WATSON INSTITUTE
INTERNATIONAL & PUBLIC AFFAIRS
BROWN UNIVERSITY

Surveying the Cyber Threat Landscape and Protecting the United States Against Cyberattacks of Significant Consequence

Spring 2023
Rep. James R. Langevin
Senior Fellow, Watson Institute
Session Dates: February 15, March 1, March 15, April 5, April 19

Overview

The United States is one of the most comprehensively interconnected nations in the world. The rapid and extensive adoption of the Internet and the development of digital networks connecting nearly every aspect of our daily lives has revolutionized our society and delivered innumerable benefits to all Americans.

The Internet, however, was not built with security in mind, and the widespread expansion of digital connectivity into nearly every facet of our society has left the United States highly vulnerable to cyberattacks. Hackers exploit this vulnerability to defraud individuals and businesses out of billions of dollars annually, compromise terabytes of highly sensitive information, steal trillions of dollars of intellectual property, and even disrupt the reliable operations of our critical infrastructure, potentially threatening the continuity of our economy and the lives of Americans throughout the nation.

While the cyber threat landscape is dynamic and ever-changing, many of the challenges we face in cyberspace are not new, nor can they be solved through technical means alone. Making cyberspace more secure for Americans also requires policy solutions that develop new partnerships, establish appropriate incentives, and enact long-needed structural reforms that collectively enable a more comprehensive and coordinated national cybersecurity effort. Equally essential is the development of a robust and skilled cybersecurity workforce to enact the cybersecurity solutions that the country needs.

These concepts became central to my work as a member of Congress over the past twenty-two years, and I hope to use this study group to explore them with you. We will learn about the risks facing our country in cyberspace, how they have developed, and why some have continued to persist for decades. We will examine cybersecurity as a whole-of-nation effort, and consider where to vest responsibility in mitigating these risks. We will explore the shared responsibility between the federal government and the private sector in securing our nation and its critical infrastructure from cyberattacks. We will consider how the U.S. can work internationally to secure ourselves and our allies in a globalized information ecosystem. And we will think through the strategic priorities that should guide the next generation of policymakers that will be focusing on these problems.

Course Expectations

This course will take place over five sessions of ninety minutes. Each session will feature remarks, either from myself or from one of the cyber policy leaders who have been invited to guest lecture one of our sessions. However, this study group places a priority on discussion, and students can expect that at least half of each class will be dedicated to open conversation on the concepts covered during the lecture and in any suggested readings.

Course Schedule

Session #1: Cybersecurity and the Cyber Threat Landscape

Our first session will begin with some introductions and background information about the course, and also about my own journey into cybersecurity. We will then discuss how interconnected information systems have come to support nearly every facet of our daily life, and how the vulnerabilities within these systems has made cybersecurity one of the preeminent national and economic security challenges of our time.

We will survey the threat actors who target individuals, businesses, organizations, and critical infrastructure using cyber means; the vulnerabilities they exploit and the tactics they use to exploit them; and the consequences of the cyberattacks they launch.

Session #2: Organization and Structure for Cyber Policymaking

Building upon our understanding of cybersecurity risks to the nation, our second session will explore how the U.S. government is organized to take action and enact policy that mitigates these risks. We will focus on the roles and responsibilities of the legislative and executive branches, identifying the committees, departments, agencies, and offices with responsibilities for our nation's cybersecurity, and how they interact with one another. Think of it as an overview of the pieces on the chessboard, and how they are allowed to move.

Alongside that overview, we will also survey key policy and strategy developments from recent years which either directly shaped the government's current authorities and resources for cyber policymaking or represented important examples of success – or failure – in the use of those authorities and resources.

For this session, we will be joined by Rear Admiral (Ret.) Mark Montgomery, Senior Director of the Center on Cyber and Technology Innovation at the Foundation for the Defense of Democracies, Executive Director of CSC 2.0, former Executive Director of the Cyberspace Solarium Commission, and former Policy Director for the Senate Armed Services Committee.

Session #3: Shared Responsibility in Cyberspace

This session will focus on the concept of "shared responsibility" in cyberspace, and the necessity of federal partnerships with private sector entities and state, local, tribal, and territorial (SLTT) governments to bolster cybersecurity. We will be joined by a senior representative from the Cybersecurity and Infrastructure Security Agency (CISA), the federal agency primarily responsible for critical infrastructure resilience and the defense of the Federal "dot gov". As part of its mission, CISA coordinates closely with SLTT governments and plays a central role in the development of public-private cybersecurity partnerships.

We will discuss the various responsibilities that CISA, other federal agencies, SLTT governments, private sector stakeholders, and individuals bear as they collaborate to secure our society from cyber threats. We will also discuss the specific policy challenges and imperatives associated with securing elections infrastructure.

Session #4: Shaping International Behavior and Defending Forward

Cybersecurity is fundamentally a global problem that negates many of the United States' traditional national security advantages, including having friendly neighbors to the north and south and thousands of miles of ocean to the east and west. Our globalized information infrastructure allows threat actors to reach out from anywhere in the world and target systems in the United States.

Our allies and partners are equally vulnerable in cyberspace, and in this session, we will discuss the necessity of working internationally with them to counter cyber threats and irresponsible state behavior. Part of this focus will be diplomatic; we will examine the role of the State Department and other U.S. government stakeholders in contributing to the development of cyber norms, the attribution of cyberattacks, and the activities of international standards-setting bodies.

We will also examine the military domain – specifically, the strategy of "defending forward" and the work undertaken by U.S. Cyber Command to support that strategy through offensive cyber operations.

Session #5: Where Do We Go From Here?

In this final session, we will be joined by a senior representative from the Office of the National Cyber Director, the federal entity with primary responsibility for the development of a soon-to-be-released National Cyber Strategy.

Alongside our guest lecturer, we will look ahead to discuss and debate the strategic priorities that should support our country's cybersecurity efforts in the coming years. How do we build a society in which cyber threat actors have to beat all of us, to beat one of us? What policy objectives should guide us, and how do we determine who should implement those objectives? And, on an individual level, what should each of us be doing in our daily lives to build a more secure cyber ecosystem not only for ourselves, but also for our society and the world at large?

About the Instructor

Rep. James R. Langevin served in the United States House of Representatives from 2001-2023, representing the second district of Rhode Island. He was a senior member of the House Armed Services Committee, where he served as the Chairman of the Cybersecurity, Innovative Technologies, and Information Systems Subcommittee. He was also a founding and senior member of the House Committee on Homeland Security.

A national leader on securing our nation's technology infrastructure against cyber threats, Langevin co-founded and co-chaired the Congressional Cybersecurity Caucus to increase awareness around the issue and served as a commissioner on the Cyberspace Solarium Commission, which was charged by Congress with developing a strategic approach to defending the United States against cyberattacks of significant consequence. He also co-chaired the Center for Strategic and International Studies (CSIS) Commission on Cyber Security for the 44th Presidency.