CRS Reports & Analysis

Cybersecurity: Education, Training, and R&D Authoritative Reports and ResourcesCybersecurity: Education, Training, and R&D Authoritative Reports and Resources
March 3, 2016 (R44406)
Jump to Main Text of Report
Rita Tehan, Information Research Specialist (rtehan@crs.loc.gov, 7-6739)

Related Author

- Rita Tehan

Contents

Tables

Summary

Much is written on the topics of current gaps in the education and training of a cybersecurity workforce and the need for technology research and development (R&D) to solve cybersecurity technical issues. This CRS report directs the reader to authoritative sources that address these 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 also includes resources and studies from government agencies (federal, state, local, and international), think tanks, academic institutions, news organizations, and other sources.

Table 1 provides education and training resources, including scholarships, internships, the cybersecurity workforce, and the National Cybersecurity Centers of Excellence (NCCoE).

Table 2 provides R&D resources, including the Defense Advanced Research Project Agency (DARPA), National Science Foundation (NSF), Department of Defense (DOD), and private industry R&D programs and funding.

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

- CRS Report R44405, *Cybersecurity: Overview Reports and Links to Government, News, and Related Resources* Cybersecurity: Overview Reports and Links to Government, News, and Related Resources
- 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 the topics of current gaps in the education and training of a cybersecurity workforce and the need for technology research and development (R&D) to solve cybersecurity technical issues. This CRS report directs the reader to authoritative sources that address many of these 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. It includes resources and studies from government agencies (federal, state, local, and international), think tanks, academic institutions, news organizations, and other sources related to

- **Table 1**—education and training, including scholarships, internships, the cybersecurity workforce, and the National Cybersecurity Centers of Excellence (NCCoE); and
- **Table 2**—R&D, including the Defense Advanced Research Project Agency (DARPA), National Science Foundation (NSF), Department of Defense (DOD), and private industry R&D programs and funding.

Table 1. Education and Training

(includes scholarships, internships, cybersecurity workforce, and the National Cybersecurity Center of Excellence [NCCoE])

Title	Source	Date	Notes
U.S. Cyber Challenge (USCC)	Center for Internet Security	Continuously Updated	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.
Information Assurance Scholarship Program	Department of Defense (DOD)	Continuously Updated	The Information Assurance Scholarship Program is designed to increase the number of qualified personnel entering the information assurance and information technology fields within the department. The scholarships also are an attempt to effectively retain military and civilian cybersecurity and IT personnel.
National Initiative for Cybersecurity Careers and Studies (NICCS)	Department of Homeland Security (DHS)	Continuously Updated	NICCS is an online resource for cybersecurity career, education, and training information. It is a partnership between DHS, the National Institute of Standards and Technology (NIST), the Office of the Director of National Intelligence (ODIN), DOD, the Department of Education (ED), the National Science Foundation (NSF), and the Office of Personnel Management (OPM).
Experimental Research Testbed (DETER)	DHS	Continuously Updated	The DETER testbed is used to test and evaluate cybersecurity technologies of more than 200 organizations from more than 20 states and 17 countries, including DHS-funded researchers, the

			larger cybersecurity research community, government, industry, academia, and educational users.
National Centers of Academic Excellence (CAE) in Information Assurance (IA)/Cyber Defense (CD)	DHS and National Security Agency (NSA)	Continuously Updated	These programs promote higher education and research in IA and increasing the number of professionals with IA expertise in various disciplines. Postsecondary institutions may receive a CAE/IAE or CAE-R designation that is valid for five academic years. A school must successfully reapply to retain its CAE designation. Students attending these designated schools are eligible to apply for scholarships and grants through the DOD's Information Assurance Scholarship Program (IASP) and the Scholarship for Service (SFS) program.
Training for High-Growth Information Technology and Cybersecurity Jobs	Department of Labor (DOL)	September 29, 2014	The Trade Adjustment Assistance Community College and Career Training (TAACCCT) competitive grant program funded $450 million in job-driven training grants to nearly 270 community colleges across the country. The program is co-administered by the DOL and ED.
Cybersecurity Initiative	George Washington University	Continuously Updated	The initiative focuses Interdisciplinary approaches to cybersecurity education, active defense, intellectual property and trade secrets, and workforce development.
The State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the United States	National Cyber Security Alliance and Microsoft	May 2011	The survey explores the perceptions and practices of U.S. teachers, school administrators, and technology coordinators in regards to cyberethics, cybersafety, and cybersecurity education. It finds that young people still are not receiving adequate training and that teachers are ill-prepared to teach the subjects due, in large part, to lack of professional development. (16 pages)

National Initiative for Cybersecurity Education (NICE)	National Institute of Standards and Technology (NIST)	Continuously Updated	NICE is an ongoing program to teach Americans sound cybersecurity practices. The program's goals are to enhance the security of the country, improve computer security in the workplace and at home, and prepare future employees in the cybersecurity workforce.
National Cybersecurity Center of Excellence (NCCoE) Partnerships	NIST's NCCoE	Continuously Updated	Established in 2012 through a partnership between NIST, the state of Maryland, and Montgomery County, the NCCoE is dedicated to furthering innovation through the rapid identification, integration, and adoption of practical cybersecurity solutions. The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division.
Federal Cyber Service: Scholarship for Service (SFS)	National Science Foundation (NSF)	Continuously Updated	The program provides funds to institutions of higher education (IHE) through two tracks: The *Scholarship Track* award scholarships to students in the IA and computer security fields for the final two years of undergraduate study, master's-level study, or Ph.D.-level study. In addition, student recipients participate in a summer internship in the federal government. The *Capacity Building Track* funds IA faculty professional development and the development of IA academic programs.
Campus Cyberinfrastructure - Data, Networking, and Innovation Program (CC*DNI)	NSF	Continuously Updated	CC*DNI Invests in campus-level data and networking infrastructure and integration activities tied to achieving higher levels of performance, reliability and predictability for science applications, and distributed research projects.
Internships, co-op program, scholarships, and work study programs	National Security Agency/Central Security Service	Continuously Updated	NSA/CSS provides scholarships and internships for high school, undergraduate, and graduate

	(NSA/CSS)		students.
National Centers of Academic Excellence (CAE) in Cyber Operations Program	NSA	Continuously Updated	The program is intended to be a deeply technical, interdisciplinary, higher-education program grounded in the computer science, computer engineering, or electrical engineering disciplines with extensive opportunities for hands-on applications via labs and exercises.
Michigan Cyber Range (MCR)	Merit Networks	Continuously Updated	MCR enables individuals and organizations to develop detection and reaction skills through simulations and exercises. This is a partnership between the state of Michigan, Merit Network, federal and local governments, colleges and universities, and the private sector.
Cyber Career Connection (SC3)	Symantec	Continuously Updated	SC3 was launched in 2014 with the Symantec Foundation at the Clinton Global Initiative America summer meeting. The program provides underserved young adults and veterans with targeted education, training, and certifications that position them to fill in-demand cybersecurity jobs and enter long-term careers. SC3 provides a mix of classroom and hands-on education, followed by on-the-job experience at cybersecurity internships with some of America's leading employers.
DHS Secretary's Honors Program: Cyber Student Volunteer Initiative	DHS	Continuously Updated	The Initiative is for current college students pursuing a program of study in a cybersecurity-related field. Selected students learn about the DHS cybersecurity mission, complete hands-on cybersecurity work, and build technical experience in key areas, such as digital forensics, network diagnostics, and incident response.
NIST to Support Cybersecurity Jobs "Heat Map" to Highlight Employer Needs and	NIST	October 27, 2015	NIST will fund a project developing a visualization tool

Worker Skills			that will show the demand for and availability of cybersecurity jobs across the United States.
VetSuccess: Scholarships and Jobs for Veterans in Cybersecurity	SANS Institute and Center for Strategic & International Studies (CSIS)	December 11, 2014	VetSuccess will provide scholarships to 12 Air Force veterans to receive training and certifications in network intrusion detection, incident handling, and cybersecurity foundations. Scholarship recipients will also be matched with highly sought-after jobs in cybersecurity.
U.S.A. Cyber Warrior Scholarship Program	(ISC)^2 Foundation and Booz Allen Hamilton	June 21, 2013	The (ISC)^2 Foundation and Booz Allen Hamilton announced the launch of the U.S.A. Cyber Warrior Scholarship program, which will provide scholarships to veterans to obtain specialized certifications in the cybersecurity field. The scholarships are intended to cover all of the expenses associated with certification, such as training, textbooks, mobile study materials, certification testing, and the first year of certification maintenance fees.
Cyber Security Test Bed: Summary and Evaluation Results	Institute for Homeland Security Solutions	October 2012	The project was a case-study analysis of how a set of interventions, including threat analysis, best-practices sharing, and executive and staff training events, over the course of one year would impact a group of nine small and mid-sized businesses in North Carolina. Pre- and post-test-bed interviews were conducted with company officials to establish a baseline and evaluate the impact of the program. After the test-bed experience, decision makers at these companies indicated an increase in their perceptions of the risk of cyberattacks and in their knowledge of possible solutions. (89 pages)
Preparing the Pipeline: The U.S. Cyber Workforce for the Future	National Defense University	August 2012	The paper addresses methods to close the gaps between demand and existing capabilities and capacity in the U.S. cyber

			workforce. A large number of professionals with not only technical skills but also an understanding of cyber policy, law, and other disciplines will be needed to ensure the continued success of the U.S. economy, government, and society in the 21st-century information age. The government, think tanks, and the private sector have developed innovative methods for closing these gaps, but more needs to be done. (17 pages)
U.S. Department of Energy to Offer $25M Grant for Cybersecurity	White House	January 15, 2015	Vice President Joe Biden and Energy Secretary Ernest Moniz announced a $25 million DOE grant over five years for cybersecurity education. The grant program will establish a Cybersecurity Workforce Pipeline Consortium within the DOE with funding from its Minority Serving Institutions Partnerships Program under its National Nuclear Security Administration. The participants are historically black colleges and universities, national labs and K-12 school districts.

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

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

Table 2. Research and Development (R&D)

(includes DARPA, NSF, DOD, and private industry R&D programs and funding)

Title	Source	Date	Notes
Digital Intelligence and Investigation	CERT Software Engineering Institute (Carnegie Mellon)	Continuously Updated	Current tools and processes are inadequate for responding to increasingly sophisticated attackers and cybercrimes. To address this problem, the Digital Intelligence and Investigation Directorate (DIID) conducts research and develops technologies, capabilities, and practices that organizations can use to develop incident response capabilities and facilitate forensics investigations. DIID team members also develop advanced tools and techniques to address gaps that are not covered by existing resources.

Transparent Computing	Defense Advanced Research Projects Agency (DARPA)	Continuously Updated	The Transparent Computing (TC) program aims to develop basic technologies that are separable and usable in isolation (e.g., within a given software layer or application environment, such as web middleware) while exploring the best way to integrate multiple TC technologies in an experimental prototype.
Cyber Grand Challenge	DARPA	Continuously Updated	Cyber Grand Challenge (CGC) is a contest to build high-performance computers capable of playing in a Capture-the-Flag style cybersecurity competition. During all competition events, fully automated systems will compete with no human involvement. The final competition event will be visualized, narrated, and streamed worldwide. CGC is open at no cost to teams around the world, and the top prize at the final competition event will be $2M.
Cyber Consortium	Fortinet and Palo Alto Networks	Continuously Updated	The consortium seeks to share intelligence on threats across large security vendors and aid a coordinated response to incidents. No customer data will be shared, only malware samples. The two companies also extend an open invitation to other security firms to join them, provided these firms can share at least 1,000 samples of new malware executables each day.
IEEE Computer Society Center for Secure Design	Institute of Electrical and Electronics Engineers (IEEE) Cyber Security	Continuously Updated	The Center for Secure Design aims to shift some of the focus in security from finding bugs to identifying common design flaws in the hope that software architects can learn from others' mistakes.
Annual Best Scientific Cybersecurity Paper Competition	National Security Agency (NSA)	Continuously Updated	The competition is for scientific papers that show an outstanding contribution to cybersecurity science. The competition was created to stimulate research toward the development of systems that are resilient to cyberattacks. Entries are judged on scientific merit, the strength and significance of the work reported, and the degree to which the paper exemplifies how to perform and report scientific research in cybersecurity.
National Cybersecurity Center of Excellence (NCCoE)	National Institute of Standards and Technology (NIST)	Continuously Updated	The NCCoE is a new public-private collaboration to bring together experts from industry, government, and academia to design, implement, test, and demonstrate integrated cybersecurity solutions and

			promote their widespread adoption.
Rapid Attack Detection, Isolation and Characterization (RADICS) Proposers Day	DARPA	November 24, 2015	DARPA is interested in technology that can detect network anomalies signaling a threat or attack, map out industrial control systems and analyze system protocols—especially for threats directed at the power grid and related systems. In general, DARPA is seeking an "automation revolution in computer security" so that machines can discover and fix software vulnerabilities within seconds, "instead of waiting up to a year under the current human-centric system."
NSF Awards $74.5 Million to Support Interdisciplinary Cybersecurity Research	National Science Foundation (NSF)	October 7, 2015	The NSF awarded $74.5 million in research grants through the NSF Secure and Trustworthy Cyberspace (SaTC) program. In total, the SaTC investments include a portfolio of 257 new projects to researchers in 37 states. The largest, multi-institutional awards include research to better understand and offer reliability to new forms of digital currency known as cryptocurrencies, which use encryption for security; invent new technology to broadly scan large swaths of the Internet and automate the detection and patching of vulnerabilities; and establish the "science of censorship resistance" by developing accurate models of the capabilities of censors.
Leveraging the Analog Domain for Security (LADS) Program	(DARPA	September 25, 2015	DARPA is soliciting innovative research proposals in the area of enhanced cyber defense through analysis of involuntary analog emissions. Proposed research should investigate innovative approaches that enable evolutionary advances in science, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice.
Federal Cybersecurity R&D Strategic Plan: Request for Information	NSF	April 27, 2015	In response to the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), federal agencies are developing a cybersecurity research and development strategic plan. On behalf of the agencies, the Cyber Security and Information Assurance Research and Development Senior Steering Group seeks public input on research objectives for the plan. The strategic plan is intended to be used to guide and coordinate federally funded

			cybersecurity research. (1 page)
DHS S&T App Technology Transitions to Commercial Market	Department of Homeland Security (DHS) Science and Technology Directorate	December 5, 2014	DHS announced it would continue funding technology company Kryptowire so the company could further pursue private-sector clients. Kryptowire sells software that identifies security vulnerabilities in mobile applications and archives the results. (1 page)
Hewlett Foundation Announces $45 Million in Grants to MIT, Stanford, UC Berkeley to Establish Major New Academic Centers for Cybersecurity Policy Research	Hewlett Foundation	November 18, 2014	The new programs, established with $45 million in grants from the Hewlett Foundation ($15 million to each school), are supported through the foundation's Cyber Initiative. The foundation has now committed $65 million over the next five years to strengthening the nascent field of cybersecurity, the largest such commitment to date by a private donor.
Sandia cyber-testing contributes to DHS Transition to Practice	DHS and Sandia National Laboratories	September 10, 2014	The Transition to Practice (TTP) program helps move federally funded cybersecurity technologies into broader use. The goal is to generate interest, initiate conversations, and build relationships and business partnerships that put important cyber technologies, including some developed at Sandia, into practice.
Cybersecurity Laboratory and Cybersecurity Research Program at the Computer Research Laboratory (CRL)	Louisiana Tech University Ruston	August 2014	The CRL consists of several unique facilities that include virtualization, visualization, networking, micro-aerial vehicle and sensor networks, and field programmable gate array (FPGA) laboratories. (6 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 of articles that are often referenced in support of the idea that de-identified data sets are at risk of re-identifying individuals through linkages with other available data. It examines the ways in which the academic research referenced has been misconstrued and finds that the primary reason for the popularity of these misconceptions is not factual inaccuracies or errors within the literature but rather a tendency on the part of commentators to overstate or exaggerate the risk of re-identification. Although the research does raise important issues concerning the use of proper de-identification techniques, it does not suggest that de-identification should be abandoned. (13 pages)

Software Defined Perimeter Working Group	Cloud Security Alliance	December 1, 2013	The document explains the software defined perimeter (SDP) security framework and how it can be deployed to protect application infrastructure from network-based attacks. The SDP incorporates security standards and security concepts from organizations such as NIST and DOD into an integrated framework. (13 pages)
Resilience Metrics for Cyber Systems (Free registration required to download.)	Seager, Thomas (Arizona State University)	November 2013	Despite their national and international importance, resilience metrics to inform management decisions are still in the early stages of development. The resilience matrix framework developed by Linkov et al. is applied to develop and organize effective resilience metrics for cyber systems. These metrics link national policy goals to specific system measures such that resource allocation decisions can be translated into actionable interventions and investments. The paper proposes a generic approach and could integrate actual data, technical judgment, and literature-based measures to assess system resilience across physical, information, cognitive, and social domains. (6 pages)
A Survey of Cyber Ranges and Testbeds	Defence Science And Technology Organisation Edinburgh (Australia), Cyber And Electronic Warfare Division	October 2013	The document reviews the state-of-the-art cyber range implementations and related computer network operations testbeds. It summarizes recently published examples and describes their purpose and functionality. The compiled information should assist organizations in making an informed decision when considering a cyber-range capability. (38 pages)
20 Critical Security Controls for Effective Cyber Defense	Center for Strategic and International Studies	November 2012	The top 20 security controls were agreed upon by a consortium. Members of the consortium include NSA, the United States Computer Emergency Readiness Team, DOD's Joint Task Force-Global Network Operations, the Department of Energy Nuclear Laboratories, Department of State, DOD Cyber Crime Center, and commercial forensics experts in the banking and critical infrastructure communities. (89 pages)
SBIR Phase II: Information Security Risk Taking	NSF	January 17, 2012	The NSF is funding research on giving organizations information-security risk ratings, similar to credit ratings for individuals.

Anomaly Detection at Multiple Scales (ADAMS)	DARPA	November 9, 2011	The report describes a system for preventing leaks by seeding believable disinformation in military information systems to help identify individuals attempting to access and disseminate classified information. (74 pages)
At the Forefront of Cyber Security Research	(NSF	August 5, 2011	The Team for Research in Ubiquitous Secure Technology (TRUST) is a university and industry consortium that examines cybersecurity issues related to health care, national infrastructures, law, and other issues facing the general public.
Designing A Digital Future: Federally Funded Research And Development In Networking And Information Technology	White House	December 2010	The President's Council of Advisors on Science and Technology (PCAST) has made several recommendations in a report about the state of the government's Networking and Information Technology Research and Development (NITRD) Program. (148 pages)
Partnership for Cybersecurity Innovation	White House Office of Science and Technology Policy	December 6, 2010	The Obama Administration released a memorandum of understanding (see below) signed by NIST, DHS Science and Technology Directorate Security (S&T), and the Financial Services Sector Coordinating Council (FSSCC). The agreement aims to speed the commercialization of cybersecurity research innovations that support the nation's critical infrastructures. (10 pages)
Memorandum of Understanding (MOU)	National Institute of Standards and Technology (NIST), DHS, and Financial Services Sector Coordinating Council (FSSCC)	December 2, 2010	The document formalizes the intent of the parties to expedite the coordinated development and availability of collaborative research, development, and testing activities for cybersecurity technologies and processes based upon the financial services sector's needs. (4 pages)
Science of Cyber-Security	MITRE Corporation (JASON Program Office)	November 2010	DOD requested that JASON, a team of scientific advisors, examine the theory and practice of cybersecurity and evaluate whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach. DOD also asked JASON to identify what is needed to create a science of cybersecurity and recommend specific ways in which scientific methods can be applied. (86 pages)

American Security Challenge: Moving Innovation to Market	National Security Initiative	October 18, 2010	The objective of the American Security Challenge is to increase the visibility of innovative technology and help the commercialization process so that such technology can reach either the public or commercial marketplaces faster to protect U.S. citizens and critical assets.

Source: Highlights compiled by CRS from the sources.

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)