U.S. Domestic and International Cybersecurity Policy

CYBR 4400/5400: Principles of Internet Policy, Lecture 6-5

Dr. David Reed, Technology, Cybersecurity, and Policy Program, CU Boulder

Today's Lecture

- Grading curve

- Take time for FCQs!

- U.S. Domestic and International Cybersecurity Policy Lecture

Recall: US Domestic Policy on Cybersecurity

Presidential Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May, 2017)

Presidential Executive Order 13800

- Policy to solve four problems
  - Secure federal networks
  - Encourage collaboration with industry to protect critical infrastructure
  - Strengthen deterrence posture of the United States and build international coalitions
  - Build a stronger cybersecurity workforce

Section 1 Cybersecurity of Federal Networks

- Dept/Agency heads accountable for managing cybersecurity risk
  - Undertake risk management measures commensurate with magnitude of harm
  - Use NIST Cybersecurity framework and provide report in 90 days
- Focus on assessing and reducing risk to improve cybersecurity using best practices, tools and services that are cloud-based
- Determine to use shared IT services such as email, cloud and cybersecurity services
  - Gather info on IT architectures and plans to determine technical feasibility and cost effectiveness of transitioning all agencies to one or more consolidated network architectures and shared IT services

Section 2 Cybersecurity of Critical Infrastructure

- Focus on how to best support cybersecurity of critical infrastructure through policies and stakeholder engagement
- Discuss with stakeholders how federal capabilities can best support designated critical infrastructure
- Commerce and DHS to promote actions to reduce risks from distributed, automated attacks (i.e., botnets)
- Assess potential scope/duration of power outage associated with significant cyber incident against electric grid

Section 3 Cybersecurity for the Nation

- Recognizes importance of cooperation of international partners and growth of cybersecurity workforce as foundation for achieving U.S. objectives in cyberspace
  - International engagement for cybersecurity investigation, attribution, threat info sharing, response, capacity building, and cooperation
  - Ensure nation has strategic options to deter adversaries and better protect from cyber threats

International U.S. Cybersecurity Policy

- U.S. Department of State leads government's diplomatic and development engagement on a wide range of activities in cyberspace

Digital Economy Strategic Goals

- Lead and shape international debate around achieving open, secure, interoperable, and reliable Internet
- Confront market access barriers that restrict importation of U.S. info and communication technology (ICT) goods and services
- Foster collaboration between public and private sector to develop international standards and share best practices that enable innovation
  - Facilitate interoperability, security, and resiliency
  - Improve trust in online transactions
  - Spur competition in global markets

International Security Strategic Goals

- Promote framework of shared voluntary norms to guide state behavior in peacetime, and advance development of practical cyber confidence-building measures (CBMs)
- <u>What are CBMs</u>
- CBMs aim to reduce risk of conflict by eliminating causes of mistrust and misunderstanding between states
- Norms of behavior, CBMs and capacity-building emerging as three main pillars in the process of developing a sustainable and stable digital environment

International Security Strategic Goals

- Promote framework of shared voluntary norms to guide state behavior in peacetime, and advance development of practical cyber confidence-building measures (CBMs)
- Achieved 2015 Group of 20 (G20) Leaders' commitments to:
  - Affirm applicability of international law to state behavior in cyberspace
  - Refrain from cyber-enabled theft of intellectual property for commercial gain
  - Endorse view that all states should abide by norms of responsible behavior

Internet Governance Strategic Goals

- Actively participate to ensure multistakeholder model of Internet governance prevails against attempts to create state-centric frameworks (that undermine openness and freedom, hinder innovation, and jeopardize functionality of the Internet)
- Multistakeholder approach: transparent, bottom-up, consensus-driven processes
  - All governments, private sector, civil society, academia, and technical community participate on equal footing

Sidebar: Internet Governance

- Technical organizations still dominate
  - World Wide Web Consortium (W3C)
  - Internet Engineering Task Force (IETF Newcomers Tutorial)
  - Internet Corporation for Assigned Names and Numbers (ICANN)
- ITU World Conference on International Telecommunications (Dubai, 2012) debated whether International Telecommunications Regulations treaty would be revised to cover the Internet - no consensus gained

Plan of Action to Guide Diplomacy

- Framework of international cyber stability
  - Designed to achieve and maintain peaceful cyberspace environment where all states are able to fully realize its benefits
  - Advantages to cooperating against common threats and avoiding conflict
  - Reduce incentive for states to engage in disruptive behavior or attack one another
- Three elements of framework
  - Global affirmation of applicability of international law to state behavior in cyberspace
  - Development of international consensus on additional norms and principles of responsible state behavior in cyberspace that apply during peacetime
  - Development and implementation of practical CBMs, which can help ensure stability in cyberspace by reducing the risk of misperception and escalation

State Department: Alternative Concepts for Cyberspace Norms

- China/Russia vision is for a system regulated by governments
  - U.S. vision of openness and collaborative, multistakeholder governance
- Russia and China are most assertive states advancing alternative visions for international stability in cyberspace and seeking to sway undecided states in regional and multilateral venues

China's Approach

- Goals
  - Maintain internal stability
  - Maintain sovereignty over its domestic cyberspace
  - Combat what it argues is an emerging cyber arms race and 'militarization' of cyberspace
- Views its online censorship regime – including technologies such as "the Great Firewall" – as necessary defense against destabilizing domestic and foreign influences
  - Has promoted this concept internationally
- Will not affirm applicability of law of armed conflict or other laws of war, believing it would legitimize state use of cyber tools as weapons of war
- Prefers "Code of Conduct" at the United Nations that affirms total national sovereignty over content and cyber infrastructure within a country's borders

Russia's Approach

- Goals
  - Maintain internal stability
  - Maintain sovereignty over its "information space"
- Supports international convention that would:
  - Create new binding rules designed to limit the development, deployment, and use of "information weapons"
  - Promote speech and content controls
  - Replace Budapest Convention's framework for combating cybercrime
  - Give United Nations authority for determining attribution and responding to malicious cyber activity
- Has committed to set of bilateral cyber CBMs with the United States, and the Organization for Security and Cooperation in Europe

Sidebar: Budapest Convention

- First international treaty on cyber crime in 2004
  - Ratified by 59 countries
- Covers range of abuses including child pornography, fraud, hate crimes, copyright infringement and hacking
- Harmonize national laws on cybercrime, and set up regime of international cooperation
- Supplemented by Additional Protocol making it criminal offense to publish racist/xenophobic propaganda via computer network
  - Ratified by 29 countries (not including United States)

Pause

Can the different view of cyber norms between the U.S. and China/Russia coexist together to support a global Internet?

Threats to United States National Security in Cyberspace

- Cyber threats to United States national and economic security are increasing in frequency, scale, sophistication, and severity
- Intelligence community foresees ongoing series of low-to-moderate level cyber operations from a variety of sources — not a catastrophic attack — that will:
  - Impose cumulative costs on U.S. economic competitiveness and national security
  - Pose risks to federal and private sector infrastructure in the U.S
  - Infringe upon the rights of U.S. intellectual property holders
  - Violate the privacy of U.S. citizens

Policy Tools for Deterrence

"Whole-of-government" approach brings full range of instruments of national power and corresponding policy tools

- Deterrence in cyberspace best accomplished by combination of:
- "Deterrence by denial" – reducing incentive of potential adversaries to use cyber capabilities against the U.S. by persuading them that the U.S. can deny their objectives
- "Deterrence through cost imposition" – threatening or carrying out actions to inflict penalties and costs against adversaries that conduct malicious cyber activity against U.S.

Specific "Whole of Government" Policy Tools Available

- Diplomatic tools communicate to adversaries when their actions are unacceptable and to build support and greater cooperation among allies to address shared threats
- Law enforcement tools investigate crimes and prosecute malicious cyber actors both within U.S. and abroad
- Economic tools (e.g., economic sanctions) respond to, and impose costs on, malicious actors in cyberspace
- Military capabilities can deter and respond to malicious cyber activity
- Intelligence capabilities detect, respond to, and deter malicious activities in cyberspace, particularly given unique challenges associated with attributing and understanding motivation behind malicious activities

Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats (May 2018)

- Framework of international cyber stability has achieved important successes in recent years in promoting responsible state behavior in cyberspace
- Continued prevalence of significant state-sponsored cyber incidents show additional measures needed below the threshold of the use of force
- U.S. and partners must be able to deter destabilizing state conduct in cyberspace
- Desired outcomes of deterrence efforts:
  - Continued absence of cyber attacks that constitute use of force against U.S.
  - Significant, long-term reduction in destructive/disruptive/destabilizing malicious cyber activities directed against U.S. interests that fall below threshold of the use of force

Strategic Approach

1. Creating policy for when the U.S. will impose consequences
   - Criteria for types of malicious cyber activities
   - Policy must be communicated publicly and privately for it to have a deterrent effect
2. Developing range of consequences
   - Prepare menu of "swift, costly, and transparent consequences below the threshold of the use of force that it can impose"
3. Conduct interagency policy planning for the time before/during/after imposition of consequences
   - Ensure consistent responses to different incidents and assist in managing the risk of escalation
4. Imposition of consequences more impactful when carried out in concert with partners
   - Partner states can support through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken following an incident

Pause

Do you think that the use of cyber as an instrument of war makes the prospects for conflicts requiring use of force among countries more or less likely?

Bottom Line…

"The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law."

—2015 Department of Defense Cyber Strategy