ATTEMPTS TO PASS U.S. CYBERSECURITY LEGISLATION

YOU NEED A SCORECARD TO FIGURE IT OUT!

Professor Pauline C. Reich
Waseda University School of Law

- cyberasia2@gmail.com
- Director, Asia-Pacific Cyberlaw, Cybercrime and Internet Security Research Institute

- Co-author/Co-editor, CYBERTERRORISM, INFORMATION WARFARE AND INTERNET IMMOBILIZATION (IGI Global, U.S. 2012)
- General Editor, CYBERCRIME AND SECURITY (Thomson Reuters/West, ongoing series now on Westlaw database)

October 11, 2012

- U.S. Secretary of Defense Leon Panetta warns that “there has been a significant escalation in the cyberthreat”
- NEVERTHELESS, THE U.S. HAS NOT PASSED ANY COMPREHENSIVE CYBERSECURITY LEGISLATION SINCE 2002

What is hampering adoption of legislation?

Fundamental questions:

- Internal construction flaws in the legislation?
- Congressional gridlock?
- Philosophical differences?
- Political differences?
- Conceptual flaws?

Ongoing problem:

- Definitions:
- No generally agreed upon definition of cybersecurity- the term is ambiguous and amorphous
- What constitutes a cyberattack?
- What constitutes a serious cyberattack?

Major issue:

- LAW, POLICY AND TECHNOLOGY COMMUNTIES DO NOT WORK COLLABORATIVELY ENOUGH
- LEGISLATORS IN EVERY COUNTRY DO NOT UNDERSTAND TECHNOLOGY ISSUES
- MAYBE U.S. HAS MORE COLLABORATION THAN OTHER COUNTRIES, BUT CLEARLY NOT ENOUGH

Another difficult issue:

- WHICH GOVERNMENT AGENCY should be the lead in dealing with cyberattacks on critical information infrastructure？
- DOMESTICALLY – Should government impose liability on private companies and individuals for not adopting adequate security measures?
- Who should be held responsible for safeguarding private networks? Government? Private sector since it owns most of them?

More questions about governance and responsibility and liability

- Should domestic entities be fined rather than law enforcement and national security seeking external perpetrators of cyberattacks due to anonymity and attribution issues?
- Should the private sector collaborate with domestic government agencies, military and intelligence agencies on cyberthreat information sharing?
- Should the government penalize private sector entities for not having adequate information security measures in place when threats and technology are changing constantly?

Internationally…

- Will global cybersecurity treaties and national laws be useful when we cannot identify the perpetrators of cyberattacks on critical information infrastructures and countries aren't even consistent in their definitions of those critical infrastructures?

Many more questions are also unresolved by U.S. legislative efforts

- When should investigative work and defense fall to government?
- Police?
- Military?
- Intelligence agencies?

-Government vs. private sector or government in collaboration with private sector?

Returning to the U.S. situation

- Congressional Research Service report issued on July 25, 2012 notes that “More than 50 statutes address various aspects of cybersecurity either directly or indirectly, but there is no overarching framework legislation in place. While revisions to most of those laws have been proposed over the past few years, no major cybersecurity legislation has been enacted since 2002.”

10 Broad Areas of Legislation Identified

- National strategy and the role of government;
- Reform of the Federal Information Security Management Act (FISMA);
- Protection of critical infrastructure (including the electric grid and chemical industry)
- Information sharing and cross-sector coordination;
- Breaches resulting in theft or exposure of personal data, such as financial information;

and

- Cybercrime
- Privacy in the context of electronic commerce;
- International efforts;
- Research and development;
- Cybersecurity workforce.

Previous attempt at analysis of legislative efforts (2009-2010)

- Melissa Hathaway, former National Security Council Acting Senior Director for Cyberspace at the White House, who headed the 90 day Cyberspace Policy Review categorized pending bills into these categories:
- Organizational responsibility;
- Compliance and accountability;
- Data accountability and identity theft;

and

- Education, awareness and research and development (R&D);
- Critical infrastructure and electric power;
- Procurement, acquisition, supply chain integrity.

Another bill that caused great controversy and did not pass

- Cybersecurity Act of 2009, the "Kill Switch" bill introduced by Senators Rockefeller and Snowe in 2009
- Would have empowered the President to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal government or United States critical infrastructure information system or network"

2012 attempts to pass legislation

- Cyber Intelligence and Sharing Act (CISPA) passed in the House of Representatives but outcry from Privacy and Civil Liberties groups
- Concern about involvement of NSA and law enforcement and whether Department of Homeland Security would be the lead agency, as well as sharing of vaguely defined “cyberthreat” information by private sector with intelligence agencies and possibly law enforcement with no sanctions
- White House staff advised President to veto the bill if it passed in Senate

Cybersecurity Act of 2012

- The Senate never got to vote on modified legislation
- Opposition from the private sector to excessive cost and government regulation
- The equivalent of a filibuster in August 2012 and again in November 2012

Inability to compromise in the Congress and now…

- Possible Executive Order by the President to take charge of the situation
- Likelihood of the President signing such an order?
- Press reports that the Secretary of the Department of Homeland Security was preparing a final draft of the executive order and that White House staff was meeting to draw up final details (September 2012)

Fundamental and important questions have been raised that may be universal

- Which type of government agency should take the lead in obtaining cyberthreat information and imposing responsibility and liability on the private sector or individual citizen?
- To what extent should government surveillance occur and to what extent can individual citizen privacy and civil liberties be protected in a democracy that also needs to monitor serious cyberthreats?
- Who should bear the cost and responsibility for dealing with cyberattacks on critical information infrastructure?

Complex set of factors – limited to U.S. only?

- Differing political philosophies about privacy, government role
- Application of existing or amended laws to an unprecedented national security issue
- Inability to compromise for the sake of national security
- Private sector concerns about costs overcoming concerns about national security
- National security overcoming privacy and civil liberties concerns

and

- What should be the role and responsibility of the private sector?
- Roles of the military and intelligence communities?

I have raised many thought provoking questions and given few if any answers

- Countries throughout the world may be facing the same kinds of questions and struggling to come up with their own answers suitable to their own political and legal systems

NO ANSWERS TODAY

- PLEASE STAY TUNED (TO TV, RADIO, INTERNET SOURCES) FOR LATEST DEVELOPMENTS
- WILL THEY COME SOON IN THE UNITED STATES? TAKE ANOTHER 10 YEARS OF DELIBERATION?
- WILL THE PRESIDENT TAKE OVER WHEN THE LEGISLATORS CANNOT COME UP WITH ANSWERS?
- WILL AN EXECUTIVE ORDER PROVIDE THE COMPREHENSIVE STRUCTURE NEEDED?

SELECTED READING

- Eric A. Fischer, FEDERAL LAWS RELATING TO CYBERSECURITY: DISCUSSION OF PROPOSED REVISIONS, Congressional Research Service, Summary, July 25, 2012.
- Melissa Hathaway, “Cybersecurity: The U.S. Legislative Agenda,” Belfer Center for Science and International Affairs, May 14, 2010, http://belfercenter.ksg.harvard.edu/files/legislative-landscape-publish-final
- The White House, “Memorandum; Paper Deputies Committee Meeting on Executive Order on Improving Critical Infrastructure Cybersecurity Practices,” September 28, 2012, pages 9-15, http://www.lawfareblog.com/wp-content/uploads/2012/11/White-House-D

Thank you for listening.

Questions?