IDB | INSTITUTE FOR DEFENSE & BUSINESS

KELLEY SCHOOL OF BUSINESS
Kelley Executive Partners

MANAGING CYBER RISK IN THE NATIONAL SECURITY CONTEXT:

Exploring the Strategic Challenges and Opportunities of Emerging Technologies

Basic cybersecurity literacy is becoming increasingly vital. Cyber attackers, ranging from hacktivists to organized crime networks and even nation states, are targeting vulnerable networks and are frequently successful in stealing funds, breaching critical infrastructure, as well as valuable intellectual property. There is a growing call from the White House, Congress, and industry groups to put in place cybersecurity best practices to better manage the multifaceted cyber threat facing the private sector. However, it is not always clear what those practices should be, or how to implement them in a dynamic, global regulatory environment. This program hosted by the Institute for Defense and Business in partnership with Indiana University's Kelley School of Business is a spin-off of the IU-IDB Strategic Studies Program (2015 - 2018 SBS) and is designed to introduce participants to the multifaceted strategic cyber risks facing the United States with a special focus on harnessing the benefits, while mitigating the risks, of emerging technologies in the national security context from a non military lens.

Learning Objectives

After successfully completing this Program, participants will:

- Better understand the multifaceted cyber threat facing the public and private sectors
- Be equipped with a toolbox of cybersecurity best practices designed to manage cyber risk exposure
- Have a firm introduction to both U.S. and comparative cybersecurity law and policy
- Know the contours of important cybersecurity debates such as the appropriate role of government in safeguarding critical infrastructure, analyzing the benefits and drawbacks of active defense, and how to manage risks and opportunities in the expanding Internet of Things
- Situate U.S. efforts at enhancing cybersecurity in a global context, and be aware of how other jurisdictions are regulating this space
- Further develop the confidence necessary to work well collaboratively on interdisciplinary cybersecurity solutions

Program Overview

This program consists of six highly interactive synchronous sessions, once per week with asynchronous work in between, and includes both practical exercises and a final project.

There will be a Kickoff on May 10 with each session taking place on Friday mornings from 8:00 - 12:00 EDT for six consecutive weeks. The breakdown of topics is as follows:

Week 1: ***Orientation, Introductions, and Understanding the Multifaceted Cyber Threat***

- The session will commence with an orientation, including introductions, and a capstone project launch.
- The session will continue with coverage of the three dimension of cybersecurity risk management (business, technical, and legal) and discuss the multi-faceted cyber threat along with hot topics like critical infrastructure protection and deterrence.
- The session will conclude by introducing best practices for managing cyber conflict, securing access to the global commons, and provide an introduction to international cybersecurity law and policy.

Week 2: ***Artificial Intelligence (AI) & Machine Learning (ML)***

- The session will introduce AI and ML with a focus on issues of both use and governance.
- The session will then feature a discussion of comparative AI governance with special reference to autonomous weapons systems, along with an array of hot topics in AI and ML, including deep fakes and how AI can help make democracy harder to hack.
- Finally, the session will also cover the related active defense debate, including the controversies surrounding private sector hack back, and feature guest commentary from leading AI thinkers and practitioners.

Week 3: ***Internet of Things & SG***

- The Internet of Things (IoT) is the notion that nearly everything we use, from gym shorts to streetlights, will soon be connected to the Internet. Industry and financial analysts have predicted that the number of Internet-enabled devices will increase from 11 billion to upwards of 75 billion by the end of 2020. Regardless of the number, the end result looks to be a mind-boggling explosion in Internet connected stuff. Yet, there has been relatively little attention paid to how we should go about regulating smart devices, and still less about how cybersecurity should be enhanced. Similarly, now that everything from refrigerators to stock exchanges can be connected to a ubiquitous Internet, how can we better safeguard privacy across networks and borders? This session will explore these issues, and more.
- The 5G debate in particular is intimately related to the realization of the so-called Internet of Everything. We will cover the economic, political, military, and Internet governance implications of this ongoing dispute, along with its potential to touch off a true digital Cold War.

Week 4: ***Securing Smart Cities***

- IU, and the Ostrom Workshop in particular, is a leading home for smart cities research having hosted a series of workshops on the topic in collaboration with Virginia Tech, Villanova, and Georgia Tech. This session will leverage this background and network by introducing participants to the security, privacy, and governance challenges in the smart city context, which is an ideal case study to see how these various cybersecurity hot topics are playing out in the real world.
- Tie in China's Belt and Road initiative, which has dozens of smart cities initiatives, which will build from the AI and 5G discussions from previous weeks

Week 5: ***Cybersecurity, Privacy, & the Pandemic***

- The session will explore the changing conceptions of privacy, including by exploring regulatory trends including the California Consumer Protection Act (CCPA) and the EU's General Data Protection Regulation (GDPR), in the face of the COVID-19 pandemic.
- We will also ascertain how the pandemic is already influencing global cybersecurity debates across the cyber powers.

Week 6: ***Supply Chain Security, Blockchain, & Capstone Presentations***

- The sessions will set the stage with coverage of logistics and managing supply chain risk from cyber-attacks as well as natural disasters, along with covering procurement best practices.
- We will also cover related cybersecurity norm building efforts as they pertain to promoting cyber peace.
- The session will conclude with a National Security Council simulation, along with capstone project presentations.

Format

The webinar series will be held once per week on Tuesday afternoons (EDT). In addition to the live sessions, supplemental content will be provided in the form of (1) targeted (short) weekly readings, and (2) supplemental readings and asynchronous discussion forums, along with live simulations.

Team

IDB Program Director: Zebrina L. Warner

- 16 Years Executive Education and Curriculum Development Experience
- Created and led three Strategic Broadening Seminars
- Areas of focus: Strategic Thinking and Decision Making, National Security, Transnational Threats, Cybersecurity, and Dense Urban Areas
- MS, Strategic Management, Indiana University Kelley School of Business (online)
- MBA, Indiana University Kelley School of Business (online)
- BS, Journalism, University of North Carolina at Chapel Hill
- ICF Coaching Certification

Core Faculty Lead: Professor Scott J. Shackelford

- Cybersecurity Program Chair and Executive Director of the Ostrom Workshop at Indiana University
- Affiliated Scholar Harvard Kennedy School's Belfer Center for Science and International Affairs and Stanford's Center for Internet and Society
- Senior Fellow at the Center for Applied Cybersecurity Research
- Author of more than 100 articles, book chapters, essays, and op-eds
- Author, Governing New Frontiers in the Information Age: Toward Cyber Peace (Cambridge University Press, 2020), The Internet of Things: What Everyone Needs to Know (Oxford University Press, 2020), and Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace (Cambridge University Press, 2014)
- Recipient of numerous awards, including a Harvard University Research Fellowship, a Stanford University Hoover Institution National Fellowship, a Notre Dame Institute for Advanced Study Distinguished Fellowship, the 2014 Indiana University Outstanding Junior Faculty Award, and the 2015 Elinor Ostrom Award.

Summary and Participant Information

After successful completion of these requirements, participants are eligible for an IU-IDB executive certificate and digital badge for their social media profiles like LinkedIn.

UPCOMING PROGRAM DATES:
May 10 - June 18, 2021

WHO SHOULD ATTEND:
Career Levels of 0-2 to 0-4, W-1 to W-3, E-7 to E-9, GS11-GS-13. Early Career Professionals from Private Industry

TUITION: $5,000

Updated:3/3/21

Professionals and organizations interested in this programshould contact IDB's Customer Advocate, Mike Bogdahn, at bogdahn@idb.org or (760) 577-8324 for enrollment information

Please note: Program sessions, faculty, dates, and pricing included above, although current at the time of publication are subject to change.