Career Opportunities in CYBERSECURITY

Description of the Field
Cybersecurity, also referred to as information technology (IT) security or computer security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. During a Senate hearing in March 2013, the nation’s top intelligence officials warned that cyber attacks and digital spying are the top threat to national security, eclipsing terrorism.

Career Paths
SIPA graduates can follow one of four or five career paths. Threat Intelligence, Government Relations, Cyber Policy, Tech Policy or Risk Management. All areas value SIPA graduates writing and analytic skills and understanding of international affairs and public policy. In Threat Intelligence, a cyber threat analyst uses public or secret information to analyze and assess cyber threat actors. In Government Relations a Director of government affairs helps companies understand new government cyber related policies, technologies and the company’s position. In Cyber Policy, a cyber policy analyst/researcher will research, analyze and write on major issues in cyber policy, especially defense and international affairs. In Tech Policy, a technology analyst/researcher will research, analyze and write on major issues in digital technologies and their impact. Threat Intelligence and Cyber Policy focus on espionage and intelligence as well as conflict and warfare. Threat Intelligence also looks for area and language specialization. China, Russia, Iran and North Korea regional expertise along with Chinese, Russian, Arabic, Korean, Hebrew and Portuguese languages are all highly sought after. Government Relations and Tech Policy share a focus on international relations and public policy, privacy and internet governance. Government Relations looks at Cybersecurity policy while Tech Policy looks at digital rights and the digital divide.

Obtaining a job – Internships are always a smart way to make connections and try to land a full time offer. For Threat Intelligence and Government Relations Interning at (threat) companies, applying online and informational interviews are all beneficial. For all paths except Threat Intelligence Schedule C government appointments are a smart choice. For both Cyber and Tech Policy jobs interning in governments or for think tanks, publishing op-eds and articles are all recommended.

QUALIFICATIONS TO ENTER THE FIELD
Qualifications vary depending on the organization and job function:

+ Analytical skills, both qualitative and quantitative
+ Ability to clearly articulate complex concepts both written and verbally
+ Knowledge and analysis of policy, trends and intelligence
+ Understanding of international affairs, public policy, security studies and the way the world works
+ Technical understanding
+ Area and language specialization
+ Problem solving skills
+ Demonstrated skills in innovation and collaboration
+ Eagerness to dig into technical questions and examine them from all sides
+ Organize events and manage projects for entry-level positions in Cyber and Tech policy jobs
+ Internet governance
+ Capacity development

Updated 7/17
Demand
As the demands of global business, computing and society revolve around information technology, the cybersecurity workload is increasing faster than cybersecurity professionals can meet the demand. The cybersecurity workforce shortage is expected to reach 1.5 million unfilled positions by 2019.

The top locations for cybersecurity jobs are in Washington DC, New York, London and San Francisco.

The top industries for cybersecurity professionals are:
- Banking/Finance/Big 4 Accounting/Insurance
- Information Technology/Management
- Government (Defense)
- Government (Nondefense)
- Consulting/Professional Services
- Dedicated Cybersecurity companies

Sample Group of Employers
Government Programs
- Commerce NTIA [https://www.ntia.doc.gov/]
- Federal Bureau of Investigation – Cybercrime [www.fbi.gov/]
- NYPD Intelligence Division [www.nypdintelligence.com]
- State Department [http://www.state.gov/]

Private Firms – Financial Institutions, Major Tech + Security Companies
- Booz Allen Hamilton [www.boozallen.com]
- Citi Cyber Fusion Center [http://www.citigroup.com/citi/]
- CACI [www.caci.com]
- CrowdStrike [www.crowdstrike.com/]
- Endgame, Inc. [www.endgame.com]
- FireEye [https://www.fireeye.com/]
- Flashpoint [https://www.flashpoint-intel.com/]
- iSight Partners [www.isightpartners.com]
- IT Security, Inc. [www.it-security-inc.com]
- K2 Intelligence [www.k2intelligence.com]
- Palantir Technologies, Inc. [www.palantir.com]

Think Tanks
- Atlantic Council [www.atlanticcouncil.org]
- Council on Foreign Relations [www.cfr.org]
- CSIS [www.csis.org]
- East-West Institute [https://www.eastwest.ngo/]
- New America [www.newamerica.org]

Non-profits
- Access Now [https://www.accesnow.org/]

FUTURE CHALLENGES OF THE PROFESSION
The workload is increasing faster than cybersecurity professionals can meet the demand. Cybersecurity is projected to be a $170 Billion market by 2020.

Cybersecurity is the most important technological and societal security challenge over the next 3-5 years, particularly as new cyber threats emerge, network-connected devises from the “Internet of everything,” and legal frameworks and social norms about cybersecurity evolve in new directions.
Cyber Skill Development Curriculum

Interested in a job in cyber issues but you don’t know much about the technology? This curriculum is for you. All the courses are online, free and listed roughly in order of how they should be taken.

At a minimum, take CS101 from Coursera. It doesn’t take long and covers the basics you’ll need. Another option is to just dive into CS50x, since that will cover most of the basics but it is a large time commitment.

Foundations

- Basic computer science: https://www.coursera.org/course/cs101
- History of the Internet: https://www.coursera.org/learn/internet-history
- Networks: https://www.coursera.org/course/comnetworks
- Security: https://www.coursera.org/course/security
- The Law: https://www.coursera.org/course/surveillance

Next Steps: Learn to Code

- C (highly recommended): https://www.edx.org/course/introduction-computer-science-harvardx-cs50x
- Python:
  - https://www.coursera.org/learn/python
  - https://www.edx.org/course/introduction-computer-science-mitx-6-00-1x-5tps://www.codecademy.com/tracks/python

Become a Cyber Ninja:

- Cybersecurity Fundamentals: https://www.coursera.org/specializations/cybersecurity?utm_medium=medium
- Crypto:
  - https://www.coursera.org/course/crypto
  - https://www.coursera.org/course/crypto2
- Hardware/Software Interaction: https://www.coursera.org/course/hwswinterface
- The Future of Networking: https://www.coursera.org/course/sdn1

In addition to the offerings above, consider enrolling and completing one or more of Udacity’s nano degrees: A very desirable combination is these two:

- Intro to Programming: https://www.udacity.com/course/intro-to-programming-nanodegree--nd000
- Data Analyst https://www.udacity.com/course/data-analyst-nanodegree--nd002

News Sources and Publications

- Twitter
- Wired Magazine