and communication technologies on security, privacy, and international affairs.
Institute for Critical Infrastructure Technology	ICIT is a tactical, bipartisan forum of federal agency executives, legislative community members, and industry leaders focused on solution-based strategies to our nation's critical infrastructure obstacles. These publications are distributed to House and Senate Members, federal agencies, DHS-sector coordinating councils, and critical infrastructure leaders.
Institute for Information Infrastructure Protection (I3P)	I3P is a consortium of leading universities, national laboratories, and nonprofit institutions. It assembles multidisciplinary and multi-institutional research teams able to bring in-depth analysis to complex and pressing problems. Research outcomes are shared at I3P-sponsored workshops, professional conferences, and in peer-reviewed journals, as well as via technology transfer to end-users.

Integrated Intelligence Center (IIC)	IIC is a unit at the Center for Internet Security that serves as a resource to facilitate collaboration across multiple levels of government (federal, state, local, tribal, and territorial), relevant domains (both cyber and physical), and key disciplines (law enforcement, military, policy, and technical) to improve the responsiveness and efficiency of anticipating and responding to cyber events. The IIC includes the CIS 24/7/365 security operations center, incident response team, forensics lab, intelligence analysts, and key partners to identify patterns that may not have been detected without this collaborative environment.
Internet Security Alliance (ISA)	ISA is a nonprofit collaboration between the Electronic Industries Alliance, a federation of trade associations, and Carnegie Mellon University's CyLab.
Maryland Cybersecurity Center (University of Maryland)	MC2 is partnering with government and industry to provide educational programs to prepare the future cybersecurity workforce, and develop new, innovative technologies to defend against cybersecurity attacks.
National Association of State Chief Information Officers (NASCIO)	NASCIO provides state chief information officers (CIOs) and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information, and promote the adoption of IT best practices and innovations. The resource guide provides examples of state awareness programs and initiatives.
National Initiative for Cybersecurity Education (NICE)	NICE's goal is to establish an operational, sustainable, and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. The National Institute of Standards and Technology is leading the NICE initiative, including more than 20 federal departments and agencies, to try to ensure coordination, cooperation, focus, public engagement, technology transfer, and sustainability.
National Security Cyberspace Institute (NSCI)	NSCI provides education, research, and analysis services to government, industry, and academic clients aiming to increase cyberspace awareness, interest, knowledge, and capabilities.
Security Studies: Cybersecurity	Research LibGuide, created by the Georgia Institute of Technology Library, is a guide to resources in international security, military, defense, and intelligence studies.
U.S. Cyber Challenge (USCC)	USCC's goal is to find 10,000 of America's best and brightest people to fill the ranks of cybersecurity professionals where their skills can be of the greatest value to the nation.

Source: Highlights compiled by CRS from the reports of related associations and institutions.

Author Contact Information

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

Acknowledgments

See CRS Report R42619, *Cybersecurity: CRS Experts*, by Eric A. Fischer, for the names and contact information of CRS experts on policy issues related to cybersecurity.