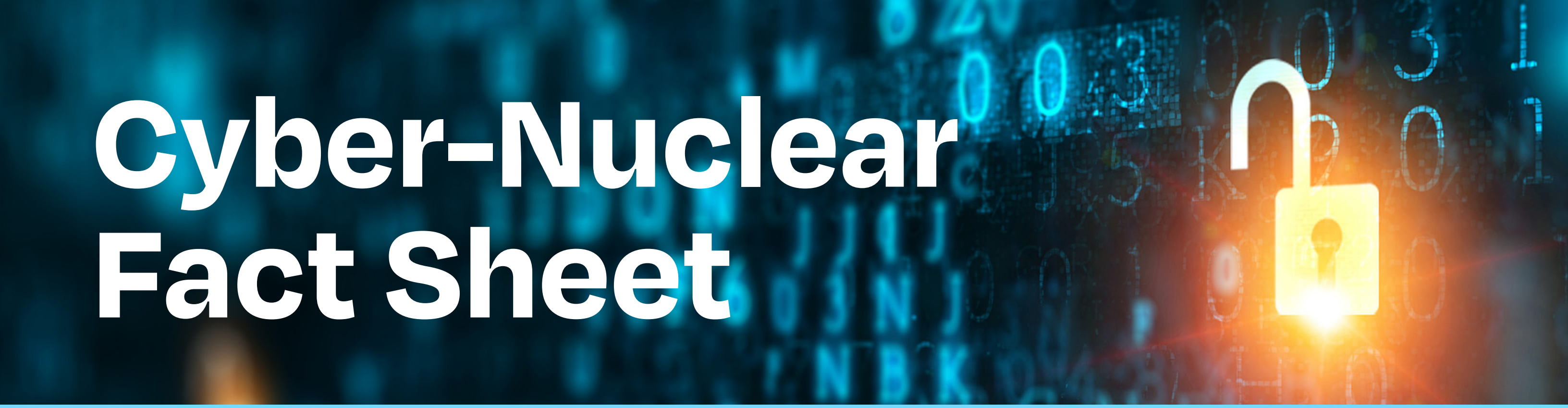
Cyber-Nuclear Fact Sheet



What is the problem?

Nuclear weapons can be hacked.

Nuclear and tech experts know that all digital systems are at risk for cyberattacks—including nuclear weapons systems. That means our own warheads, delivery vehicles, and the technology we use to control them are prime targets for hackers. The systems we rely on to detect incoming attacks are susceptible, too. These cyber vulnerabilities in nuclear weapons systems undermine the safety and security of nuclear weapons around the world.

Since the first explosion of a nuclear weapon in 1945, the world has avoided an accidental, unauthorized, or miscalculated launch. But there have been dozens of close calls—and in today's cyber age, our luck could run out. Watch this explainer video to learn more.

Why does it matter?

A nuclear weapon detonated anywhere, by any means, would be catastrophic for us all.

Unlike the many hacks and cyberattacks we have grown accustomed to in everyday life, a successful cyberattack on a nuclear weapon system could result in a nuclear detonation or even lead to an all-out nuclear war.

Russia and the United States have the vast majority of the world's nuclear weapons, and tensions are high. Here are three ways cyber threats could increase the chance of miscalculation and lead to nuclear use in the U.S.-Russia context:

1. An anonymous, malicious actor could interfere in U.S. or Russian nuclear command and control systems and set off an unintended and dangerous chain of actions and reactions.
2. A hacker could spoof the U.S. or Russian early warning system, leading either country to believe they're under attack. With just minutes to decide whether to use nuclear weapons in response to an incoming attack, a leader could launch a retaliatory strike before there is time to confirm that the alert is real.
3. A cyberattack on a communication system or other element of nuclear weapons infrastructure could render the United States or Russia unable to ensure that their nuclear weapons remain under proper control.

This problem isn't unique to the United States or Russia. Nine countries have nuclear weapons, and a compromised nuclear system anywhere creates a nuclear risk everywhere.

Why should we pay attention now?

The spread of new cyber capabilities combined with the increasing digitization of nuclear systems increases the likelihood of dangerous cyber-nuclear attacks.

The United States and other countries with nuclear weapons are swapping outdated technologies for modern digital components as part of broad nuclear modernization programs. But according to the U.S. Government Accountability Office, at least in the U.S., these technologies could create more problems than they solve: there are “mission critical cyber vulnerabilities” in nearly all the weapons systems under development by the Department of Defense.

Is there any good news?

Yes. For the first time since the end of the Cold War, the United States is formally reviewing its nuclear “failsafe” protocols and procedures. Failsafe measures can prevent or mitigate dangerous unintended nuclear incidents. It is important to regularly update such measures to account for new technologies and evolving threats.

What can be done?

Fortunately, the U.S. government is taking this threat seriously. Going forward, it must ensure the failsafe review is credible, subject to Congressional oversight, and involves top experts from within and outside of the government. There also are critical actions that all countries with nuclear weapons should take:

- Make cybersecurity a priority during all nuclear modernization efforts
- Review and modify, where appropriate, nuclear policies to account for cyber-nuclear threats and, as much as possible, to give the chain-of-command more time to evaluate the situation and review intelligence before considering the use of nuclear weapons in a crisis

Ultimately, the only way to ensure nuclear weapons are never used is to continue reducing the number of weapons globally through verifiable arms control agreements, until we eventually eliminate them entirely.

What can you do?

Help us spread the word.

We’re in a risky situation, and the stakes are high. We need to spread the word that the cybersecurity of our nuclear weapons is a top national security issue. Here’s how you can help:

1. Contact your elected officials and ask them to pay close attention to the failsafe review to ensure that it is as thorough and robust as possible; tell them you support efforts to expand and strengthen existing arms control agreements and pursue new ones.
2. Share this explainer video and this fact page with your friends, family, and colleagues.
3. Get involved with grassroots organizations working toward the elimination of nuclear weapons or start your own network.

All of us have a part to play in making the world—and cyber world—a safer place.

For additional information:

- NTI Cyber Nuclear Report
- NTI Modernization Report
- UNIDIR: The Cyber-Nuclear Nexus
- *Command and Control* by Eric Schlosser (book)
- *Cyber Threats and Nuclear Weapons* by Herbert Lin (book)
- *Hacking the Bomb* by Andrew Futter (book)