U.S. Army and Air Force

Cybersecurity Careers:

Information for Students

Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

> *Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*

There is no doubt that there is a great need for well trained professionals working in cybersecurity roles. These professionals are critical in both private industry and the government for the security of individuals and the nation. The U.S. Government is committed to strengthening the nation's cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity workers today as well as a strong pipeline of future cybersecurity leaders of tomorrow.

In concert with other agencies, the U.S. Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. In a manner consistent with U.S. and international law, the Department of Defense seeks to deter attacks and defend the United States against any adversary that seeks to harm U.S. national interests during times of peace, crisis, or conflict. To this end the Defense Department has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools.

The President has established principles and processes for governing cyber operations. The purpose of these principles and processes is to plan, develop, and use U.S. capabilities effectively, and to ensure that cyber operations occur in a manner consistent with the values that the United States promotes domestically and internationally.

There are growing cyber threats to U.S. interests. State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States' technological and military advantage. DoD contends that the U.S. is vulnerable in cyberspace, and the scale of the cyber threat requires urgent action by leaders and organizations across the government and the private sector.

Since developing its first cyber strategy in 2011, the DoD has made significant progress in building its cyber capabilities, developing its organizations and plans, and fostering the partnerships necessary to defend the country and its interests. More must be done. Stemming from the goals and objectives outlined in the DoD strategy, appropriate resources must be aligned and managed to ensure progress.

The DoD strategy presents an aggressive, specific plan for achieving change. For DoD to succeed in its mission of defending the United States and its interests in cyberspace, leaders from across the Department must take action to achieve the objectives outlined in the strategy. Because of the nature of networks and computer code, no single organization can be relied upon to do this work. Success requires close collaboration across DoD, between agencies of the U.S. government, with the private sector, and ith U.S. allies and partners.(1)

As high priority has been strengthening cybersecurity by creating higher education to programs to produce skilled and capable cybersecurity. DHS and The National Security Agency (NSA) jointly sponsor the National Centers of Academic Excellence (CAE) program, designating specific 2- and 4-year colleges and universities as top schools in Cyber Defense (CD). Schools are designated based on their robust degree programs and close alignment to specific cybersecurity-related knowledge units (KUs), validated by top subject matter experts in the field. CAE graduates help protect national security information systems, commercial networks, and critical information infrastructure in the private and public sectors.(2)

The National Cybersecurity Workforce Framework

The number of cybersecurity-related jobs already outpaces the number of people qualified to fill them, and that demand is growing rapidly. The Department of Homeland Security (DHS) is working with our nation's private industry, academia, and government to develop and maintain an unrivaled, globally competitive cyber workforce.

One of the biggest challenges is the lack of consistency in the way cybersecurity is defined. Job descriptions and titles for the same job roles vary from employer to employer. This makes it harder for universities and colleges to prepare students for their first job. Employers spend time and resources retraining new hires and employees do not have clear career options.

The National Cybersecurity Workforce Framework is the foundation for increasing the size and capability of the U.S. cybersecurity workforce. It provides a common definition of cybersecurity, a comprehensive list of cybersecurity tasks, and the knowledge, skills, and abilities required to perform those tasks. By using the Framework:

- Educators can create programs that are aligned to jobs.
- Students can graduate with knowledge and skills that employers need.
- Employers can recruit from a larger pool of more qualified candidates.
- Employees will have portable skills and better defined career paths and opportunities.
- Policy makers can set standards to promote workforce professionalization.

DHS partnered with industry, academia, and government to develop the Workforce Framework. It is being implement across the Federal Government and is accepted as a best practice resource

to define the field of cybersecurity. DHS has also published resources to help employers, educators, and training providers implement the Workforce Framework within their organizations and communities.(2)

The National Cybersecurity Workforce Framework provides a blueprint to categorize, organize, and describe cybersecurity work into Specialty Areas, tasks, and knowledge, skills, and abilities (KSAs). The Workforce Framework provides a common language to speak about cyber roles and jobs and helps define personal requirements in cybersecurity.

Within the Framework, there are seven Categories, each comprising of several Specialty Areas. This organizing structure is based on extensive job analyses that groups together work and workers that share common major functions, regardless of job titles or other occupational terms.

Category One) Analysis specialty areas are responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence:

- All Source Intelligence analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
- Exploitation Analysis specialists analyze collected information to identify vulnerabilities and potential for exploitation.
- Targets specialists apply current knowledge of one or more regions, countries, non-state entities, and/or technologies.

- Threat Analysis specialists identify and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Category Two) Collect and Operate areas are responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence:

- Collection Operations specialists execute collection using appropriate strategies and within the priorities established through the collection management process.
- Cyber Operations specialists perform activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
- Cyber Operations Planning specialists perform in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conduct strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Category Three) Investigate has specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence:

- Digital Forensics specialists collect, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

- Investigation specialties apply tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Category Four) Operate and Maintain has specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security:

- Customer Support specialists address problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries.
- Data Administration specialists develop and administers databases and/or data management systems that allow for the storage, query, and utilization of data.
- Knowledge Management specialists manage and administer processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
- Network Services specialists install, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
- System Administration specialists install, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and

availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

- Systems Security Analysts conduct the integration/testing, operations, and maintenance of systems security.

Category Five) Oversight and Development specialty areas provide leadership, management, direction, and/or development and advocacy so that all individuals and the organization may effectively conduct cybersecurity work:

- Education and Training specialists conduct training of personnel within pertinent subject domain. Develop, plan, coordinate, deliver and/or evaluate training courses, methods, and techniques as appropriate.
- Information Systems Security Operations (Information Systems Security Officer) oversee the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).
- Legal Advice and Advocacy specialists provide legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
- Security Program Management (Chief Information Security Officer) manages information security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel,

infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).

- Strategic Planning and Policy Development specialists apply knowledge of priorities to define an entity.

Category Six) Protect and Defend specialty areas are responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks:

- Computer Network Defense Analysts use defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
- Computer Network Defense Infrastructure Support specialists test, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
- Incident Response specialists respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats and use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
- Vulnerability Assessment and Management specialists conduct assessments of threats and vulnerabilities, determine deviations from acceptable configurations, enterprise or

local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Category Seven) Securely Provision specialty areas are concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development:

- Information Assurance Compliance specialists oversee, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's information assurance and security requirements and ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
- Software Assurance and Security Engineering specialists develop and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
- Systems Development specialists work on the development phases of the systems development lifecycle.
- Systems Requirements Planning specialists consult with customers to gather and evaluate functional requirements and translate those requirements into technical solutions while providing guidance to customers about applicability of information systems to meet business needs.
- Systems Security Architecture specialists develop system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and

environmental conditions (e.g., law and regulation) into system and security designs and processes.

- Technology Research and Development specialists conduct technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
- Test and Evaluation specialists develop and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.(3)

The U.S. Department of Defense Cyber Strategy

The May 2011 Department of Defense Strategy for Operating in Cyberspace guided the DoD cyber activities and operations in support of U.S. national interests until the strategy was updated in 2015. The updated strategy sets prioritized strategic goals and objectives for DoD's cyber activities and missions to achieve over the next five years. It focuses on building capabilities for effective cybersecurity and cyber operations to defend DoD networks, systems, and information; defend the nation against cyberattacks of significant consequence; and support operational and contingency plans. The updated strategy builds on previous decisions regarding DoD's Cyber Mission Force and cyber workforce development and provides new and specific guidance to mitigate anticipated risks and capture opportunities to strengthen U.S. national security.

As a matter of first principle, cybersecurity is a team effort within the U.S. Federal government. To succeed in its missions the DoD must operate in partnership with other Departments and Agencies, international allies and partners, state and local governments, and, most importantly, the private sector.

To support its missions in cyberspace, the DoD conducts a range of activities outside of cyberspace to improve collective cybersecurity and protect U.S. interests. For example, the DoD cooperates with agencies of the U.S government, with the private sector, and with international partners to share information, build alliances and partnerships, and foster norms of responsible behavior to improve global strategic stability.

DoD seeks to share information and coordinate with U.S. government agencies in an integrated fashion on a range of cyber activities. For example, if DoD learns of malicious cyber activities that will affect important U.S. networks and systems that are vital for U.S. national and economic security or public safety, DoD supports agencies like the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) as they reach out to U.S. entities, and often other countries, to share threat information such as technical indicators of a potential attack. Such information sharing can significantly improve an organization's ability to defend itself against a broad range of cyber attacks. In addition to sharing information, DoD partners with other agencies of the U.S. government to synchronize operations and to share lessons-learned and cybersecurity best practices. This includes incident management and network defense response.

From application developers to Internet Services Providers, private companies provide the goods and services that make up cyberspace. The DoD relies on the private sector to build its networks, provide cybersecurity services, and research and develop advanced capabilities. The DoD has benefited from private sector innovation throughout its history. Going forward, DoD will work closely with the private sector to validate and commercialize new ideas for cybersecurity for the Department.

The Defense Department engages in a broad array of activities to improve cybersecurity and cyber operations capacity abroad. DoD helps U.S. allies and partners to understand the cyber threats they face and to build the cyber capabilities necessary to defend their networks and data. Allies and partners also often have complementary capabilities that can augment those of the

United States, and the United States seeks to build strong alliances and coalitions to counter potential adversaries' cyber activities. Strategically, a unified coalition sends a message that the United States and its allies and partners are aligned in collective defense. In addition to the Five Eyes treaty partners, DoD works closely with key partners in the Middle East, the Asia-Pacific, and Europe to understand the cybersecurity environment and build cyber defense capacity.

Three Primary Missions in Cyberspace

The Defense Department has three primary cyber missions. **First, DoD must defend its own networks, systems, and information.** The U.S. military's dependence on cyberspace for its operations led the Secretary of Defense in 2011 to declare cyberspace as an operational domain for purposes of organizing, training, and equipping U.S. military forces. The Defense Department must be able to secure its own networks against attack and recover quickly if security measures fail. To this end, DoD conducts network defense operations on an ongoing basis to securely operate the Department of Defense Information Network (DoDIN). If and when DoD detects indications of hostile activity within its networks, DoD has quick-response capabilities to close or mitigate vulnerabilities and secure its networks and systems. Network defense operations on DoD networks constitute the vast majority of DoD's operations in cyberspace.

In addition to defense investments, DoD must prepare and be ready to operate in an environment where access to cyberspace is contested. During the Cold War, forces prepared to operate in an environment where access to communications could be interrupted by the adversary's advanced capabilities, to include the potential use of an electromagnetic pulse that could disrupt satellite