

Cyber Threats and Nuclear Weapons

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

12/15/2021

The two-slide version of the talk

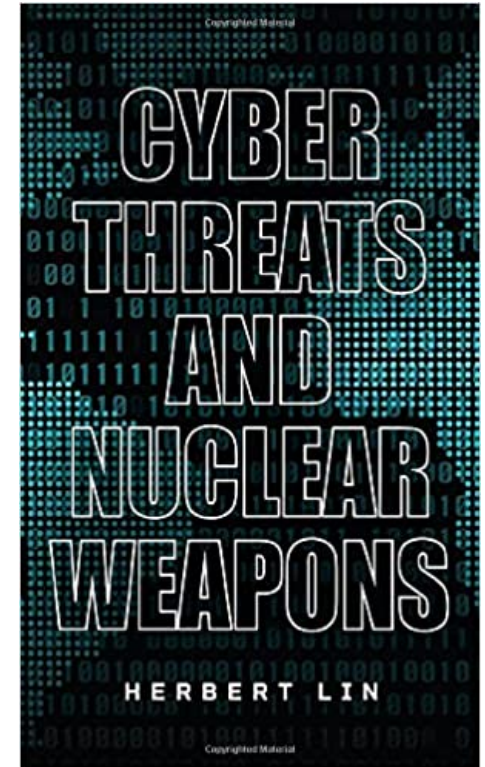
- Two types of cyber risk
 - Deliberate cyberattack against US may lead to inability to use nuclear weapons when appropriate (e.g., in retaliation)
 - An adversary conducts offensive cyber operations to compromise or degrade a proper and authorized U.S. nuclear use.
 - Risk of inadvertent/accidental 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)

- Policy implications

- Entanglement of conventional/nuclear systems raises the risk of inadvertent nuclear escalation.
- Legacy NC3 system has not failed catastrophically, and corrective procedures and technology have been deployed. Can't say the same for any modernized system.
- The tension between keeping up with a rapidly changing threat environment and maintaining adequate cybersecurity posture cannot be resolved.
- Do best practices for cybersecurity
- Strategic choices can compensate for additional cyber risk to some extent.

Outline

- **On Cyber Threats and the Nuclear Enterprise**
 - Cyber Threats
 - The U.S. Nuclear Enterprise
 - Cyber-Nuclear Information Technology
- The Cyber Nuclear Connection
- Cybersecurity Lessons for Nuclear Modernization
- Cyber Risks in Selected Nuclear Scenarios
- Designing the Cyber-Nuclear Future
- Closing Thoughts



Stanford University Press
LIN20 discount code

Cyber Threats

- Offensive cyber capabilities can compromise
 - Confidentiality
 - Integrity
 - Availability
- Technical aspects
 - Penetration (access and vulnerability)
 - Access is impossible to limit to just the good guys
 - Vulnerabilities are everywhere
 - Payload (specifies what effects will occur)
 - Impossible to know intent of penetration until payload executes
 - Possibilities for effect span a very large range (selectivity, timing, scope)
- Offense dominates defense in most pre-war scenarios and many war scenarios.
- 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.
- On strategy
 - Deterrence of low-level cyberattack is impossible, 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 holistic, emergent.
 - Includes many local factors (e.g., failure to practice good cyber hygiene, insider threats, configuration, cultural disincentives) as well as technical factors.

The Nuclear Enterprise

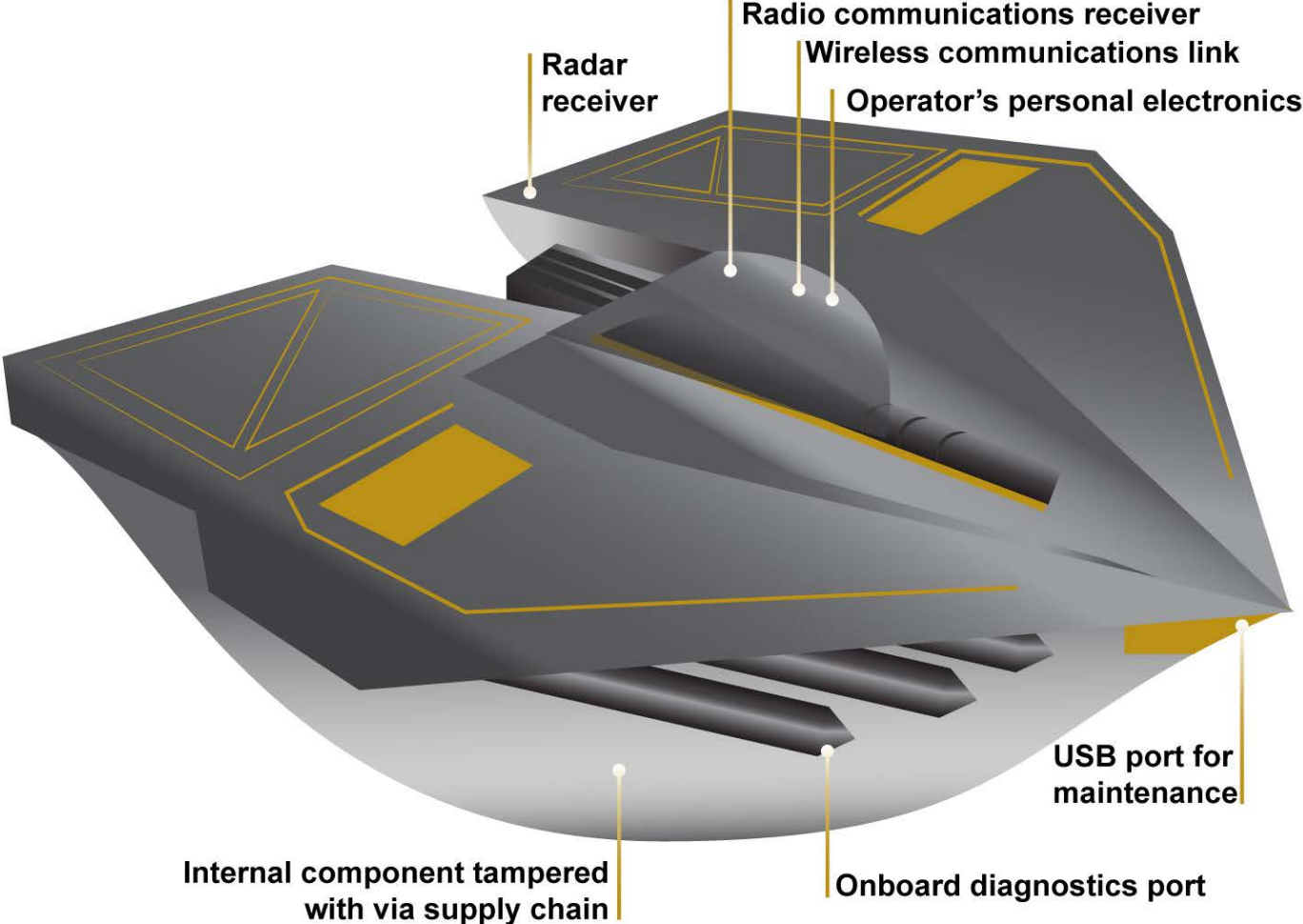
- Nuclear weapons design and production (and stewardship)
- Nuclear delivery systems
- Nuclear command, control, and communications
 - Early warning/attack assessment
 - Nuclear planning
 - Nuclear decision-making
 - Communications: National Command Authority \leftrightarrow US forces, adversary leadership
- Nuclear operations
 - Execution of operational plans—turning plans into effects
- Extensive nuclear modernization program starting now.

Information technology is (increasingly) critical to **all** of these elements.

Possible cyber risks across the enterprise

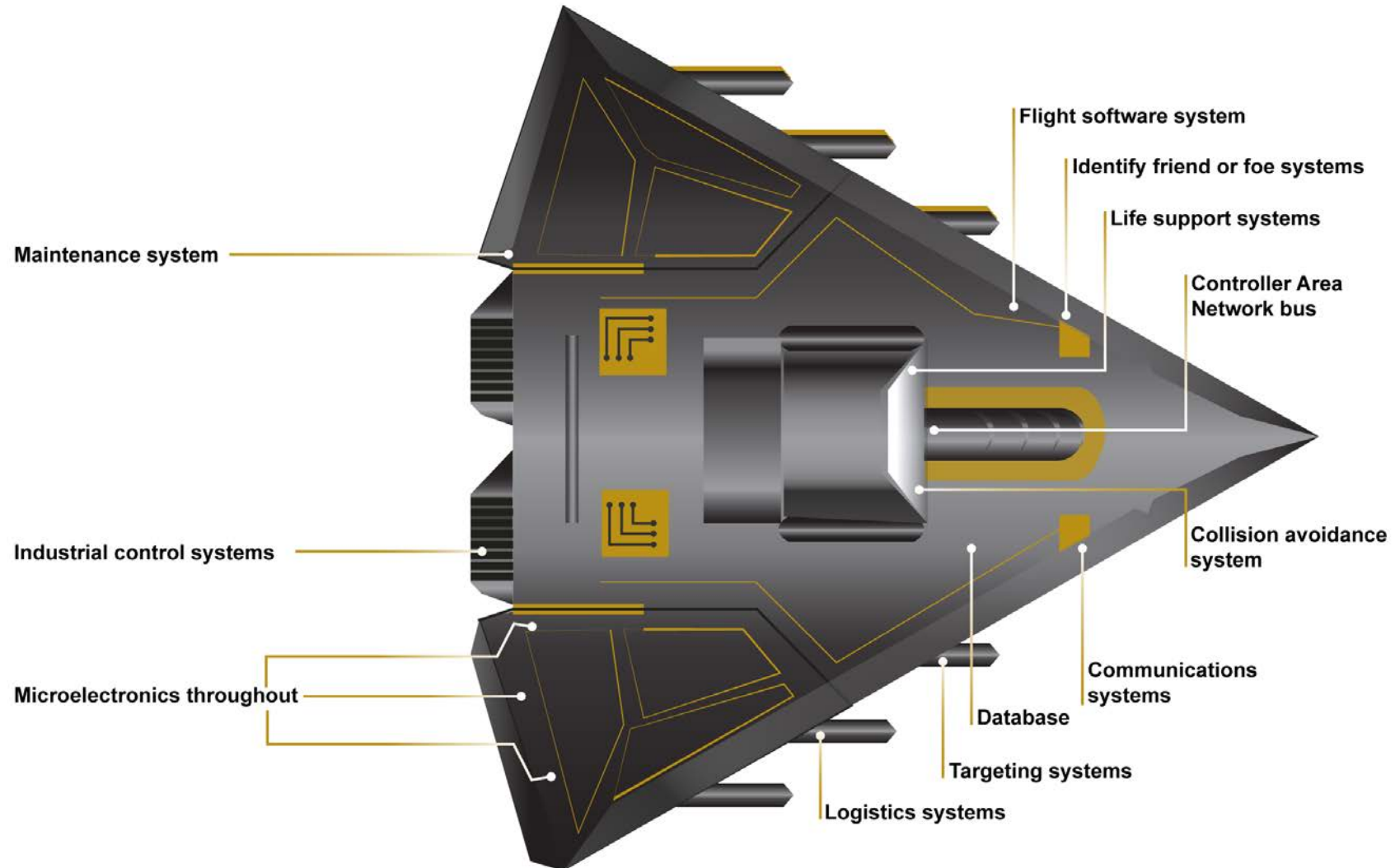
- Nuclear weapons design and production (and stewardship)
 - corrupted nuclear simulation codes, databases → degraded or unwarranted confidence in judgements of stockpile reliability
- Nuclear delivery systems
 - Cyber vulnerabilities to compromise nuclear delivery systems
- Nuclear command, control, 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

Possible access points in a weapons system



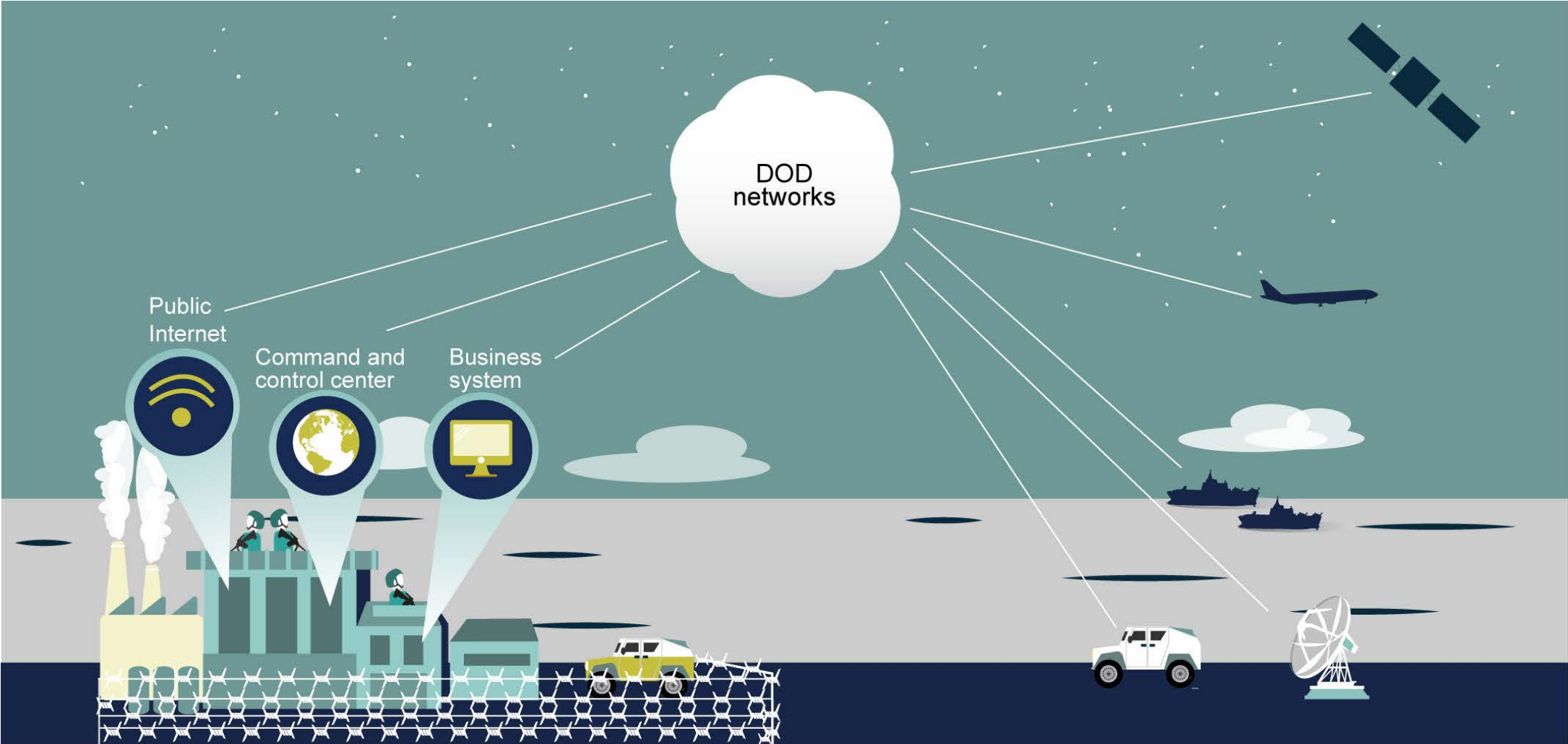
Source: GAO analysis of Department of Defense information. | GAO-19-128

Possible points of vulnerability in a weapons system



Source: GAO analysis of Department of Defense information. | GAO-19-128

Possible connections of DOD systems to the “outside” world



Source: GAO analysis of Department of Defense information. | GAO-19-128

What DOD penetration testers could do with simple tools

- 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(!)

Outline

- On Cyber Threats and the Nuclear Enterprise
- **The Cyber Nuclear Connection**
 - Information technology and NC3
 - Modernization and cyberization
- Cybersecurity Lessons for Nuclear Modernization
- Cyber Risks in Selected Nuclear Scenarios
- Designing the Cyber-Nuclear Future
- Closing Thoughts

Information Technology and NC3

- IT is increasingly the lifeblood of military organization and power, enabling commanders to direct appropriate amounts of force where and when needed.
 - The U.S. nuclear enterprise is not an exception.
- U.S. NC3 rely on computers for virtually every aspect of operations.
 - Early-warning radars, launch facilities, chain of command communications
 - That these technologies improve U.S. operations makes them natural targets for adversaries
 - Attacks on NC3 can generate fog of war and lead to unintended escalation.
- The cyber security and resilience of U.S. nuclear forces (especially NC3) is of comparable importance to that of the reliability and performance of U.S. nuclear weapons themselves. (cf DSB 2017)

Attacks on NC3

- Fundamental principle of nuclear command and control – NEVER used nukes without proper orders; ALWAYS use when properly ordered.
 - Note tension between ALWAYS and NEVER
 - Military emphasizes ALWAYS; civilians emphasize NEVER
- Attack on “ALWAYS” requirement prevents or otherwise interferes with a properly authorized launch order.
 - Cyberattack or glitch may sever communications.
 - Authentication procedures of key individuals may be compromised or made cumbersome.
 - Cyberattacks (or threat of cyberattacks) to degrade confidence in nuclear forces.
 - Orders may be compromised (e.g., improperly altered)
 - Communications with outside world may trick insiders into operating foolishly (e.g., questioning a valid order).
- Attack on “NEVER” requirement enables the improper issuance of a valid launch order.
 - Insider is able to spoof authentication of POTUS.
 - Cyberattack enables wireless communication with ICBM launch control centers to launch as if a valid order were coming from airborne command post.
 - Cyberattacks are likely to focus on compromises and trickery of people in launch command chain.

- Corruption of or interference with of communications systems needed to plan and coordinate. Confidentiality here particularly important.
 - National leadership (US and foreign)
 - Military leadership
 - Critical infrastructure providers
 - ...
- Vulnerabilities in nuclear planning
 - Coordination of assets requires large databases.
 - Databases used for planning can be corrupted by cyber means.
 - Corruption may not be detected for a long time (slow corruption also affects backups).
 - Operational plans based on these databases will not be executed optimally.
- Communications with adversary leadership
 - Not usually considered part of NC3, but essential to conflict termination
 - How to ensure communications with adversary
 - in a nuclear environment
 - with leaders whose electromagnetic emissions could be geolocated and thus targeted
 - whose communication systems will not have been designed for interoperability

Outline

- On Cyber Threats and the Nuclear Enterprise
- The Cyber Nuclear Connection
- **Cybersecurity Lessons for Nuclear Modernization**
 - Complexity and Security
 - Building complex systems with rapidly changing requirements
 - Maintaining security vs getting work done
- Cyber Risks in Selected Nuclear Scenarios
- Designing the Cyber-Nuclear Future
- Closing Thoughts

Complexity and Security

- Appetite for increased functionality afforded by information technology is unlimited.
 - Systems will be increasingly insecure if we do not find a way to moderate/curb/manage the appetite for functionality.
- Increased functionality of information technology necessarily entails increased complexity of design and implementation.
 - A larger, complex system necessarily creates a larger attack surface.
 - Consider difference in complexity of conventional-nuclear integration vs mostly nuclear NC3.
- Complexity is the enemy of security.
 - System designers can choose between making:
 1. A system that is so simple it obviously has no errors.
 2. A system that is so complex it has no obvious errors.
 - #2 is a bad way to design a system for NC3.

Building complex systems when requirements change rapidly

- “We must design an [NC3] architecture that is flexible, resilient, and adaptive and can evolve with the threat and advances in technology.”
 - ✓ Elizabeth Durham-Ruiz, director of US Strategic Command’s NC3 Enterprise Center, 2019
- “As we move towards the next generation of NC3, we must work with industry to rapidly prototype new technologies.”
 - ✓ Adm Charles Richard, CDR USSTRATCOM, 2020
- Understandable sentiments, but **cybersecurity is inherently a drag on development schedules that does not add to the system’s utility for the end user.** Implications:
 - Always faster and cheaper to develop a less secure system of a given functionality than a more secure one of equal functionality, OR
 - Choose between a less secure system of greater functionality and a more secure one of lesser functionality.
- Silicon Valley techniques for software development do not change these fundamental tradeoffs.
 - SV does not produce software that is robust and secure, though it *is* functional.
 - SV has tangible metric for goodness of product—user willingness to pay for using it.
 - NC3 has multiple user communities, with conflicting requirements at different levels.
 - Ongoing challenge to distinguish between requirements that should be changed, can be changed, and should never be changed – SV techniques for “agile devops” not optimized for nuclear environment

Being secure or getting work done

- Trade-off between security and productivity
 - “It is possible to have convenience if you want to tolerate insecurity, but if you want security, you must be prepared for inconvenience.”
 - ✓ Gen BW Chidlaw, CDR CONAD, 1954 (CONAD predecessor to NORAD)
 - Day-to-day incentives drive towards convenience at expense of security
 - Consider passwords written on Post-its, spare keys hidden under doormats, or emailing attachments to avoid multiple-step intranet file transfer.
- Because military is more aligned with “always use with proper authorization” rather than “never use without proper authorization,” military operators have more incentives to compromise security functions.
 - In mid 1970s, PAL codes on Minuteman III missiles were set to all zeros.

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
- 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

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!

Outline

- On Cyber Threats and the Nuclear Enterprise
- The Cyber Nuclear Connection
- Cybersecurity Lessons for Nuclear Modernization
- Cyber Risks in Selected Nuclear Scenarios
- **Designing the Cyber-Nuclear Future: Policy Implications**
- Moving Forward

Designing the Cyber-Nuclear Future: 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.
 - Designers of modernized computer-driven systems, whether NC3 or weapons platforms, should moderate their appetites for increased functionality.
 - US STRATCOM should have acquisition authority for nuclear C3.
 - Decision makers should identify the minimum essential core functionality for NC3 and develop an independent backup system if primary systems are compromised.
 - 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.

- The tension between keeping up with a rapidly changing threat environment and maintaining adequate cybersecurity posture cannot be resolved.
 - Users and designers must be prepared to make trade-offs between measures to reduce cyber risk and performance requirements.
- Do best practices for cybersecurity
 - All of the cybersecurity problems already identified across the entire nuclear enterprise should be fixed!
 - All operators should take precautions that would be necessary if they were using systems and networks known to be compromised by an adversary.
- 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 well reduce cyber risks associated with short warning times.

Outline

- On Cyber Threats and the Nuclear Enterprise
- The Cyber Nuclear Connection
- Cybersecurity Lessons for Nuclear Modernization
- Cyber Risks in Selected Nuclear Scenarios
- Designing the Cyber-Nuclear Future
- **Closing Thoughts**

Closing Thoughts

- On the importance of mitigating cyber risk
 - Senior management in DOD is aware, at least rhetorically:
 - “Our NC2 hardware infrastructure fails if the NC3 fails due to a cyber-attack. . . Cyber defense is not a ‘trade space’ discussion; it is an additive necessity in today’s technology centric world.”
 - Admiral Charles Richard, Commander, U.S. Strategic Command, testimony before the Senate Committee on Armed Services, 13 February 2020.
 - Lowest-level operators are also aware of cyber risks (since they must cope with them all the time)
 - Mid-level personnel are most oblivious.
- On the difference between cyber threats against nuclear forces vs threats against conventional forces
 - Likely to be more sophisticated and better resourced
 - All-out cyber attack from technically sophisticated nation-state can target the entire supply chain from chip fabrication & requirements specification to implementation and operations.
 - Stakes are higher because nuclear weapons pose existential threat.

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.

LIN20 discount code if ordered from SUP website.