Permalink

W4-A: Roundtable: Taking [some of] the Wicked out of the Cyber Problem

Wed, December 13
3:30 PM - 5:00 PM
Potomac Ballroom Salon I
Conference Center
Roundtable

Renaissance Hotel, 999 9th St., NW, Washington, DC

Info

Title:
Taking [some of] the Wicked out of the Cyber Problem

Theme: Emerging Technologies
Primary specialty group: Applied Risk Management
Other specialty groups: Security and Defense, Economics and Benefits Analysis, Decision Analysis and Risk, Risk Policy and Law
Application / Topics: cybersecurity, digital environment, Web3, public safety/security, regulatory and policy development

Description:

The concept of the “wicked problem” was introduced decades ago to characterize the complexity of applying science to policy, with different stakeholder valuations, complex causes, changing definitions of causation and success – to name a few issues. https://www.sympoetic.net/Managing_Complexity/complexity_files/1973%20Rittel%20and%20Webber%20Wicked%20Problems.pdf Cybersecurity is indeed a wicked problem. It has been primarily viewed a problem that users of information and communications technology (ICT) have to manage through having stronger security and more resiliency to reduce consequences of inevitable incidents. Few have been dealing with the nature of insecurities inherent in cyberspace and the threat itself. Some insecure aspects of ICT appear to be changing as demands increase for ICT firms to provide “security by design” and to be accountable, to some extent, for their products/services' security. Thus, vulnerabilities are just starting to be better assessed/managed. However, less attention has been paid to the underlying issue of malicious actors and how to affect their capacity, capability and intent. This roundtable will consider how cybersecurity can become less of a *wicked* problem.

Other areas of international risk have been considered wicked problems but have been managed by the international community. The Stimson Center, a nonpartisan DC-based think tank working on international security issues, has undertaken a project to look at some other areas of international risk - from chlorofluorocarbons to dual-use materials – to consider lessons (including decision processes) that could be translated to better managing cyberspace, with a focus on accountability. One of the lessons emerging is the importance of detailed risk assessments with stakeholder input and valuations, something cyberspace has generally lacked.

This interactive session will include discussions among panelists and with the audience on:

- How better to apply some of Stimson's project findings (see: https://www.stimson.org/project/cyber-accountability/), what other risk areas could help inform the research, whether other emerging technologies might learn from the examples
- How risk management drives international law, norms, policy and regulations, including through regional/industry leadership, and how to better promote sound risk governance
- Efforts by governments to take a proactive approach to risk assessment and management, including by changing the benefit/cost judgments of threat actors.

Panelists:

Dean Rosa Celorio, Associate Dean and Distinguished Lecturer for International and Comparative Legal Studies, George Washington University Law School. In this capacity, she directs the International Law program and teaches courses in the areas of international law, human rights, and constitutional law. Dean Celorio currently serves on the Executive Council of the American Society of International Law and as a Member of the World Health Organization Global Advisory Committee on Maternal Health Issues. https://www.law.gwu.edu/rosa-celorio

Dr. Christopher Ford is visiting fellow at the Hoover Institution and Visiting Professor with Missouri State University's Graduate Department of Defense and Strategic Studies. Previously, as a MITRE Fellow, he was founding Director of the Center for Strategic Competition. From 2018 until 2021, Dr. Ford served as Assistant Secretary of State for International Security and Nonproliferation, also exercising the authorities of Under Secretary for Arms Control and International Security. Earlier, he served as Special Assistant to the President and Senior Director for Weapons of Mass Destruction and Counterproliferation at the U.S. National Security Council. https://www.hoover.org/profiles/christopher-ford; https://www.newparadigmsforum.com/

Dr. Fabio Massacci is full Professor in Computer Science, University of Trento and chair of Security at the Vrije Universiteit, Amsterdam. He chairs SRA's Security and Defense Specialty Group. He is Associate Editor-in-Chief of IEEE Security & Privacy. https://www.computer.org/csdl/magazine/sp. He is member of the CVSS SIG, the world industry standard on vulnerability assessment. He works on cyber attackers, advanced persistent threats (APTs), security economics, and risk reduction/vulnerability assessments. https://fabiomassacci.github.io

Dr. Unal Tatar is Assistant Professor at the State University of New York at Albany's Cybersecurity Department and the chair Committee of SRA's Economics and Benefits Analysis Specialty Group. Most recently, he served as the head of the National Computer Emergency Response Team of Turkey (TR-CERT) coordinating cybersecurity exercises and helping create Turkey's first national cybersecurity strategy. He has assisted initiatives such as the NATO Center of Excellence Defense Against Terrorism (COE-DAT). https://www.albany.edu/cehc/faculty/unal-tatar

Panel Moderator, **Debra Decker,** SRA member since 2008, Senior Advisor Stimson Center, strategy and risk consultant. https://www.stimson.org/ppl/decker/