The growing prominence of cyberattacks raises the risk that the systems undergirding nuclear weapons infrastructure could potentially be vulnerable. Cyber-induced uncertainty over whether nuclear-armed states can assure the authorized use of nuclear weapons and prevent the accidental, mistaken, or unauthorized use of nuclear weapons has significant policy ramifications that must be addressed, especially in the context of the upcoming modernization of U.S. nuclear forces. I examined the technological infrastructure supporting nuclear command & control using available open source materials. Technologies were organized as belonging to nuclear employment planning systems, early warning systems, communications systems, or delivery systems. Subsequently, I then analyzed these systems for potential vulnerabilities and identified the nuclear policies that were implicated by these vulnerabilities.

Nuclear planning systems generate target sets and operational parameters for the use of nuclear weapons. Without predetermined attack plans, determining the optimal nuclear option is extremely impractical. Reducing the integrity of launch plans by changing launch times and target coordinates could pose significant risk to the credibility of the strategic deterrent, while cyber-enabled espionage could enable adversaries to develop more effective countermeasures against nuclear weapons. *Early warning systems* provide operational awareness, including the ability to detect an incoming nuclear attack. The U.S. employs both radar and satellites in this capacity. The threat posed by cyberattacks is twofold: legitimate warnings of nuclear missiles could be suppressed to reduce retaliatory capability, or false warnings could be triggered by a third party state or terrorist group to catalyze a genuine nuclear exchange. *Communications systems* relay Emergency Action Messages (EAMs) between the National Command Authority (NCA) and nuclear forces. Cyberattacks could degrade or disrupt EAMs in transit, rendering them unintelligible and preventing the execution of proper launch orders. Spoofing attacks could also substitute improper orders, though this is less likely for launch orders. *Delivery systems* are responsible for arming nuclear weapons, transporting them to their targets, and successfully detonating them. These systems include not only missiles and bombs, but also the supporting technologies. These systems could be compromised by the introduction of malware into the supply chain. These logic bombs could target fire-control software or more mundane systems such as sanitation on submarines, potentially forcing the premature termination of deterrent patrols.

A shift to a *no first use and sole purpose policies* may reduce the likelihood of an accidental nuclear war resulting from false alarms or the spoofing of early warning systems, by reassuring other states about U.S. intent. Without concurrent changes in posture or alert status, these policy changes may only have negligible effect. However, such a stance may undermine extended deterrence and would reduce the ability of the U.S. to deter non-nuclear WMD or conventional attacks.

Reducing the *alert status* of ICBMs, which are most subject to "use them or lose them" pressures, could decrease the likelihood of mistaking a false alarm for a legitimate nuclear attack due to the compression of decision making time. Similarly, adopting a launch after detonation policy would eliminate the chance of an accidental nuclear war over false warnings and increase Presidential decision time in the event of an actual nuclear war. A launch after detonation policy would reduce the potency of a U.S. second strike, especially with regards to the poor survivability of ICBMs and, to a lesser extent, strategic bombers. However, reductions in alert status have been criticized for having destabilizing potential in a crisis; the re-alerting of nuclear weapons may induce an adversary to strike preemptively.

Differential levels of cyber risk for each leg of the triad (strategic bombers, intercontinental ballistic missiles, & submarine launched ballistic missiles) could impact future *force structure* decisions and even precipitate a move to a dyad or monad. Additionally, there is a trade-off between ensuring nuclear capabilities and reducing the risk of an accidental, mistaken, or unauthorized nuclear launch. Having multiple legs increases the potential for a vulnerability to be found and exploited by virtue of the greater attack surface, while a triad minimizes the risk of a comprehensively disabling cyberattack subjecting the U.S. to nuclear coercion or a first strike.

The cyber threat could force changes on U.S. counterforce targeting doctrine or on its management of more complex nuclear operations involving two-way communications. *Operational policies* may have to be adjusted to ensure proper execution of missions in a communications-degraded environment, especially in the context of spoofed EAMs.

I'd like to acknowledge the Nuclear Threat Initiative, where I conducted and presented my research as a Scientific & Technical Affairs Intern.

RSAConference Security Scholar

Hacking the Bomb: Analyzing the Cyber Threat to Nuclear Command & Control

Andreas Constantine Pavlou
Stanford University

Problem Statement & Approach

- Cyberattacks raise the risk that the systems undergirding nuclear weapons infrastructure could potentially be vulnerable.
- Cyber-induced uncertainty over whether nuclear-armed states can assure the authorized use of nuclear weapons and prevent the accidental, mistaken, or unauthorized use of nuclear weapons has significant policy ramifications that must be addressed, especially in the context of the upcoming modernization of U.S. nuclear forces.
- I examined the technological infrastructure supporting nuclear command & control using available open source materials. Technologies were organized as belonging to nuclear employment planning systems, early warning systems, communications systems, or delivery systems.
- I then analyzed these systems for potential vulnerabilities and identified the nuclear policies that were implicated by these vulnerabilities.

Results: Nuclear Weapons Systems

- Nuclear planning systems generate target sets and operational parameters for the use of nuclear weapons.
- Reducing the integrity of launch plans by changing launch times and target coordinates could pose a risk to the credibility of the strategic deterrent.

- Early warning systems provide operational awareness, including the ability to detect an incoming nuclear attack.
- The threat posed by cyberattacks is twofold: legitimate warnings of nuclear missiles could be suppressed to reduce retaliatory capability, or false warnings could be triggered by a third party state or terrorist group to catalyze a genuine nuclear exchange.

- Communications systems relay Emergency Action Messages (EAMs) between the National Command Authority and nuclear forces.
- Cyberattacks could degrade EAMs in transit, preventing the execution of proper launch orders. Spoofing attacks could potentially substitute improper orders.

- Delivery systems are responsible for arming nuclear weapons, transporting them to their targets, and successfully detonating them.
- These systems could be compromised by the introduction of malware into the supply chain.

Results: Nuclear Weapons Policies

Declaratory Policy

- A shift to a no first use and sole purpose policies may reduce the likelihood of an accidental nuclear war resulting from false alarms or the spoofing of early warning systems, by reassuring other states about U.S. intent.
- However, such a stance may undermine extended deterrence and would reduce the ability of the U.S. to deter non-nuclear WMD or massive conventional attacks via the threat of nuclear retaliation.

Nuclear Posture & Alert Status

- Reducing the alert status of ICBMs, which are most subject to "use them or lose them" pressures, could decrease the likelihood of mistaking a false alarm for a legitimate nuclear attack due to the compression of decision making time.
- Adopting a launch after detonation policy would eliminate the chance of an accidental nuclear war over false warnings and significantly increase Presidential decision time in the event of an actual nuclear war.
- A launch after detonation policy would reduce the potency of a U.S. second strike, especially with regards to the poor survivability of ICBMs and, to a lesser extent, strategic bombers. However, reductions in alert status may have destabilizing potential in a crisis; the re-alerting of nuclear weapons may induce an adversary to strike preemptively.

Nuclear Force Structure

- Differential levels of cyber risk for each leg of the triad (strategic bombers, intercontinental ballistic missiles, & submarine launched ballistic missiles) could impact future force structure decisions and even precipitate a move to a dyad or monad.
- There is a trade-off between ensuring nuclear capabilities and reducing the risk of an accidental, mistaken, or unauthorized nuclear launch. Having multiple legs increases the potential for a vulnerability to be found and exploited by virtue of the greater attack surface, while a triad minimizes the risk of a comprehensively disabling cyberattack subjecting the U.S. to nuclear coercion.

Operational Policy

- The cyber threat could force changes on U.S. counterforce targeting doctrine or on its management of more complex nuclear operations involving two-way communications.
- Operational policies may have to be adjusted to ensure proper execution of missions in a communications-degraded environment, especially in the context of spoofed EAMs.