Defense One

As America's Nukes and Sensors Get More Connected, the Risk of Cyber Attack Is Growing

By Patrick Tucker

January 17, 2018

Building nuclear weapons and warning systems that can be relied upon is harder than it was during the Cold War, thanks to the growing number of digital connections between various parts of the nuclear enterprise. Those links are intended to improve everything from commanders' response times to the accuracy of missile defenses, but they also provide more avenues of attack and make it harder to know your exact level of readiness, according to new reports from U.S. Air Force advisors and a London think tank.

The U.S. military is planning to revamp its nuclear weapons arsenal, including the gear that would detect enemy launches and the command-and-control systems that would facilitate a response. A draft of the Nuclear Posture Review that leaked to the *Huffington Post* urges the United States to "Strengthen Protection Against Cyber Threats" in order to "ensure the continuing availability of U.S.-produced information technology necessary for the [nuclear command, control, and communication] system." But it also calls for a lot more digital links between the various parts of the nuclear enterprise, particularly among the systems intended to spot enemy missiles.

More sensors trading more data can give leaders more time to respond to launch reports, help prevent false alarms, increase the chance of intercepting incoming missiles, and give leaders more time to decide how to respond to data indicating an incoming missile. But more links and data exchanges also makes cybersecurity harder.

Last September, the Air Force Science Board released a major study into "surety" for next-generation nuclear weapons — that is, making sure that control networks can't be incapacitated or, worse, made to convey incorrect information. The board, which hadn't certified a nuclear program since the B-2 bomber, found that surety has become a bigger task in the era of interconnected weapons.

Board chair James Chow noted that the United States is about to build many new weapons and pieces of equipment, including a new bomber, new ICBMs, and new nuclear cruise missiles.

"These nuclear systems are increasingly reliant on cyber-enabled components. The adversary has advanced its capability to threaten those nuclear weapon systems, including that cyber and supply chain. The demand for the capability to certify this advanced number … of new systems that will be coming online and be able to protect them in this new type of threat environment …there certainly were resource constraints that might limit their ability to certify that number of upcoming systems," Chow told reporters.

When asked if more digital interlinks among weapons made it harder to certify and secure them, Chow took a diplomatic evasion. Difficult was not the right word. "It's more complicated," he said. "The proliferation of those sorts of technologies, its a fact of life of on our weapons systems. There are new tools to provide cyber resilience to reduce your risk… the study found we need to consider those and come up with metrics that can help the decision maker." Resilience in the context of digital and computer program functioning generally means ensuring that programs or systems continue to function as designed even when under cyber attack.

A new report from London-based think tank Chatham House notes that while some risks associated with nuclear weapons have been around for decades, "new technology has exacerbated these risks. With each new digital component embedded in the nuclear weapons enterprise, new threat vectors may emerge."

During the Cold War, for instance, the United States could much better guarantee the provenance of the microchips, microelectronic components, and other pieces of computer and digital equipment. In 2018, that becomes harder to do, especially as you loop in more pieces of complex equipment.

It's not just a U.S. problem. Take North Korea, which imports almost all of the camera equipment, pressure transmitters, and computer parts used in its nuclear weapons program.

"With such a number of outsourced items it seems clear that the North Korean missile programme is vulnerable to cyber infiltration, at least through the supply chain," says the report.

"The vulnerability of North Korea's nuclear weapons programme to cyber infiltration in turn raises questions regarding the cybersecurity of other nations that possess nuclear weapons," the report concludes.

The review says that the U.S. should rely on domestic sourcing for components, but as the number of sensors, satellites, and pieces of IT aimed at the North Korean problem grows — and as those pieces become more complex — that becomes harder to do.

Consider the Space-Based Infrared System satellites, which watch for the heat of rocket launches and missile tests. Unlike the older constellation they are replacing, SBIRS satellites have two sensor systems: one to scan wide areas and one to zoom in on suspected launches. They are intended to give military commanders more time to react, and to feed tracking data to anti-missile defenses.

"I can think of two areas of vulnerability here," said Chatham House researcher Beyza Unal. Both concern SBIRS' ground-based command-and-control links and its backup mission control station. "One is the physical security of these locations from any incoming attacks, especially considering the possibility of a low-yield nuclear weapons use or limited nuclear war scenario. Second is the possibility of manipulation of hardware or software in these locations. What happens if hardware or software is compromised? The Enhance Integrated Tactical Warning and Attack Assessment—which is mentioned both in the [posture review] and in our report—may not be able to detect attacks in a timely manner or the information it receives may not be reliable or have been compromised," Unal said.

So cyber insecurity is more than just a complicating factor for the United States as it builds new nuclear weapons. It changes the entire cost-benefit analysis. North Korea doesn't have to hack locations or components, it just has to credibly threaten to do so. If you can't be sure that your nuclear response has not been hacked, then you aren't effectively deterring anything. And that's the only reason to have nuclear weapons.

"A compromised nuclear system that cannot be trusted and lacks credibility will undermine nuclear deterrence and its rationale. Additionally, the assurances that nuclear weapons states make to allies would likely lose their reliability if an adversary could successfully hack into the nuclear weapons systems on which several countries rely," the report notes.

By Patrick Tucker // Patrick Tucker is technology editor for Defense One. He's also the author of The Naked Future: What Happens in a World That Anticipates Your Every Move? (Current, 2014). Previously, Tucker was deputy editor for *The Futurist* for nine years. Tucker has written about emerging technology in *Slate*, *The Sun*, *MIT Technology Review*, *Wilson Quarterly*, *The American Legion Magazine*, *BBC News Magazine*, *Utne Reader*, and elsewhere.

January 17, 2018

https://www.defenseone.com/technology/2018/01/americas-nukes-and-sensors-get-more-connected-risk-cyber-attack-growing/145229/