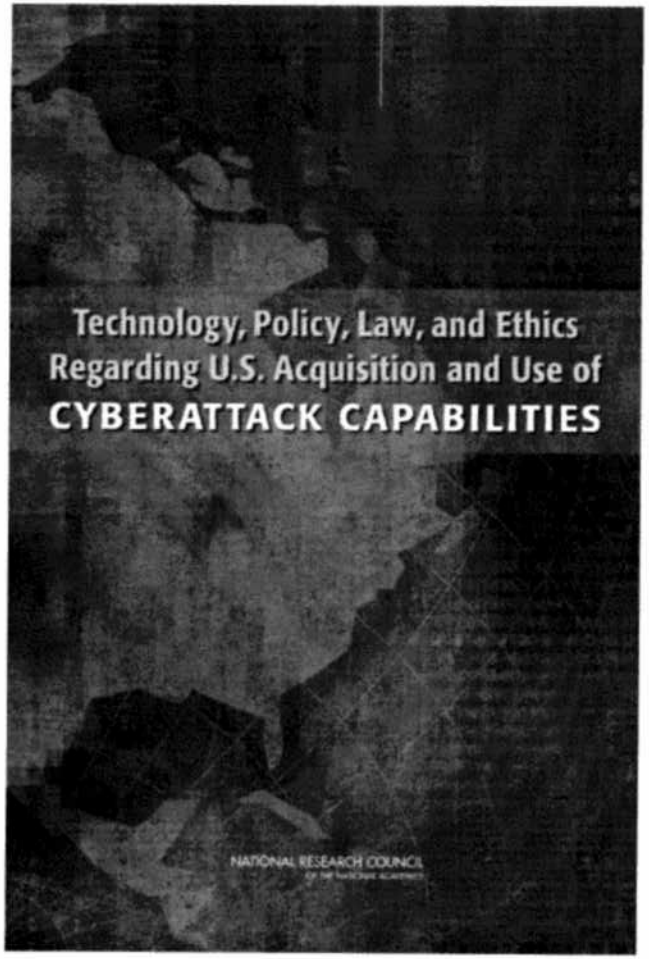
# Understanding Cyberattack as an Instrument of U.S. Policy

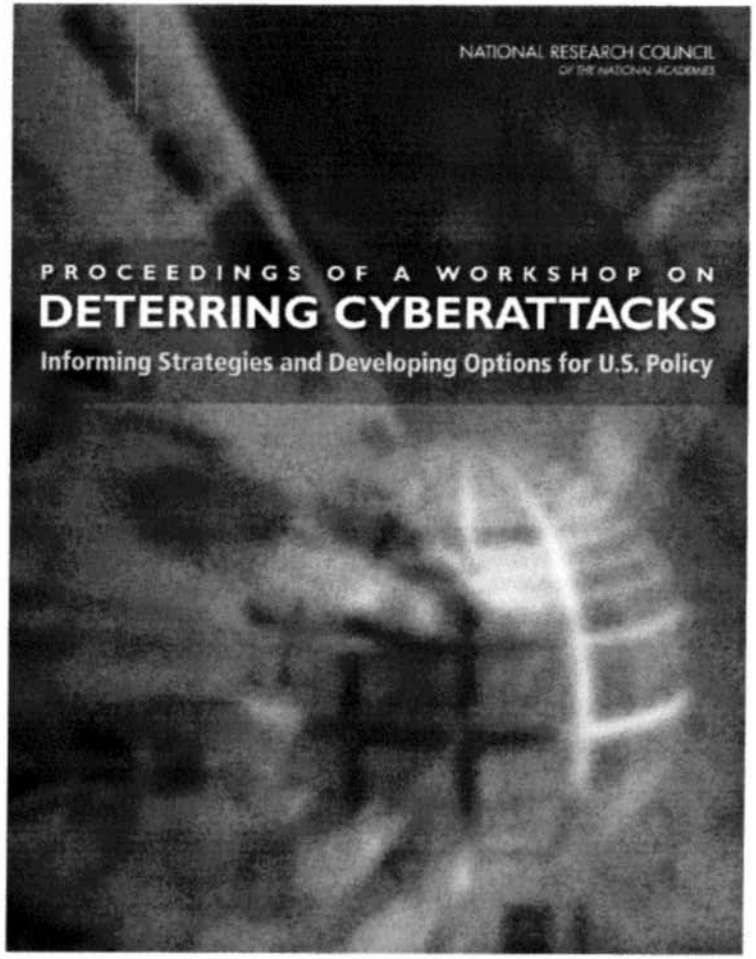
Herb Lin
The National Academies
Project supported by the MacArthur Foundation, Microsoft, and the National Research Council
May 9, 2011
Council on Foreign Relations, New York City

# SOURCE MATERIAL

## 2009




## 2010



# The one slide version of cyber (security) policy

- Nations 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?)

# Comparison of kinetic and cyber operations

- Space of conflict largely separate from civilians
- Offense – defense technologies often in rough balance
- Attribution to adversary presumed
- Capabilities of non-state actors relatively small
- Significance of distance large
- National boundaries important
- Clear lines between attack and spying as security threats
- Effects reasonably predictable

- Space of conflict is where civilians live and work
- Offense always beats defense
- Attribution hard, slow, uncertain
- Capabilities of non-state actors relatively large
- Significance of distance minimal
- National boundaries irrelevant
- Attack and spying hard to distinguish
- Effects hard to predict or control

# Defensive measures

- Passive defenses
  - Anti-virus software
  - Intrusion and anomaly detection
  - Firewalls
  - Better password security (e.g., don't use ABC123)
  - Greater attack resistance in software
- More robust law enforcement mechanisms
  - Convention on Cybercrime
  - FBI cyber division

# Basic facts about offensive cyber operations

- Two categories of interest:
  - Cyberattack: action to destroy, degrade, disrupt adversary IT or information therein
  - Cyberexploitation: action to (very quietly) obtain information from adversary IT
- Technical operations
  - Remote (virus, DOS attack, attacks over the Internet)
  - Close-access (supply chain attack, compromise of 3rd party supplier (antivirus vendor) or service provider (ISP)).
- Note role of social engineering in technical operations
  - Trick, bribe, extort, turn, persuade system operator, 3rd party
- Cyberattack and cyberexploitation are very similar to the victim—both use the same access paths to exploit the same vulnerabilities. (Also look very similar to the news media.)
- Cyberexploitations are different from cyberattacks primarily in their objectives and in the US legal constructs surrounding them.

# Important characteristics of offensive cyber operations

- Indirect effects of cyberatacks more consequential than the direct effects of the attack → must judge cyberattacks by **total** effect, and "indirect" does not mean "not primary"
  - Effects can span an enormous range; cyberattack is a methodology, not a specific weapon.
- Cyberattacks and cyberexploitations are inherently deniable
  - Technical attribution very difficult
- Offensive technology is relatively inexpensive, widely available, and easy to obtain.
  - Many nonstate actors can be able to cause some of the same kinds of effects as state actors.
- A given cyberattack may be
  - Usable only once or a few times (thus, may be hard to sustain an effect over time)
  - Delayed in effect
  - Limited in scope (if highly targeted)
  - Technically fast but operationally slow; hence most suitable in non-time-urgent operational scenarios (e.g., early use); "speed of light" vs "speed of law/thought/analysis"

# Important characteristics continued…

- Outcomes of a cyber operation are highly contingent.
  - Identifying what targets to strike/penetrate
  - Limiting collateral damage, predicting cascading effects may be hard when computers interconnect
  - Conducting battle damage assessment? How do you know what you did?

- Success of cyber operations depends on good advance intelligence (e.g., connectivity, security measures) and preparation of target system
  - Note bias towards early use in conflict against target of our choosing rather than as response against target of adversary's choosing

- Many possible forms of offensive operations have not yet been seen □ future of conflict in cyberspace may be very different.

# Using offensive operations for defense

- Before adversary attack
  - Early warning of attack 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 that may require multiple intrusions into proximate and intermediate nodes.
  - Retaliation a possibility to discourage further attacks.

- And what of non-defensive purposes?

# Illustrative non-defensive applications of offensive operations

- Traditional military operations
  - Suppression of adversary air defenses.
  - Degrade electrical power supporting adversary war-making capacity.

  Cyberattack as military operation may work best in connection with coordinated kinetic action.

- Covert action
  - Influencing the outcome of a foreign election using electronic voting machines.
  - Disruption of adversary R&D or production of WMD

  Cyberattack as covert action may work best as unfriendly action less than war.

- Cyberexploitation
  - Exfiltration of negotiating positions, political plans, commercial information.

# U.S. national security policy today

# (parts of) DOD policy re cyberwarfare

- DOD seeks superiority in the cyber domain--the state in which U.S. and friendly forces have complete freedom of action in the domain and adversary forces have no freedom of action.
  - "Unlike the physical domain, achieving dominance may be impossible," Rear Adm. William Leigher, DEPCDRUSNCC
- DOD implied declaratory policy on cyberattack:
  - Cyberattack is just like any other weapon in the DOD arsenal except for operational considerations.
  - Cyberattack is better suited for early use, when there is time to collect intelligence

# Intelligence community has responsibilities for exploitation and covert action

- Intelligence collection (including cyberexploitation) undertaken to further the interests of the United States outside CONUS – unlimited except if US persons involved. Not a violation of international law.

- Covert action – regulated by US statute: "activities of the U.S. government to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. government will not be apparent or acknowledged publicly." Must be authorized by findings of the President, and reported to appropriate individuals in the U.S. Congress.

Note alignment of plausible deniability requirement and technical characteristics of cyberattack.

# On cyberdeterrence

# The why and how of deterrence

- How can we persuade adversaries to refrain from launching damaging cyberattacks?
- Deterrence seems like the obvious inevitable choice in an offense-dominant world.
  - Passive defense is inadequate and eventually will fail;
  - Law enforcement actions are too slow and uncertain in outcome.
- Deterrence of nuclear threats in the Cold War establishes the paradigm – largely successful. Based on a credible threat to:
  1. Deny the attacker the benefits of an attack
  2. Punish the attacker by imposing unacceptable costs

# Applying deterrence to cyberconflict

- Denial (#1) is too hard, hence punishment (#2) is a more appealing strategy.

- Threat of punishment requires:
  - Attribution of attack to adversary
  - Knowing that an attack has happened
  - Credibility
    - Nations conduct many highly visible military training exercises in part to demonstrate capabilities to potential adversaries. How should nations demonstrate (secret) cyber capabilities?

- Bottom line on cyberdeterrence – uncertainty about how traditional concepts of deterrence (i.e., #2) apply to cyberspace. Thus, denial has greater appeal (cf., recent William Lynn Foreign Affairs article)

- The irony of deterrence
  - Defense is too hard, so we need to explore deterrence.
  - But now, deterrence is too hard, so we need to do better defense.

# The meaning of attribution

- "Attribution is necessary for deterrence"
- Attribution can mean
  - Identification of the proximate machine that is attacking
  - Identification of the machine that launched/initiated the attack
  - Identification of the individual who pressed the keys on the initiating machine
  - Identification of the nation under whose jurisdiction the individual falls
  - Identification of the entity under whose auspices the individual acted, if any.
- In practice, attribution is all-source, not just technical.
- Attribution is separate from the presence of an electronic access path for retribution/punishment.
- Not all forms of attribution contribute to deterrence.

# On escalation and termination

- Deterring escalation is just as important (perhaps more so) as deterring onset of conflict.
- Unintended escalation particularly dangerous when
  - operational actions are less visible to senior decision makers
  - outcomes of actions are more uncertain (e.g., cascading effects)
- How can cyberconflict be terminated?
  - Requirements for "termination" – how to de-mine?
  - How to suppress patriotic hackers?
  - How to implement a "cyber cease-fire"?

# 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

# *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
  - 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

# Economic damage w/o physical damage

- Theft of economically valuable information
  - Blueprints and technical specifications
  - Negotiating positions
  - Trade secrets
- Destruction or alteration of economically valuable information
  - Tampering with manufacturing processes (e.g., Stuxnet and production of weapons-grade uranium)
  - Alteration of delivery timetables to disrupt production/delivery schedules
- Denial of service
  - Loss of access to critical information processing facilities
  - Time lost in recovering from disruptive attack
  - Similar to blockade?

- Both government and private sector actors (e.g., companies) have some capability to perform such actions

# *Jus in Bello*

- Principle of Non-Perfidy
  - Cannot pretend to be legally protected entity
    - Hard case in traditional war: distinction between ruse of war (e.g., use of misinformation to mislead adversary) and perfidy (e.g., pretending that a military installation is a hospital).
- Principle of Proportionality
  - Collateral damage on civilian targets acceptable if not disproportionate to the military advantage gained.
    - Hard cases in traditional war: human shields, chemical plant in suburbs, etc.
- Principle of Distinction
  - Military operations only against "military objectives" and not against civilian targets
    - Hard cases in traditional war: Serbian television station, Baghdad electrical grid, etc.

## Distinction—legitimacy of attacks that disable computer-dependent civilian services or communications?

- Large fraction of US military communications take place over the Internet, and the US military is dependent to some extent on commercial power grid. Are the US Internet (e.g., routers) and power grid valid military targets for adversaries?
- To what extent are computer-dependent civilian services or communications "essential" to life in a modern society? Does disruption in these services rise to the level of causing death and destruction?

# International Regimes for Promoting Cybersecurity?

# Why might regimes be desirable?

- Reduce likelihood of conflict, damage if conflict occurs.
- U.S. significantly more dependent on IT, thus restrictions on cyberattack asymmetrically benefit U.S.
- Delegitimize cyberattack as a military weapon and discourage other nations to develop such capabilities for use against U.S. interests.

# Reasons for skepticism

- Other nations will develop cyberattack capabilities under any circumstances. (Some see cyberattack as an ideal instrument of asymmetrical warfare.)

- Verification of limiting capabilities essentially impossible.
  - Can't restrict code, expertise/knowledge, underlying technology
  - Infrastructure needed to conduct attacks is small, easily hidden.

# Restrictions on use of cyberattack?

- Refrain from striking at national financial systems or power grids (similar to “no kinetic attack on hospitals” or “no blinding lasers”)
- May require cooperative measures (e.g., electronic identification of permitted and/or prohibited targets)
- Attackers can violate such agreements (just as a kinetic attacker can target ambulances or fire mortars from sanctuaries), and compliance in wartime is not assured.
- Complicating factors
  - Living with any regime we claim to want – must be reciprocal.
  - Ambiguity of cyberexploitation during crisis and possible misintepretations
  - Hard to prove a violation.
  - Private sector in cyberspace
  - High intrusiveness; national responsibility for private action

# Some ideas re international agreements concerning cybersecurity

- Stephen J. Lukasik – Hold nations for eliminating the distribution of malware and the capturing of computers for use as botnets within their jurisdictions, and require them to attach a state label to each packet leaving their jurisdictions.

- Michael A. Vatis – Expand membership of Cybercrime Convention, and strengthen provisions where if a country refuses to lend assistance when requested.

- Bill Owens (personal) – Bilateral agreement with China to refrain from large-scale cyberattacks on critical infrastructure.

- Richard Clarke – Agree to refrain from economic espionage.

- NRC – Seek common ground for understanding basic issues.

# Some broad observations

# Great confusion and uncertainty about cyberwar and cyberattack

- What is not cyberwar
  - A teenager defacing a DOD/MOD web site.
  - Criminals hacking into the bank accounts of a defense contractor to steal money.
  - An unfriendly nation stealing plans for a new jet fighter.
  - A terrorist group using the Internet for recruiting, fund raising, propaganda, and communications.
  - Countries stealing IP stored in computers from commercial firms.

  Dividing lines between criminal acts and acts that might implicate the UN charter or IHL are unclear.

  Many examples of cyberattack; few (if any) examples of cyber war.

- Cyberattack and cyberexploitation conflated in public discourse

- Responses to hostile subthreshold actions are the most relevant dimension of policy today.

# Biases and red herrings

- The public process for "net assessment" of cyber power is inherently biased against us
  - "Their" offensive capabilities are matched against "our" defensive capabilities only.
  - Uncertainties drive worst-case analysis
  - "Our" offensive capabilities and "their" defensive vulnerabilities are never discussed in public.

- Offense is largely irrelevant to defense in cyberspace, and the most likely uses relate to offensive purposes.
  - We don't know how to do good cyber defense.
  - We don't know how to do good cyber deterrence.
  - We don't know how to do offensive operations that will enhance defense.
  - The only thing left is offensive cyber operations for their own purposes.

- Attribution is not nearly a silver bullet
  - Does little against high-end threat, which is likely to compromise attribution

# Nuclear conflict as bad analogy for cyber

- Many superficially obvious connections
  - Role of deterrence
  - WMD/strategic significance
- But deeper analysis suggests badness of fit
  - Private sector doesn't have nuclear weapons.
  - Many of the same questions/issues arise in cyber as in nuclear (as well as in many other forms of conflict)
  - Answers to these questions are mostly very different
- Biological weapons may be a better metaphor from a strategic point of view (deterrence, arms control, and so on).

# Bottom line

- Many unanswered questions in the scientific and technical, policy, legal spaces.
  - 50 interesting and important questions can be found in the **NRC letter report on deterring cyberattacks**
    - Theoretical Models for Cyberdeterrence
    - Cyberdeterrence and Declaratory Policy
    - Operational Considerations in Cyberdeterrence
    - Regimes of Reciprocal/Consensual Limitations
    - Cyberdeterrence in a Larger Context
    - The Dynamics of Action/Reaction
    - Escalation Dynamics
- Serious study of conflict in cyberspace as a national security issue is needed.
- Subject is inherently interdisciplinary.

# Backup material

# x-The meaning of neutrality?

- Nation A, sending bombers to attack Nation B but flying through the air space of Nation C, must obtain C's permission to do so. C may not be regarded as neutral if A does indeed fly through C's airspace.

- Nation A, sending messages that direct its forces to attack Nation B but using the telecommunications facilities of Nation C need not obtain C's permission to do so, and need not obtain C's permission to do so (as long as C allows all nations to do so). C is neutral even if it allows A's messages to be transmitted through C's telecommunications facilities.

Which is the right model for an Internet-based attack of A against C?

Extension of issue--

- How, if at all, does compromise of innocent computers for a botnet differ from allowing transit? Are compromised computers legitimate targets? What if a nation does not have the capability for identifying compromised computers or for preventing them from participating in an attack?

# x-Non-perfidy

- Requirement for identification of USG cyberattacks?
  - USAF insignia on airplanes and cruise missiles.
  - Military personnel in distinctive uniforms.
  - Trojan horses with distinctive identifiers "This agent is a bona fide weapon of the US government"?
  - Public infrastructure so that any victim can verify the authenticity of such an identifier?
- Requirement for identifying military and civilian targets in cyberspace?
  - Nations have obligations to enable identification of military assets (distinctive vehicles with insignias) and are entitled to identify entities legally immune to attack (Red Cross on ambulances, white flags).
  - What must be done to identify military computers/networks? IT assets of hospitals and religious institutions? Who will verify the latter? (International Red Cross?)

# x- 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?

- Should US government conduct offensive operations to respond to cyberattacks on private sector? Authorize private sector response? Would the US government be responsible under international law if operations rise to use of force?

- Important issues raised by private sector action
  - Possible interference with US government cyber operations
  - 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.
  - U.S. domestic law (e.g. Computer Fraud and Abuse Act) might ban some DOD cross-border computer intrusions
  - Do such actions increase or decrease the threat to private sector entities?

# x-New knowledge needed, such as…

- Conveying the intent of an offensive cyber operation to an adversary.
- Understanding likely paths for escalation and de-escalation/termination.
- Understanding how, if at all, offensive capabilities enhance or detract from defensive postures.
- Conducting better assessments of adversary intent in crisis and in peacetime
- Incentivizing appropriate defensive measures.