Atlantic Council

BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

Cyber Statecraft Initiative

The Cyber Statecraft Initiative examines the intersection of cybersecurity and public safety. Societies' dependence on connected technology is growing faster than their ability to secure it, especially in areas impacting human life, national security, and confidence in key markets, at home and abroad. We collaborate among diverse stakeholder groups, including policymakers, security researchers, industry, regulators, and others around the globe to ensure the technology we depend on is trustworthy.

OUR MISSION AND VISION

Our mission is to strengthen global prosperity and security by developing and promoting cyber safety strategies and policies for trustworthy connected technology. Our vision is to make the world safer, sooner, together.

OUR CORE STRATEGY

The Cyber Statecraft Initiative anticipates future cyber safety issues and facilitates public policy discussions, investigates national security and international policy implications of cybersecurity's public safety impacts, and examines new approaches to emerging problems in the field. The Initiative brings together a diverse network of respected experts, bridging the gap between the technical and policy communities.

Student team presenting in the semifinals of the 2016 US Cyber 9/12 Challenge in Washington, DC.

Bits and Bytes meet Flesh and Blood: A Safety Focus on Cybersecurity

To bring cyber safety into national and global public policy discussions as a distinct issue from cyber war, norms and treaties, corporate financial impacts, privacy, and data loss. We will no longer measure cybersecurity failure simply in terms of financial losses; now, consequences impact human life, public safety, market confidence, and national security. Our shared goal of avoiding these impacts and the shared weaknesses of technological dependence can help create unity in the international community, strengthen partnerships, and broker new alliances.

Emerging Actors and Increasing Capabilities

To examine new classes of actors, their capabilities, and their impact on national security and global prosperity. New technologies and new dependencies give rise to new classes of actors. We will draw from the Atlantic Council's extensive work on innovative national security strategies, such as *Dynamic Stability* (2015), to account for these new conditions and expand their relevance.

Radically Different Cybersecurity Strategies and Policy Alternatives

To investigate and model strategies and policies that dramatically improve national and global cybersecurity postures and resilience. Cyber safety fundamentally differs from enterprise IT security. Consequently, we must develop radically different strategic and policy approaches that are both safe and effective in the new environment.

CYBER STATECRAFT INITIATIVE BY THE NUMBERS IN 2016

GLOBAL ENGAGEMENT IN TENS OF DIFFERENT COUNTRIES AND CITIES INCLUDING LONDON, NEW YORK, BERLIN, BOSTON, ABU DHABI AND SINGAPORE

50+
PUBLIC AND PRIVATE EVENTS IN POLICY, TECHNOLOGY, AND ECONOMIC HUBS

100+
BRIEFINGS WITH U.S. EXECUTIVE AND LEGISLATIVE BRANCH

100+
BRIEFINGS WITH CORPORATE AND EXECUTIVE MEMBERS

PUBLIC POLICY IMPACT IN 2016

IN 2016, OUR WORK WAS REFLECTED IN OVER A DOZEN DIFFERENT GOVERNMENT REPORTS AND GUIDELINES

- PRESIDENTIAL COMMISSIONS REPORT
- DOC/NTIA GUIDANCE
- DHS GUIDELINES
- FTC GUIDELINES
- FDA GUIDELINES
- DOD POLICY
- DOD POLICY
- NHTSA GUIDANCE
- CONGRESSIONAL LETTERS
- HHS TASK FORCE
- EU GUIDANCE
- DOT PRINCIPLES

Cyber Crisis Scenarios

To investigate and develop capabilities to respond to cyber crises, and develop a future cybersecurity workforce both nationally and globally. The Cyber Statecraft Initiative has a robust capability and strong brand in cyber crisis exercises, particularly with our flagship annual Cyber 9/12 Student Challenges. In addition, we will initiate a first-of-its-kind cyber crisis event series in 2017, focusing on healthcare cyber safety, along with hosting private events with corporate, government, and foundation partners. To date, over 700 students and over 200 policymakers, corporate representatives, academics, and other global leaders have participated in these simulation exercises.

Former President of Estonia Toomas Hendrik Ilves speaks at an Atlantic Council reception following the launch of the *Tallinn Manual 2.0.*

Hacking Technical Literacy: A Knowledge Project

To bridge the divide between cybersecurity and policy, by building a repository of collective knowledge that allows Washington, DC and Silicon Valley to connect. The majority of policymakers and corporate leaders have little to no cybersecurity background and lack accessible, consistent, credible cybersecurity advice. The Knowledge Project engages the policymaking community with easily digestible, technically literate cybersecurity concepts to close the cognitive cultural gap. This project leverages a diverse network of expertise to experiment with fresh, innovative techniques that will explosively expand reach and impact.

Mobilizing Resources and Playing to Our Strengths

To draw on the Atlantic Council's strengths and resources in accomplishing our goals. The Cyber Statecraft Initiative's deep connection to the technical community complements the Atlantic Council's strong ties to international policy, academic, and industry leaders. These individuals and groups match wealth, work, and wisdom with our convening power and global reputation to accelerate our impact.

LOOKING TO 2017 AND BEYOND

The era of high-consequence cybersecurity failures is now upon us, yet policymakers are not yet poised to take the right actions. Against a backdrop of increasing technological dependence, vulnerability, and exposure of society, the number, skill, and ill-intent of our adversaries are also increasing. Where other domains of cyber policy progress in inches, we can have an outsized impact in cyber safety. And where other cyber policy topics have created tension among global powers, cyber safety aligns the international community interested in stability and prosperity.

As international societies struggle to come to grips with cybersecurity, we will continue to pioneer public policy thoughts and discussion on cyber safety. While many cybersecurity issues can be divisive, we will bring together diverse nations and peoples on issues where we have common ground. Alongside likeminded partners, we will make our world **safer, sooner, together**.