**Cybersecurity Jobs for SIPA Grads**

**What You’ll Do**
- Use open-source and proprietary data to analyze and investigate cyber threats
- Perform strategic, operational, and tactical research and analysis of adversarial cyber threat and threat actors
- Use tools and best practices to track the tools, techniques, and procedures of APTs
- Relay information to stakeholders through written reports and verbal briefings

**Threat Intelligence**
- Develop and analyze data solutions that protect the confidentiality, integrity, and availability of assets
- Analyze and present the most important business risks (and opportunities) based on company particular and offer recommendations
- Plan and manage the execution and delivery of risk-based cyber assessments
- Ensure compliance with current cybersecurity regulations, policies, and standards

**Business Cyber Risk**
- Develop, research, analyze and write on major issues in cyber policy, especially defense, risk and international affairs
- Design and author research products, op-eds, provide thoughtful analysis on current events
- Monitor scholarly developments and policy statements
- Especially at entry-level, organize events and manage projects

**Cyber Policy**
- Engaging with governments and civil society to share understandings around new technologies
- Researching cyber security trends and technology globally and in the region
- Support the development of partnerships with government stakeholders and customers
- Stay up-to-date on upcoming legislation which may involve advocacy and lobbying with government entities

**Government Relations**
- Research, analyze and write on major issues in digital and technology policy, especially defense and international affairs
- Comment through research papers, op-eds, and media engagements on current events
- Monitor scholarly developments and policy statements
- Especially at entry-level, organize events and manage projects

**Tech and Digital Policy**
- Monitor and mitigate abusive activity including harmful content, theft, fraud, online abuse and other policy violations
- Triage, prevent and respond to Trust and Safety related incidents and reports
- Utilize information platforms for analyzing and identifying the tactics, techniques and patterns of abusive users
- Develop guidelines and policies around online content moderation, privacy, and user safety

**Why a SIPA Graduate?**
- You will apply your understanding of geopolitics, intelligence and policy to contextualize activity
- You will be able to better understand adversary behavior from a financial or security perspective
- You will be better positioned to communicate concerns to non-technical stakeholders
- You will hold an advantage if you have programming or data analysis skills

**Useful Certifications**
- (ISC)2 Certified in Cybersecurity
- Google Cybersecurity Certificate
- CompTIA Security+
- AWS Certified Cloud Practitioner
- Splunk Level 1
- Shodan
- WireShark
- Python
- SQL
- R
- Maltego
- Excel

**Skills to Improve**
- Policy Analyst
- Political Risk Analyst
- Public Policy Manager
- Program Manager, Government Affairs
- Lead, Government Affairs
- Policy Analyst
- Tech Policy Fellow
- Technology Reporter
- Digital and Technology Policy Advisor
- Program Assistant at Think Tank

**Places to Work**
- Google, Microsoft, Intuit, Booz Allen Hamilton

**Recommended Courses**
- INAF U6509 Basics of Cybersecurity
- INAF U6523 Cyber Risks and Vulnerabilities
- INAF U6833 Foundations of Cyber Conflict
- INAF U6502 Intro to Text Analysis in Python
- INAF U8412 Intelligence and Foreign Policy
- INAF U6832 International Intelligence Systems
- INAF U6829 Global Financial Services in the 21st Century

**Skills to Improve**
- Intel & Data Analysis
- Tech Writing, Briefing

**Useful Certifications & Technical Skills**
- (ISC)2 Certified in Cybersecurity
- Google Cybersecurity Certificate
- CompTIA Security+
- AWS Certified Cloud Practitioner
- Splunk Level 1
- Shodan
- WireShark
- Python
- SQL
- Maltego
- Excel

*Updated as of July 2023*