Location: 1010 Dow Engineering Building (North Campus).

Co-taught with Dr. Carl Landwehr, Lead Research Scientist, Cyber Security Policy & Research Institute, George Washington University.

Future leaders will need to understand the science, technology, and human considerations behind cybersecurity well enough to make informed decisions when provided advice and options for action. Over the last decade cybersecurity issues have risen in prominence from a U.S. national security perspective, as well as from the perspective of individuals and organizations. There have been near daily reports regarding cyber operations launched by nation states, hacking groups, criminal organizations, and individuals against a variety of targets, using different tools and methods, and with different effects. Technology has accelerated the rate of cyber operations, enabling those intent on using cyber tools for a variety of malign purposes. The U.S. government has also attempted to reorganize and reorient towards this multi-dimensional threat, in addition to private industry, state and local governments, and academia—but there are still a number of gaps and vulnerabilities that deserve technical and policy attention and solutions.

This class will examine the broad landscape of cybersecurity from both a technical and policy perspective. It will introduce fundamental concepts of computing and cyber security, including information theory, computability, cryptography, networking fundamentals, how vulnerabilities arise, and how attacks work. In addition, it will explore foundational ideas including definitions, cyber norms, and ethics; identify existing U.S. laws, authorities and governmental constructs; and frame classic security concepts like deterrence, attribution, offense, defense, and retaliation. The course will also involve guest speakers, short writing assignments designed to capture technical or policy insights, policy papers designed to explore alternative views on different cybersecurity topics, and simulated National Security Council policy meetings where students assume different interagency roles and examine potential courses of action.

The objectives of the course include:

1. Enhancing knowledge on technical and policy aspects of cybersecurity.
2. Sharpening critical thinking, executive briefing, and team collaboration skills.
3. Understanding real-world implications of cyber operations.
4. Identifying possible solutions or opportunities to address existing cybersecurity challenges.