# Thinking about Nuclear and Cyber Conflict: Same Questions, Different Answers

Herb Lin

CISAC/Hoover

May 15, 2015

# Thinking about cyber through a nuclear lens

- Thinking about nuclear issues is far more advanced than thinking about cyber issues.
- Lots of former nuclear strategists thinking about cyber conflict today.
- How does the conceptual framework of nuclear strategy, operations, acquisition , and arms control help in thinking about cyber issues, given that nuclear weapons and cyber weapons are very different from each other?

# The fundamental proposition

Nuclear thinking and cyber thinking are (or should be) closely aligned in the questions that arise but the answers in each conceptual domain are in general quite different.

Strategy

Operations

Acquisition

Arms Control

# Strategy: What is the nature of the escalation ladder involving domain X?

- Nuclear
  - Nuclear comes AFTER conventional conflict has commenced.
  - Failure of extended deterrence provides another path to escalation.
  - Escalation concerns involve moving from conventional conflict to nuclear conflict. Going nuclear is escalatory.
  - Countervalue strikes are at the TOP of the escalation ladder.
- Cyber
  - Cyber comes in earliest stages of conflict (BEFORE kinetic war)
  - In principle, cyber just another weapon to be used by U.S. military forces (cf., nukes in early 1950s).
  - Escalation concerns involve moving from cyber conflict to conventional (or nuclear) conflict. Going cyber is pre-escalatory.
  - Countervalue strikes happen all the time now and are at the BOTTOM of the escalation ladder as well as elsewhere on the ladder.

# Operations: What is the tactical warning/attack assessment function in domain X?

- Nuclear
  - Zero background of nuclear explosions in peacetime
  - Nuclear detonations readily identified re time/place
  - Early warning satellites provide minutes notice of strategic attack
- Cyber
  - Constant background of cyber events in peacetime
  - Cyber weapons effects may be hard to identify, recognize
  - Weapons effects can manifest themselves with essentially zero warning time.
  - Streaming information flows are only one kind of cyberattack. More likely is multiple implants that are triggered or that enable real-time access (from within country!).

# Acquisition: What is the nature of the X weapons acquisition process?

- Nuclear (depends on knowledge + nuclear materials)
  - Production is key attribute: numbers of (identical) weapons is a common measure of offensive nuclear strength
  - Delivery platforms part of standard DOD acquisition process (decades long process)
- Cyber (depends primarily on knowledge)
  - R&D is key attribute: numbers of *different* weapons is one measure of offensive cyber strength.
  - Delivery platforms (should  be) part of O&M, not Acquisitions (should be days to months): speed really matters!

# Arms control: What is the feasibility of limiting acquisition in domain X?

- Nuclear: SALT/START limited nuclear acquisitions.

- Cyber: "No development of or acquisition of offensive capabilities in cyberspace"
  - No possible way to verify
  - Penetration testing only way to validate defenses
  - No government monopoly on cyber attack technology

# Meta-question: How did/does/will technological change affect strategy in domain X?

- Nuclear
  - Plentiful nuclear materials (countervalue to counterforce)
  - Accuracy (fixed targets vulnerable)
  - SSBNs (secure second-strike)

- Cyber
  - Growing user base (Africa, South Asia, IoT)
  - Mobile and cloud computing
  - Social networking
  - Possible quantum computing makes current RSA infrastructure vulnerable

  Many more opportunities for vulnerability, more noise to hide attacks

# Backup

# Strategy

- What does offensive dominance for domain X?
- What are does deterrence mean in domain X?
- What are we trying to deter in domain X?
- What is the meaning of “assured destruction” in domain X?
- What is the nature of the escalation ladder involving domain X?
- What is the role of counterforce and damage limitation in domain X?
- What is strategic stability in domain X?
- How are tactical and strategic uses differentiated in domain X?
- How is signaling accomplished in domain X?
- What is the strategic value of X weapons to non-peer competitors?

# Operations

- **What are the weapons effects in Domain X?**
- **What is the meaning of "lethality" in domain X?**
- **What is the tactical warning/attack assessment function in domain X?**
- How are events in domain X attributed?
- What is the nature of battle damage assessment in domain X?
- How is intelligence preparation of the domain X battlefield performed?
- How are target identification and selection for domain X accomplished?
- How can forces for domain X be stood down?

# Acquisition and Arms Control

- Acquisition
  - **What is the infrastructure needed to support acquisition of X weapons?**
  - **What is the nature of the X weapons acquisition process?**

- Arms Control
  - **What is the feasibility of limiting acquisition in domain X?**
  - **What is the feasibility of limiting use in domain X?**
  - **What is the feasibility of CBM in domain X?**

# Some meta-questions (cf., Nye)

- How did/does/will technological change affect strategy in domain X?
- How and to what extent is there an empirical basis for strategy in domain X?
- How does the technology in domain X affect civil-military relations?

# Strategy

# What does offensive dominance mean for domain X?

- Nuclear
  - Hardening impossible against nuclear explosion in close proximity
  - Overwhelming power of single weapon can mean catastrophe if defense is not perfect.
  - Cost exchange ratio favors offense (low-cost weapon for high-value target)
- Cyber
  - Individual target hardening possible, but complex IT systems and networks have a virtually unlimited number of exploitable vulnerabilities.
  - Given sufficient time, it is virtually certain that an attacker will penetrate a target's defenses.
  - The defender needs to succeed every time and everywhere, the attacker only once: the cost of defense is thus far less than the cost of attack.

# What does deterrence mean in domain X?

- Deterrence by denial—denying adversary the ability to achieve operational objectives.
  - Nuclear
    - Missile defenses and ability to strike at nuclear C2 complicate attack planning, deny adversary certainty of success.
  - Cyber
    - Uncertainty inherent in attack planning: cyberattacks are difficult to execute with high confidence on preplanned timetable. Also helped by good cyber defenses.
- Deterrence by punishment—imposing costs
  - Nuclear attack virtually demands nuclear response against some high value target(s).
  - Cyber attack in no way demands cyber response, even though the debate is often couched in such terms.

# What are we trying to deter in domain X?

- Nuclear
  - Nuclear attack against U.S.?
  - use of chem or bio or cyber weapons against U.S.?
  - Conventional attack against allies?
  - Nuclear attack against allies?
- Cyber
  - All hostile cyber activities including espionage?
  - All attacks?
  - Serious attacks?
  - Only catastrophic attacks?

# What is the meaning of "assured destruction" in domain X?

- Nuclear
  - Modest levels of nuclear use can produce tens of millions of deaths in minutes.
  - Higher levels of nuclear use can destroy a country beyond recognition.
- Cyber
  - Nuclear EMP attack can (may be able to?) produce large-scale destruction of electronics.
  - Other than EMP attack, no way. In general, can produce large impact for a short time, or small impact (e.g., fewer people affected) for longer time. Most likely is small impact for short time.

# Operations

# What are the weapons effects in Domain X?

- Nuclear
  - Effects are quantized (especially going from zero to one)
  - Weapons have only destructive effects
  - Effects not reversible
  - Civilian use limited
- Cyber
  - Effects can be infinitely graduated
  - Weapons can have non-destructive effects (DOS, espionage)
  - Easily confused/conflated with espionage
  - Effects are often reversible
  - Civilian use extensive

# What is the meaning of “lethality” in domain X?

- Nuclear (physics provides a basis for calculating weapons effects from first principles)
  - Lethality $K \sim (Y^{1/3}/CEP)^2$
  - $P_k \sim f(H, K)$, where H = hardness of target
- Cyber (no science-based first principles underlying weapons effects)
  - No idea what a lethal radius might be
  - No way to calculate a $P_k$

# How are events in domain X attributed?

- Nuclear
  - Geographic origin
  - Spectrographic analysis (prior collection needed)
  - Tracking nuclear delivery platforms (only a few threaten United States)
  - Presumption of national control
- Cyber
  - Geographic origins uncertain
  - Assembly of forensics slow
  - Integration of all-source intelligence necessary
  - Lots of prior intelligence collection necessary
  - No presumption of national control

# Acquisition

# What is the infrastructure needed to support acquisition of X weapons?

- Nuclear
  - Physical infrastructure large and extensive, hard (though not impossible) to conceal
  - Limited numbers of experts
  - Hard to purchase if lacking expertise
- Cyber
  - Physical infrastructure minimal, easy to conceal under ordinary roofs
  - Many experts
  - Easy to purchase if lacking expertise

# Arms Control

# Types of agreement

- Limit acquisition (research, development, testing, production, or combination)
- Limit use
  - e.g., certain targets may not be struck in armed conflict
- Promote confidence-building (take or refrain from taking certain actions to reassure others about true purposes (e.g., benign intent).
  - to enhance mutual knowledge and understanding of military activities;
  - to reduce the possibility of conflict by accident, miscalculation, or the failure of communication;
  - to increase stability in times of both calm and crisis.

# What is the feasibility of limiting use in domain X?

- Nuclear: “no first use of nuclear weapons”
  - Non nuclear example: no attacks of hospitals, places of worship (Geneva Con)
- Cyber: No cyber strikes at national financial systems or power grids
  - May require cooperative measures (e.g., electronic identification of permitted and/or prohibited targets)
- In both cases, compliance is not assured. But such agreements:
  - Create international norms regarding the acceptability of such behavior.
  - Help to Inhibit overt threats regarding such use
  - Help to clarify certain red lines in an escalation ladder.

# What is the feasibility of CBM in cyberspace?

## Examples from traditional arms control

- Notification of activities that might be observed but misinterpreted
  - Movement of certain forces, notification of military exercise, ballistic missile launches
- Means for communication during times of tension
  - hot lines, nuclear risk reduction centers
- Agreed conventions for behavior
  - Avoiding naval incidents.
  - Prevent harmful interference with command and control networks.
- Enhancement of and noninterference with gathering data for verification of compliance
  - Deployment of observers, Treaty on Open Skies, noninterference with national technical means

# Application to cyberspace

- Notification of activities that might be observed but misinterpreted
  - Seeing activities in cyberspace is hard unless conducted on a large scale.
- Means for communication during times of tension
  - Cyber operations depend on deception—credibility is an issue
- Agreed conventions for behavior
  - Behavior is not intent, and intent is important (e.g., exploitation vs attack)
  - Understanding behavior depends on knowledge of adversary's concept of operations.
- Enhancement of and noninterference with gathering data for verification of compliance
  - Instrumenting for gathering data would necessarily be extensive and highly intrusive (and easy to evade)

# Some meta-questions
# cf., Nye article in SSQ
# “Nuclear Lessons for Cybersecurity”

# How and to what extent is there an empirical basis for strategy in domain X?

- Nuclear
  - No examples of post-WWII nuclear use in anger
  - Many examples of using nuclear weapons and/or forces for non-explosion purposes
- Cyber
  - Huge numbers of hostile cyber events daily
  - Hostile cyber events are mostly low-consequence taken one-by-one. High consequence in the aggregate.

# How does the technology in domain X affect civil-military relations?

- Nuclear
  - Nuclear power (a peaceful and largely desirable civilian use of nuclear technology) vastly complicates non-proliferation efforts.

- Cyber
  - Cyber technology is intimately integrated into the fabric of everyday life.
  - Cyber technology and application driven almost entirely by private sector.
  - Cooperation of government and private sector essential for progress in cybersecurity.

New/better questions and answers invited!

# For more information…

Herb Lin

Stanford University

Center for International Security and Cooperation

Encina Hall, C-236

616 Serra Street

Stanford, CA  94305

herbert.s.lin@stanford.edu

650-497-8600

# Additional questions re strategy

# What is the role of counterforce and damage limitation in domain X?

- Nuclear
  - Counterforce against nuclear weapons systems is more feasible than commonly assumed.
  - Likely results of DL strike insufficient to forestall significant countervalue retaliation.
- Cyber
  - Impossible to degrade adversary cyber attack assets that are not accessible without previous access. (Thus, "preemption" against weapons systems per se not possible.)
  - Attacks likely to have been preplanned , hence no good targets
    - launched from 3rd party computers;
    - Implants previously installed, triggered by easily accessible signal.

# What is strategic stability in domain X?

- Nuclear
  - Secure second-strike capabilities are the enabling condition that eliminates the advantage gained by a first (strategic) strike.
  - Submarines (and land-mobile missiles?) provide the requisite capability (though they can be tracked to a large degree).
- Cyber
  - Secure second-strike capability is easy to obtain—just have computers that have not been connected to the Internet and have only software you've provided.
  - But SSSC is NOT known to be the enabling condition for strategic stability.
    - Nothing is known that will eliminate the advantages of first strike.
  - Not clear that strategic stability is even at issue in cyber, given that cyber is relevant at the *lowest* levels of conflict.

# How are tactical and strategic uses differentiated in domain X?

- Nuclear
  - Strategic targets defined through SIOP.
  - NCA approval required for all uses of nuclear weapons (though pre-delegation may be approved).
  - Strategic and tactical targets are easily distinguished (relatively so), with possible exception of C2.
- Cyber
  - Strategic targets (likely) defined through PPD-20 process.
  - Tactical targets defined through Cyber Tasking Order (analogous to ATO). Presumably many targets of opportunity.
  - Necessity of NCA approval for DOD cyberattack on strategic targets unclear from public documents; clearly necessary for IC-covert action cyberattack and for very sensitive collection operations.
  - Strategic and tactical or civilian targets may not be easily distinguishable if on same control/communications network.

# How is signaling accomplished in domain X?

- Nuclear
  - Example: demonstration use
  - Example: generation of forces
    - Redeploy forces
    - Go to higher Defcon
- Cyber
  - Demonstration use presumes high confidence in outcome of attack; visible connection between attack and signaling party; willingness to lose the use of that particular weapon.
  - Generation of cyber forces is difficult to observe.

# What is the strategic value of X weapons to non-peer competitors?

- Nuclear
  - Equalizer between militarily strong and weak states.
  - Effects are mostly on deterrence
- Cyber
  - Equalizer between militarily strong and weak states.
  - Effects are mostly on actual conflict

# Additional questions re operations

# What is the nature of battle damage assessment in domain X?

- Nuclear
  - Nuclear destruction if target is within known lethal radius.
  - Conventional attack against nuclear platforms no different from attack against other platforms
- Cyber
  - No “smoking hole”.
  - Cessation of target function is not clearcut indication of damage; higher confidence requires IPB to instrument the target.

# How is intelligence preparation of the domain X battlefield performed?

- Nuclear
  - Battlefield must be instrumented
  - Once target is located, small details don't matter much to target kill.
- Cyber
  - Adversary systems (and battlefield) must be instrumented
  - Small details matter a lot to target kill even after target is located.

# How are target identification and selection for domain X accomplished?

- Nuclear
  - Imint is critical source of intelligence
  - photo-interpretation is critical analytical skill
- Cyber
  - Sigint is critical source of intelligence
  - Understanding of system internals and field-specific knowledge about system are critical analytical skills
  - In practice, lawyers have very important role in selection and ROE.

# How can forces for domain X be stood down (essential aspect of conflict termination)?

- Nuclear
  - SSBNs can surface
  - Bombers and land mobile missiles can return to base
  - Other nuclear capable forces (e.g., warships) can withdraw.
- Cyber
  - Personnel for cyber forces cannot be visibly stood down.
  - Implanted cyber weapons can be revealed but only at the cost of losing future utility.
  - May be difficult to keep track of where friendly cyber weapons have gone
  - Intelligence gathering for monitoring cyber cease fire incompatible with attack stand down since they are indistinguishable to adversary.