Cyber Risks in Nuclear Escalation Scenarios

Herbert S. Lin

Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution

Senior Research Scholar at the Center for International Security and Cooperation, Stanford University

10/27/2021

Brief Description: Given the catastrophic potential inherent in incidents involving nuclear weapons, scenarios that potentially lead to nuclear conflict or increase the likelihood of nuclear use have always warranted the highest levels of concern and attention. Cyberspace, cyber operations, and the modern information environment are variables that did not exist several decades ago, and adding them complicates the assessment process. This talk will consider cyber's impact on a number of scenarios involving nuclear weapons.

Cyber Threats—a quick review

- Cyber weapons can compromise
  - Confidentiality
  - Integrity
  - Availability
- Technical aspects of a cyber weapon
  - Penetration
    - Access is impossible to limit to just the good guys
    - Vulnerabilities are everywhere
  - Payload (specifies what hostile action to take)
    - Impossible to now intent of penetration until payload executes
    - Possibilities for payload span a very large range (selectivity, timing, scope)
- Intelligence support for cyber operations is critical; strong coupling between target characteristics and weapon
- On attribution
  - Offensive operations can be conducted with plausible deniability in the short term.
  - Attribution may be possible in the long term, drawing on all sources of intelligence. Usually no smoking guns.
- On strategy
  - Deterrence of cyberattack at low level is essentially impossible
  - Deterrence of cyberattack at high level may be possible
  - Logic of cyberattack and offense dominance before conflict starts suggest early use can lead to significant escalation potential
- In practice, security is the poor stepchild of IT design/implementation, since it does not add functionality.
- Cybersecurity is not just a technical problem.

Outline

- On Cyber Threats and the Nuclear Enterprise
- The Cyber Nuclear Connection
- Cybersecurity Lessons for Nuclear Modernization
- **Cyber Risks in Selected Nuclear Scenarios**
  - Scenario 1: Cyberattack vs espionage/intelligence gathering
  - Scenario 2: Cyberattacks on ambiguous targets
  - Scenario 3: Cyberattack to damage confidence in nuclear forces
  - Scenario 4: Cyberattack as Counterforce
  - Scenario 5: Social Media and Nuclear Risk
- Designing the Cyber-Nuclear Future
- Closing Thoughts

Irreducible uncertainties/ambiguities—a sampling

- Uncertainty in interpreting signaling message:
  - Restraint may be intended; provocation seen
- Ambiguity in intent of cyber operation
  - Attack vs espionage/intelligence gathering vs operational preparation of battlefield
    - Access and vulnerabilities are the same, payload characteristics determined only upon execution
- Uncertainty about nature of targets in a cyber operation
  - Nuclear vs non-nuclear target
  - Military vs non-military target
  - Direct vs indirect effects
- Difficulty of prompt attribution, possible conflation with other actors

Scenario 1: Cyberattack vs espionage/intelligence gathering

- China announces conduct of nuclear exercises that simulate preparation for execution of a strategic nuclear attack.
  - Exercise involves flushing Chinese mobile missiles from garrison and increases cyber scans of NC3 to improve its security.
- US needs to know what China what China is intending to do given the dispersal of mobile missiles so that the US does not overreact – is this just an exercise or a cover for launching an actual attack?
  - US activates long-dormant implants in China's NC3 system.
- Due to its own intensified defensive efforts, China detects activity from newly activated implants.
- Outcome 1: The US does not trust China's statements that these activities are "only" an exercise, and thus wants to collect its own intelligence—collected surreptitiously without China's knowledge—to ascertain China's true intentions. **The US believes its cyber activities are benign**.
- Outcome 2: China must consider that the US cyber activities could be part of or prelude to a cyber attack on China's NC3 system. Recent discovery of a penetration may correspond to recent emergence of hostile intentions on the part of the US, and thus may force China to shift to war footing. **The Chinese cannot assume that US cyber activities are benign**.
- Both the US and China have incentives to take more aggressive action.

Scenario 2: Cyberattacks on ambiguous targets

- Some targetable systems serve both nuclear and conventional missions.
  - During the initial phases of a conflict, Chinese ballistic missiles are being shot down by US tactical ballistic missile defenses, which accept cueing data from U.S. early warning satellites.
    - China launches cyberattack against U.S. EW satellites, which also provide strategic warning of nuclear attack on U.S. homeland.
    - US is fearful that loss of important strategic warning capability threatens its nuclear forces, and raises nuclear alert levels.
- Attackable entities in cyberspace usually do not have labels indicating their character – nuclear, conventional, or dual use. Attacker must make inferences from data obtained in prior intelligence-gathering.
  - During the initial phases of a conflict, U.S. attacks directed at Chinese conventional C3 accidentally disable Chinese nuclear C3 channel.
    - China fears that loss of this nuclear C3 channel is part of U.S. attempt to sever nuclear forces from CCP authority, and implements standing orders to delegate launch authority to field commanders and thus raising the risk of nuclear escalation.

Scenario 3: Cyberattack to damage confidence in nuclear forces

- As part of a supply chain attack on the U.S. military forces, China inserts malware (or hardware vulnerabilities) in a number of U.S. nuclear weapon delivery platforms.
- During an escalating crisis, China communicates to the U.S. that it has done so and provides clues that enable the U.S. to discover these vulnerabilities—and then informs the U.S. that China has done so on many more U.S. platforms.
- U.S. leaders must then consider whether China's claim is genuine, whether the problem is widespread, whether China has access to additional vulnerabilities that China did not announce, and how to react.

Scenario 4: Cyberattack as Counterforce

- Nuclear weapons capabilities are openly advertised
- Cyber weapons capabilities are often concealed
  - Based on deception; may be treated as weapons for one-time use
- Nation A and B have equal nuclear capabilities.
- Assume for this scenario:
  - Nation A penetrates B's NC2 system (unbeknownst to B)
  - Nation B is at a disadvantage but does not realize it.
  - During crisis,
    - A knows that is stronger than B and does not feel the need to back down.
    - B believes it is equal to A in capability and feels condiment that it can stand fast and raise the stakes beyond what it would be willing to do if it understood its disadvantage.
    - Each side's willingness to escalate creates more risk for the other side.
    - Probably increases that A or B will conclude that deterrence has failed.

Scenario 5: Social Media and Nuclear Risk

- Social media adds to the information environment of nuclear decision-makers by adding unanalyzed, unvetted information feeds.
  - POTUS engages directly with social media
  - Twitter feed in Global Operations Center at USSTRATCOM
- Social media is designed for short, simple messages that target human cognitive vulnerabilities
  - Simple messaging (lacking context) that emphasize audio/visual inputs
  - Trending information gives illusion of consensus
  - Authenticity of provenance not assured
- Classical theories of nuclear deterrence based on economic rationality in decision-making. Psychological evidence to date suggests people systematically deviate from economic rationality in decision.
- Impulsive decision makers are most vulnerable.
  - Reactive, intuitive, fast decision-making vs deliberate, analytical, slow decision-making.
- Adversaries can use social media to confuse or complicate decision making.

For more information…

Herb Lin
Center for International Security and Cooperation
Hoover Institution
Stanford University
650-497-8600
herblin@stanford.edu

Cyber Threats and Nuclear Weapons. Stanford University Press, October 2021.