Recent cyber-security studies in the U.S.

David D. Clark

MIT CFP

May, 2009

Two recent studies

- National Academies Study: *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Computer Science and Telecommunication Board, May 2009
- "60 Day Review": comprehensive high-level review of state of U.S. cyber-security. Melissa E. Hathaway, Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils. (Undergoing White House and security review.)

CSTB study

- Emphasis: *offensive* activities, and *cyber-attack* (as opposed to cyber-exploits).
  - *Attack* implies the goal of disruption, destruction, deception, interference, loss of capability.
  - *Exploit* implies penetration for purposes such as espionage.

Why “offensive” activities?

- Offensive activities have largely been classified, with many implications.
  - No/little opportunity for open policy discussion.
  - Much misunderstanding of capabilities and potential.
    - Do the movies have it right?

What is different?

- Compared to other attacks, cyber-attacks:
  - Seem easy to use.
  - Can give a high degree of anonymity and plausible deniability.
    - So tempting for covert operations.
  - Are more uncertain in their outcomes.
    - Estimation of collateral or indirect damage is hard.
  - Can be used over a wide range of scopes, time-frames, and degrees of intended outcomes.
  - Indirect and 3rd order outcomes will be the most important.

Starting point

- Judge an attack by its effects, not its means.
    - E.g. compare its effect to that of a non-cyber equivalent (kinetic) attack to see what law applies.
    - Does it seem like an “armed attack” or “use of force”?
        - These terms have special meaning in the U.N.Charter and the laws of armed conflict.

High-level theme

- Ambiguity and ambivalence
  - Attack vs. exploit: same tools, different intent.
    - Inference of intention hard, and prone to misunderstanding.
  - Attribution: hard to do.
  - Scope of damage: hard to define, but tools *seem* very versatile. Seems to expand scope of options.
  - Tools are cheap--anyone can play, but nation states can marshal lots of resources.
    - Easy or hard to use?
    - Some tools can only be used once.
      - No demonstration or war-games can be undertaken.
  - Existing laws seem to provide the right framework, but do not account for non-state actors and technology specifics.

Select findings

- In the U.S. (and perhaps in most countries) policy and organizational issues are unclear.
    - Having clear policy can help in lots of ways.
    - Many stakeholders: military, intelligence, law, private sector.
        - Where secrecy impedes understanding.
- While nation states may have an advantage in scale, no country (e.g. the U.S) can expect to dominate the battle.
    - Cannot rely on superiority.
    - Advanced nation states have much to lose.
        - Accordingly, non-state actors may have an advantage.

An interesting question

- When might a cyber-attack be seen as a violation of human rights?
  - What are the ethical issues?
- Do we (in this modern society) have a *right* to the Internet and our Blackberry.
  - Is disrupting the Internet “bombing us back to the stone age”?
- This has real implications with respect to war crimes.
  - My prediction: the first cyber war crime will be *perfidy*.

Another interesting question

- What is the difference between cyber-attack (as an act of a nation state or a non-state actor) and a crime?
  - Totally different laws.
  - But can we find the bright line?
  - Should we judge it by its effects?
    - Hard to assess, especially in real time.

Recommendations

- Most follow directly from findings.
  - If policy and operational rules are ill-defined, sort this out.
- But some are note-worthy.
  - Consider the establishment of an arm of the government intended to help private sector actors that are under attack.
  - Specific R&D: better limits on scope, attribution, geo-location of attacks, IFF

The “60 day review”

- White House called for comprehensive review of U.S. posture and status with respect to cyber-security.
- Will (probably) lead to major initiative to improve status of the nation.
- Review is complete, but undergoing review. The director, Melissa Hathaway, has given a public speech.

An example from her talk

November 2008 illustrates both the speed and the scope of these challenges. In a single 30-minute period, 130 automated teller machines in 49 cities around the world were illicitly emptied. These and other risks have the potential to undermine our confidence in the information systems that underlie our economic and national security interests.

What she would say

- It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and to ensure that the United States and the world can realize the full potential of the information technology revolution.
- This responsibility transcends the jurisdictional purview of individual departments and agencies because, although each agency has a unique contribution to make, no single agency has a broad enough perspective to match the sweep of the challenges.
- It requires leading from the top -- from the White House, to Departments and Agencies, State, local, tribal governments, the C-Suite, and to the local classroom and library.

Continued…

- The national dialogue on cybersecurity must advance now. We need to explain the challenges and discuss what the Nation can do to solve problems in a way that the American people can appreciate the need for action.
- The United States cannot succeed in securing cyberspace if our government works in isolation. Cyberspace knows no boundaries. There is a unique opportunity for the United States to work with countries around the world to make the digital infrastructure a safe and secure place that drives prosperity and innovation for all nations.

More…

- The Federal government cannot entirely delegate or abrogate its role in securing the nation from a cyber incident or accident. The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well-being of citizens.
- The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that government and private sector use in concert. The public and private sector’s interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government services depend.

Finally…

- Building toward the architecture of the future requires research and development that focuses on game-changing technologies that could enhance the security, reliability, resilience and trustworthiness of our digital infrastructure.
- The White House must lead the way forward with leadership that draws upon the strength, advice and ideas of the entire nation.