Cyber Threats and Nuclear Weapons

Herb Lin

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

Senior Research Scholar, Center for International Security and Cooperation

Stanford University

Two types of cyber risk

- Deliberate cyberattack against US may lead to inability to use nuclear weapons when appropriate (e.g., in retaliation)
  - An adversary conducts offensive cyber operations to compromise or degrade a proper and authorized U.S. nuclear use.
- Risk of inadvertent/accidental escalation by the US as result of cyber operation
  - An adversary conducts offensive cyber operations against the US for a non-nuclear purpose and the US misinterprets this act as being for nuclear purposes.
  - An adversary conducts offensive cyber operations to provoke or catalyze an inappropriate use of nuclear weapons (e.g., false flag operation by terrorists)

Possible cyber risks (deliberate) across the enterprise

- Nuclear weapons design and production (and stewardship)
  - corrupted nuclear simulation codes, databases ➔ degraded or unwarranted confidence in judgements of stockpile reliability
- Nuclear delivery systems
  - Cyber vulnerabilities to compromise nuclear delivery systems
- Nuclear command, control, and communications
  - Glitches in early warning/attack assessment (EW/AA) cause false warning of attack; cyberattack causes EW/AA to fail to warn of actual attack
  - Nuclear planning: data corruption leads to suboptimal outcomes
  - Nuclear decision-making
    - Conflations between nuclear/conventional, intelligence/attack preparation ➔ overreaction
    - Corruption of decision-making processes through cyber-enabled information operations
  - Cyber attack or glitches cause disconnect of NCA with nuclear forces
  - Crisis communications with adversaries
- Nuclear operations
  - Execution of operational plans—turning plans into effects

Deliberate risk: What DOD penetration testers could do

- Testers took one hour to gain initial access to a system, one day to gain full control.
- Security measures prevented access by remote users, but not insiders and near-siders.
- Testers took control of the operators' terminals, and …
  - Saw, in real-time, what the operators were seeing on their screens
  - Manipulated the system.
  - Able to disrupt the system and observe how the operators responded
- Testers caused a pop-up message to appear on users' terminals instructing them to insert two quarters to continue operating.
- Testers were able to copy, change, or delete system data, including one team that downloaded 100 gigabytes of data.
- Testers successfully used default passwords for open-source software to achieve access.
- Testers found one system using access controls but also unencrypted communications that allowed them to capture credentials in transit.
- Testers were sometimes detected but no action was taken.
- Testers rebooted a system in operation.

Known vulnerabilities represent a fraction of total vulnerabilities

- Not all programs have been tested
- Tests do not reflect the full range of threats.
- Review sometimes prohibited for proprietary software(!)
- Cybersecurity testing would interfere with operations.

Program officials said systems were secure and discounted some test results as unrealistic(!)

Inadvertent/accidental risk: hypothetical scenarios

Scenario 1: Cyberattack vs espionage/intelligence gathering

- During crisis (or during limited conventional conflict), U.S. detects Russian or Chinese cyber intrusion in nuclear NC3.
  - US is concerned that R/C is attempting to degrade US nuclear capabilities
  - R/C wants to know that US is not preparing to escalate to nuclear.

Scenario 2: Cyberattacks on dual-purpose targets

- Some US systems serve both conventional and nuclear missions.
  - During the initial phases of a conflict, R/C conduct offensive operations to degrade U.S. conventional capabilities.
  - US sees cyberattacks on systems with a nuclear mission, raising concerns that R/C seeks to degrade US nuclear capabilities
  - Examples: US early warning satellites, AEHF communications satellites

In both scenarios, US and R/C perceptions of intent underlying cyber intrusion are entirely different!

Policy implications

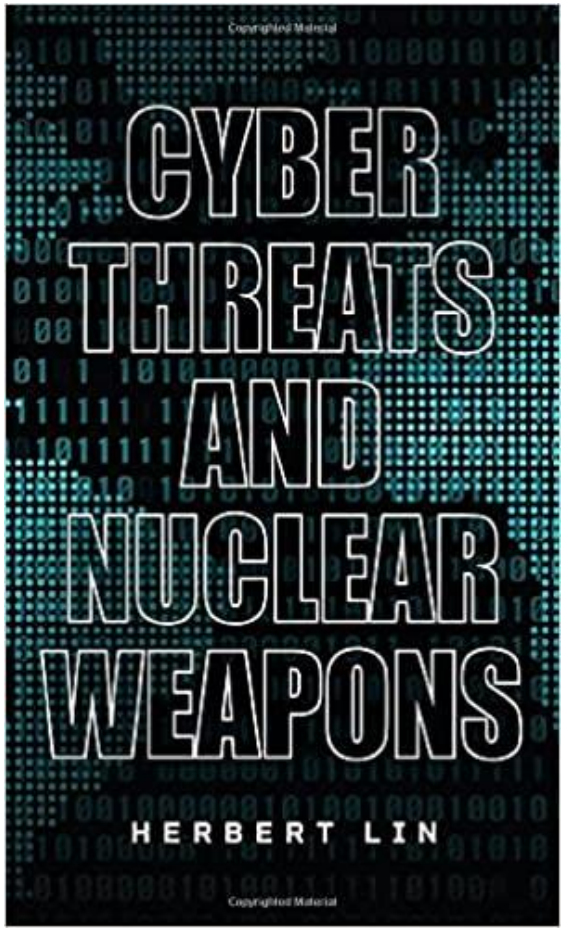
- Entanglement of conventional/nuclear systems raises the risk of inadvertent nuclear escalation.
  - Operational advantages in warfighting must be weighed against an increased escalatory risk.
  - Minimize possibility that cyber attacks on conventional assets will be seen as attacks on nuclear.
    - Require impact statements as part of war plans to ensure consideration of possible adversary conflation between attack on conventional vs nuclear capabilities
    - Require impact statements for U.S. systems regarding nuclear decision making by both adversaries and U.S. decision makers.
  - US STRATCOM should have acquisition authority for nuclear C3.
  - Decision makers should develop an independent backup system to provide the minimum essential core functionality for NC3.
  - Assured communications channels between nuclear adversaries should be maintained.

- Legacy NC3 system has not failed catastrophically, and corrective procedures and technology have been deployed. Can't say the same for any modernized system.
  - System architects should ensure that a modernized system does what a legacy system would do in the same situation and should run both systems until the track record is proven.
  - Downside of keeping two systems running simultaneously for multiple years is high—more people; more cost—but it's worth it.

- The tension between keeping up with a rapidly changing threat environment and maintaining adequate cybersecurity posture cannot be resolved.
  - Designers of modernized computer-driven systems, whether NC3 or weapons platforms, should moderate their appetites for increased functionality.
  - Users and designers must be prepared to make trade-offs between measures to reduce cyber risk and performance requirements.
  - Reduce conventional-nuclear integration (often done to reduce cost)
- Do best practices for cybersecurity
  - All of the cybersecurity problems already identified across the nuclear enterprise should be fixed!
  - Do periodic red-teaming against nuclear-capable systems.
  - All operators should take precautions that would be necessary if they were using systems and networks known to be compromised by an adversary.
    - Inconvenient, but the only way to limit the effects of an actual security compromise.
    - Systems should a possibility of manual control for humans to take over a minimal set of functions when necessary.
- Strategic choices can compensate for additional cyber risk to some extent.
  - Elimination of LOW has some negative effect on credibility of deterrence threat but also allows time for decision making and technical examination of systems to address risk of cyber failure.
  - As Prob [attack on ICBMs] decreases, risk of cyber failure becomes relatively higher.
  - Reconfiguration of U.S. nuclear forces to eliminate such missiles could reduce cyber risks associated with short warning times.

For more information…

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



Stanford University Press
LIN20 discount code