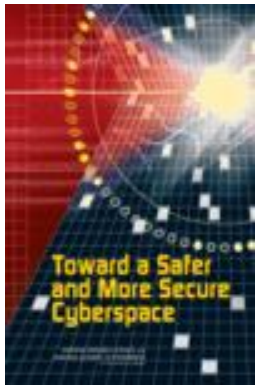
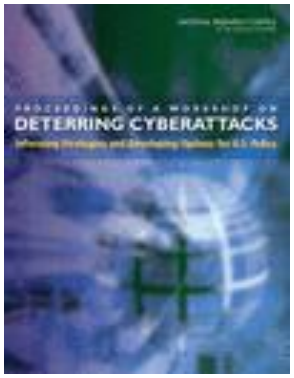
Cyber Security and Infrastructure: Problems of Today, Challenges for Tomorrow

Herb Lin
Computer Science and Telecommunications Board
NAE Convocation of Engineering Professional Societies
Washington DC
April 17, 2013

SOURCE MATERIAL

- Cybersecurity Today and Tomorrow: Pay Now or Pay Later (2002)
- Toward a Safer and More Secure Cyberspace (2008)
- Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (2009)
- Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)





The one slide version of cyber (security) policy

- We are increasingly dependent on information technology for military and civilian purposes.
- Important IT functionality must be protected.
- Cybersecurity: measures taken to protect or preserve a computer system or network and the information it holds.
  - Defensive cybersecurity (highly publicized)
    - Passive defenses
    - Law enforcement
  - Offensive cybersecurity (rarely discussed in public by government officials)
    - Offensive cyber operations taken against an adversary for defensive purposes (e.g., active cyber-response by USG responding to hostile cyber operation from abroad to disable attack in progress)

- Offensive cyber operations can also have non-defensive purposes
  - e.g., cyberattack by USG to achieve military or political goal (Stuxnet?)

Background

What can go wrong with a computer system or network?

- What can happen?
  - Cyberattack (degrade, disrupt, destroy, deny system/network or information therein)
    - Integrity (data/operations are altered)
    - Authenticity (data/operations are forged)
    - Availability (data/operations is inaccessible)
    - Indirect effects may be the **primary** intended effect:
  - Cyber exploitation
    - surreptiously obtain confidential information
- Cyberattack and cyberexploitation look very similar to the victim. (Also look very similar to the news media.)

Some basic facts about offensive cyber operations

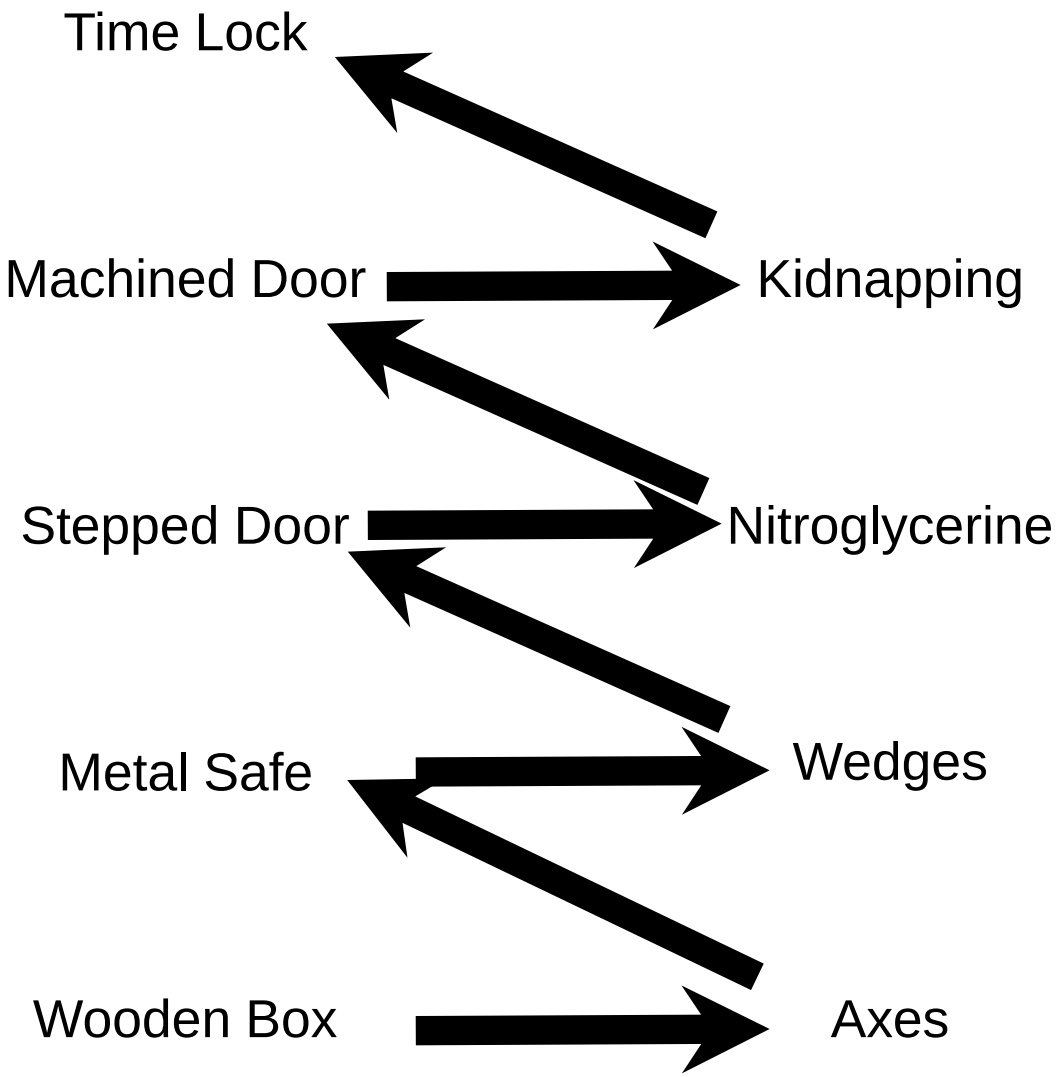
- Cyber operations can undermine confidence as well as technology and data.
- Effects may be significantly delayed in time from moment of insertion.
- Offensive operations can be conducted with plausible deniability
- Offensive technology is relatively inexpensive, easy to obtain; → non state actors (terrorists, organized crime, companies) have some capability to perform offensive operations.
- Offensive cyber operations will always beat defensive operations given enough time.
  - Information technology has changed dramatically in the two decades, except for cybersecurity.
  - Defense has to succeed everywhere; offense has to succeed just once and has lots of time.

From the perspective of defenders…

General Observations

- Security is not just technical: has social, economic, organizational, regulatory dimensions.
- Large uncertainties about “how much is enough?” especially given the costs of security ($$ and interference in daily work)
- Security is a never-ending game of action and reaction.

Security is a never-ending game of action and reaction.
Consider safe cracking…



What to do?

- Conduct frequent, unannounced red-team penetration testing and report the results to responsible management; fix problems and vulnerabilities that are found.
- Assume compromise will be successful:
  - Develop fallback action plans: do less in order to lower vulnerability or to cope with attack or exploitation
  - Design systems under the assumption that they will be compromised
    - Encrypt data onsite
    - Encrypt laptops
- Change public policy to promote greater attention to and investment in cybersecurity. (HOW? Stay tuned…)

From the perspective of national users of offensive capabilities..

Governments need policy to guide use of offensive capabilities: guns for police as an example

- If police officers carry guns, policy regarding police must address:
  - Doctrine:
  - Training
  - Rules of engagement
  - Command and control
  - Identification friend-or-foe (IFF)
  - Liability and insurance: responsibility for mistakes
- Bad guys rarely need to worry about these issues.

Illustrative defensive applications of offensive operations

- Before adversary attack
  - Early warning means living inside adversary network
  - May need to pre-empt offensive cyber action about to be undertaken by adversary
- During adversary attack (the announced case)
  - May need to disrupt a cyberattack in progress by disabling attacking computers
- After adversary attack
  - Need for conducting forensic investigation.
  - Retaliation a possibility to discourage further attacks.

Illustrative non-defensive applications of offensive operations

- Traditional military operations
  - Suppression of adversary air defenses.
  - Interference with adversary command and control
- Covert action
  - Influencing the outcome of a foreign election using electronic voting machines or destroying pension records.
  - Financially destablizing a nation through attacks on the financial system.
  - Damaging an adversary's nuclear weapons production facilities (Stuxnet?)
- Cyberexploitation
  - Exfiltration of negotiating positions, political plans, commercial information.
- Rules of engagement are highly classified... as are most USG discussions of doctrine and strategy regarding offensive cyber operations.

From the perspective of operators of cyber infrastructure…

What's included in cyber infrastructure?

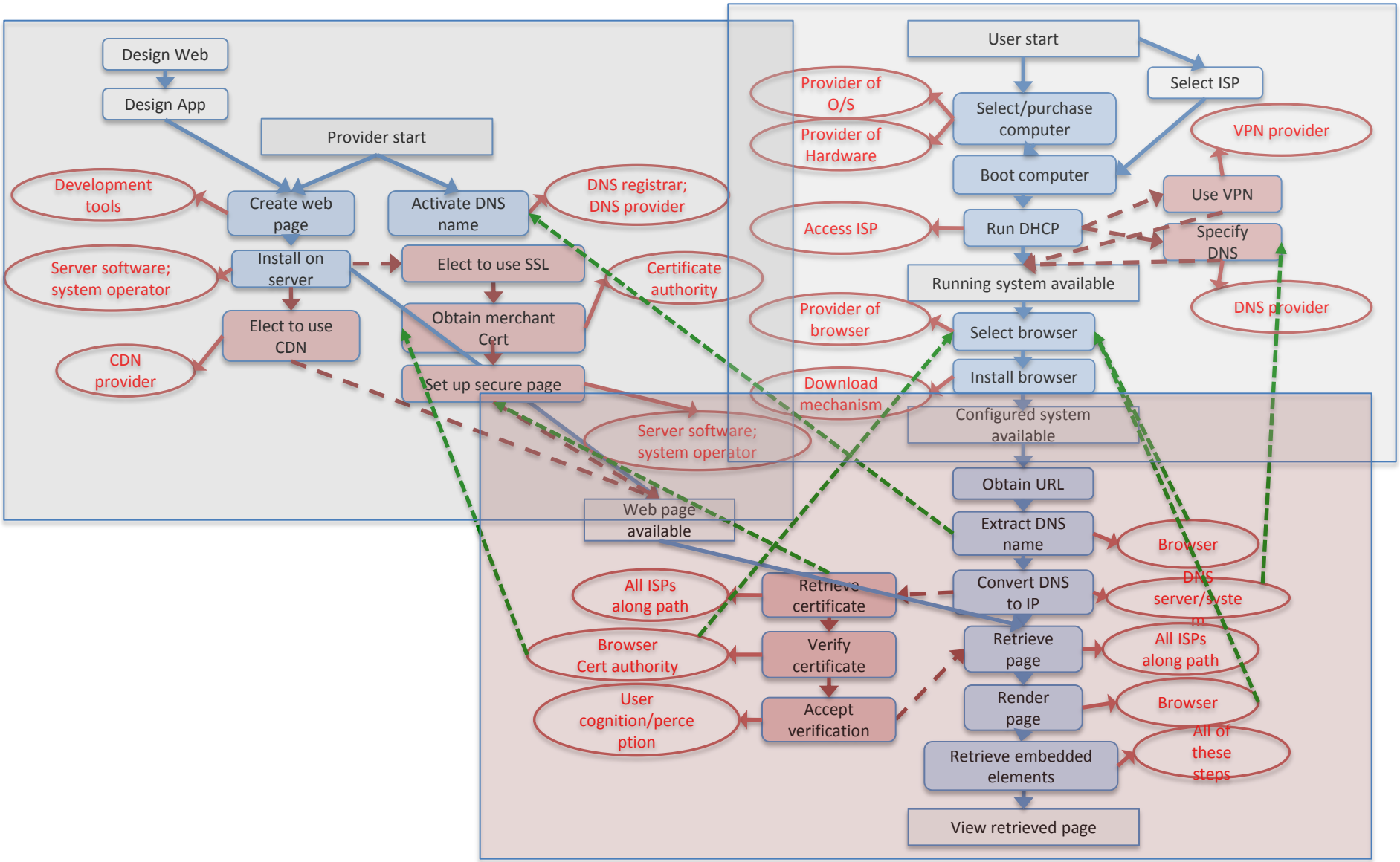
- Cyber-dependent elements of critical infrastructure (from PCCIP 1997)
  - Transportation
  - Oil/gas production and storage infrastructure
  - Water supply
  - Emergency services
  - Government services
  - Banking and finance
  - Electrical power
  - Telecommunications
  - Information and communications infrastructure
    - Public Telecommunications Network (PTN)
    - Internet
    - Computers

Common elements

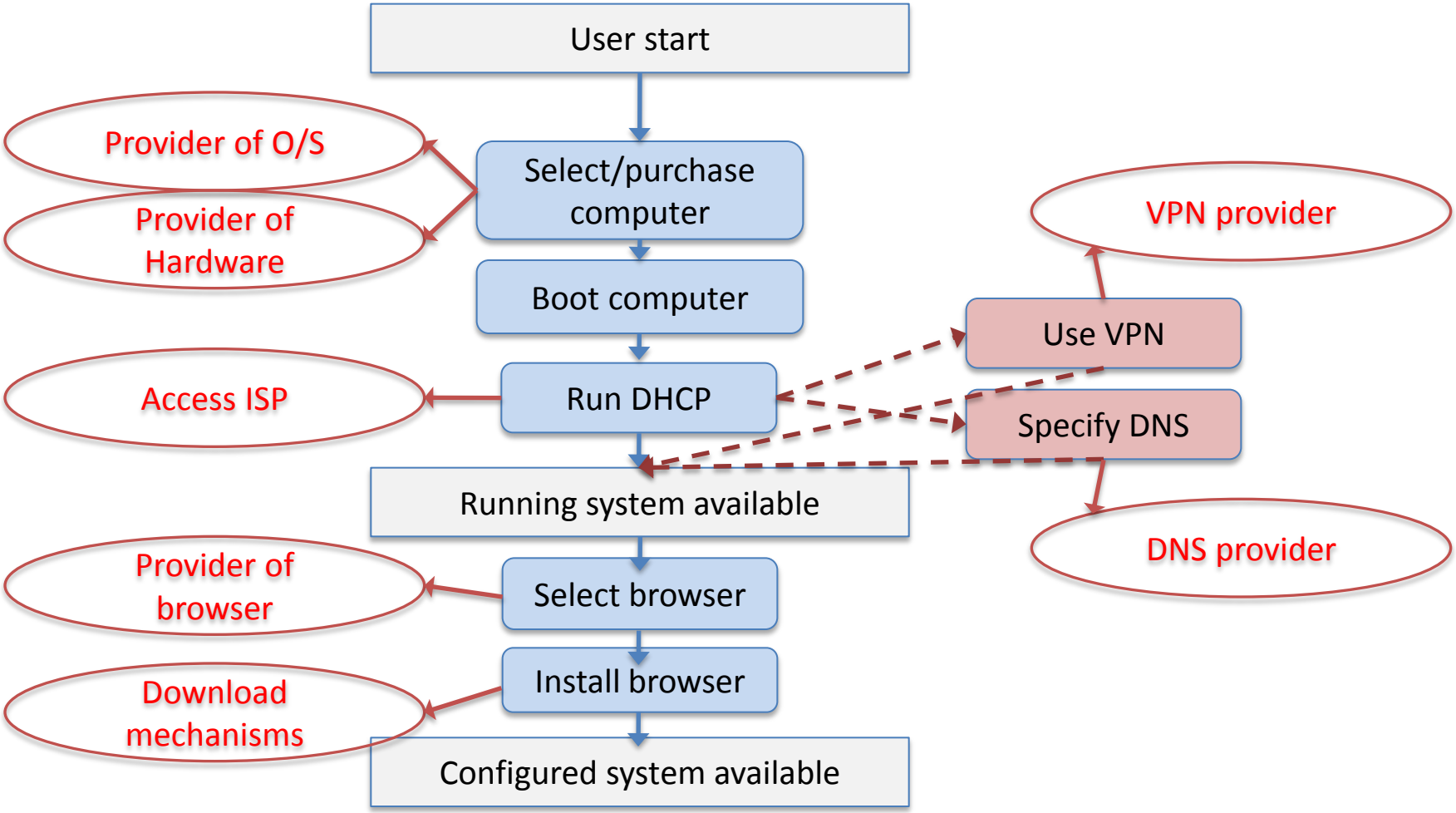
- Standalone computing (desktop to cloud)
- Cyberphysical systems (embedded computing in physical artifacts)
- Internet and other infrastructures for transporting bits
- Software

NB: Complex supply chain to produce all of these elements

How to view a web page…



Getting a running computer



Domestic policy/law and cybersecurity

Some key legal and policy issues

- Cybersecurity investment as a business decision commensurate with firm-level risk leaves the nation less protected against cyber harm than it needs to be (because of systemic risks to all of society). **How to incentivize greater investment/attention by private sector?**
- Information sharing to enable coordinated responses to large-scale cyber assault raises anti-trust and privacy concerns. **Extent, nature, and circumstances of information retention and sharing?**
- Human resources needed for cybersecurity exceed the supply available. **How best to grow cyber workforce?**

International law and offensive cyber operations

Two Legal Paradigms

- U.N. Charter (*Jus ad Bellum*)
  - Defines when a nation can lawfully commence war, and what counts as war
- Geneva Conventions (*Jus in Bello*)
  - Rules that govern warfare (not addressed here)

Jus ad bellum – some key terms not defined

- UN Charter prohibits “threat or use of force against the territorial integrity or political independence of any state” (Art. 2(4))
  - “Force” not defined. By practice, it
    - includes conventional weapon attacks that damage persons or property
    - excludes economic or political acts (e.g. sanctions) that damage persons or property
- UN Charter Art. 51 - “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations..”
  - “Armed attack” not defined, even for kinetic force.

When is a cyberattack a “use of force”or “an armed attack”?

- Answers matter to **attacked** party, because they influence when and under what authority law enforcement (vis a vis military) takes the lead in responding, and what rights the victim might have in responding.
- Answers matter to **attacking** party, because they set a threshold that policy makers may not wish to cross in taking assertive/aggressive actions to further its interests.

When is a cyberattack a “use of force” or “an armed attack”?

- Some hard cases:
  - Economic damage without physical damage
  - Temporary, reversible interference with computer system
  - “Mere” data destruction or degradation
  - Transit through third nation
  - Cyberattack to enforce trade sanctions
  - Introduction of Trojan horse software agents
    - Payload with exploitation and attack capabilities?
    - Payload to accept a future upgrade with unknown capabilities?
    - Destructive payload with delayed action capability? (cf., pre-planted remotely detonatable mine)
    - Empty payload – a shell that can be remotely upgraded in the future

Offensive cyber operations and non-state actors

Cyberattacks and Non-State Actors

- International cybercrime not well regulated
- Non-state actors generally challenge *jus ad bellum* and *jus in bello* paradigms
- Problems exacerbated in cyber context
  - Attribution (public/private and geographical)
  - State responsibility factually and legally unclear
  - War v. crime paradigm (scale of attack)

Some broad questions raised by private sector involvement

- What actions beyond changes in defense posture and calling law enforcement should private sector be allowed to take?
  - Conduct investigations?
  - Get back compromised data?
  - Shoot back to disable/retaliate?

  What DOES actually happen today is uncertain.

- Should US government conduct offensive operations to respond to cyberattacks on private sector? Authorize private sector response?

Some broad questions raised by private sector involvement (continued)

- Important issues raised by private sector action
  - Do such actions increase or decrease the threat to private sector entities?
  - Possible interference with US government cyber operations
  - US government responsibility for private sector actions that rise to “use of force”

- Other implications

  - US cyberattack may require cooperation of U.S. ISPs (and complicate OpSec)
  - Preparation for US cyberattack may require cooperation of U.S. IT vendors and service providers to cooperate (and damage business prospects)
  - Adversary response to U.S. cyberattack may affect U.S. ISPs and critical infrastructure.

Illustrative future NRC work in cybersecurity

- Escalation dynamics in cyber conflict
- Responding to sub-threshold penetrations
- Market calculus/incentives for cybersecurity
- Role of offensive operations for protection of private sector and non-military government cyber infrastructure
- Sector-specific cybersecurity (technical and policy dimensions)
  - Electric power grid
  - Air traffic control
  - Supply chain
  - Insider threats

For more information…

Herb Lin

Chief Scientist, Computer Science and Telecommunications Board

National Research Council

202-334-3191

hlin@nas.edu

www.cstb.org