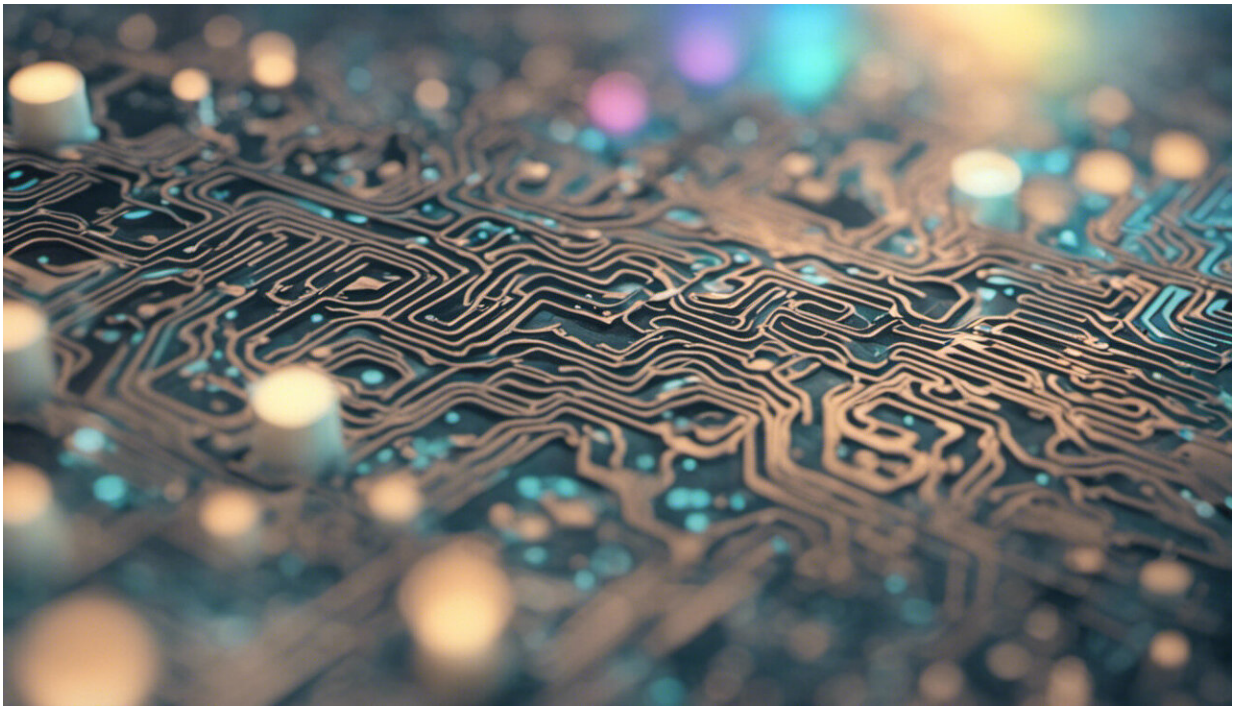
A cyberattack could wreak destruction comparable to a nuclear weapon

August 19 2019, by Jeremy Straub



Credit: AI-generated image (disclaimer)

People around the world may be worried about nuclear tensions rising, but I think they're missing the fact that a major cyberattack could be just as damaging—and hackers are already laying the groundwork.

With the U.S. and Russia pulling out of a key nuclear weapons pact

—and beginning to develop new nuclear weapons—plus Iran tensions and North Korea again test-launching missiles, the global threat to civilization is high. Some fear a new nuclear arms race.

That threat is serious—but another could be as serious, and is less visible to the public. So far, most of the well-known hacking incidents, even those with foreign government backing, have done little more than steal data. Unfortunately, there are signs that hackers have placed malicious software inside U.S. power and water systems, where it's lying in wait, ready to be triggered. The U.S. military has also reportedly penetrated the computers that control Russian electrical systems.

Many intrusions already

As someone who studies cybersecurity and information warfare, I'm concerned that a cyberattack with widespread impact, an intrusion in one area that spreads to others or a combination of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon.

Unlike a nuclear weapon, which would vaporize people within 100 feet and kill almost everyone within a half-mile, the death toll from most cyberattacks would be slower. People might die from a lack of food, power or gas for heat or from car crashes resulting from a corrupted traffic light system. This could happen over a wide area, resulting in mass injury and even deaths.

This might sound alarmist, but look at what has been happening in recent years, in the U.S. and around the world.

In early 2016, hackers took control of a U.S. treatment plant for drinking water, and changed the chemical mixture used to purify the water. If changes had been made—and gone unnoticed—this could have led to

poisonings, an unusable water supply and a lack of water.

A cyberattack wouldn’t be launched from a nuclear operator’s console, like the one shown here from the decommissioned Oscar Zero site, but rather through cyberspace. A human might not even be required. Credit: Jeremy Straub

In 2016 and 2017, hackers shut down major sections of the power grid in Ukraine. This attack was milder than it could have been, as no equipment was destroyed during it, despite the ability to do so. Officials think it was designed to send a message. In 2018, unknown cybercriminals gained access throughout the United Kingdom's electricity system; in 2019 a similar incursion may have penetrated the U.S. grid.

In August 2017, a Saudi Arabian petrochemical plant was hit by hackers who tried to blow up equipment by taking control of the same types of electronics used in industrial facilities of all kinds throughout the world. Just a few months later, hackers shut down monitoring systems for oil and gas pipelines across the U.S. This primarily caused logistical problems—but it showed how an insecure contractor's systems could potentially cause problems for primary ones.

The FBI has even warned that hackers are targeting nuclear facilities. A compromised nuclear facility could result in the discharge of radioactive material, chemicals or even possibly a reactor meltdown. A cyberattack could cause an event similar to the incident in Chernobyl. That explosion, caused by inadvertent error, resulted in 50 deaths and evacuation of 120,000 and has left parts of the region uninhabitable for thousands of years into the future.

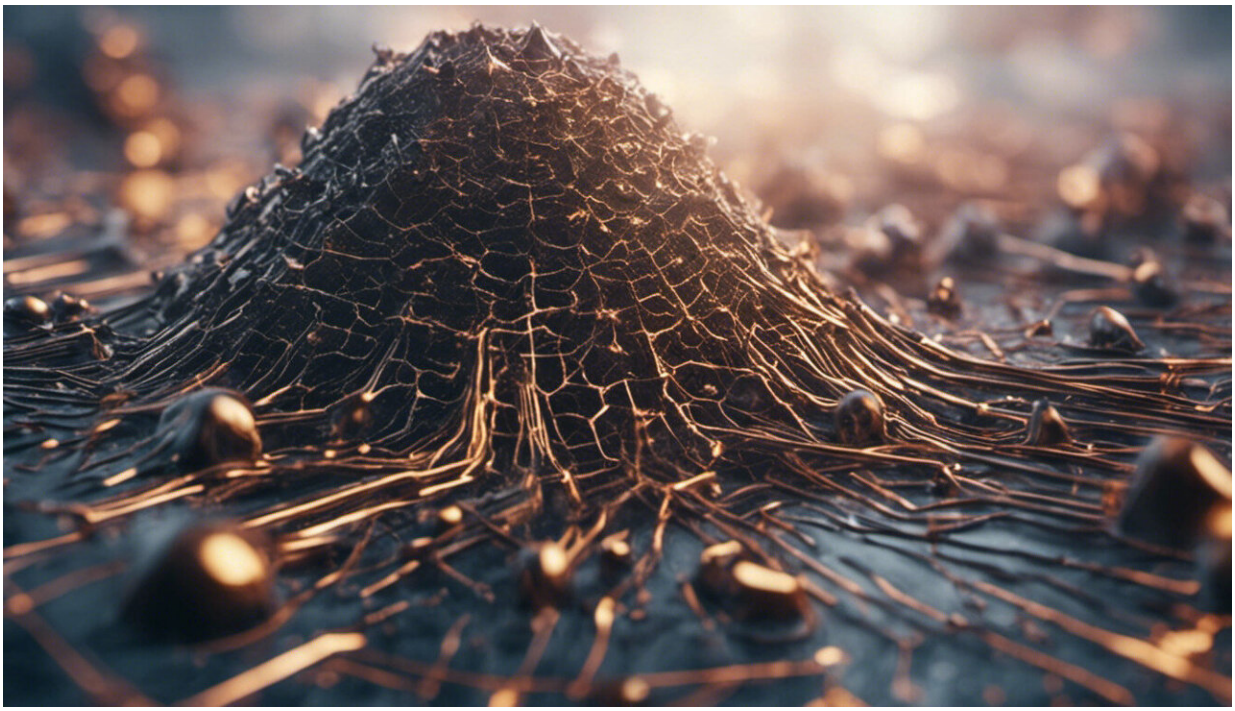
Mutual assured destruction

My concern is not intended to downplay the devastating and immediate effects of a nuclear attack. Rather, it's to point out that some of the international protections against nuclear conflicts don't exist for cyberattacks. For instance, the idea of "mutual assured destruction" suggests that no country should launch a nuclear weapon at another nuclear-armed nation: The launch would likely be detected, and the target nation would launch its own weapons in response, destroying both nations.

Cyberattackers have fewer inhibitions. For one thing, it's much easier to disguise the source of a digital incursion than it is to hide where a missile blasted off from. Further, cyberwarfare can start small, targeting even a single phone or laptop. Larger attacks might target businesses, such as banks or hotels, or a government agency. But those aren't enough to escalate a conflict to the nuclear scale.

Nuclear grade cyberattacks

There are three basic scenarios for how a nuclear grade cyberattack might develop. It could start modestly, with one country's intelligence service stealing, deleting or compromising another nation's military data. Successive rounds of retaliation could expand the scope of the attacks and the severity of the damage to civilian life.



Credit: AI-generated image (disclaimer)

In another situation, a nation or a terrorist organization could unleash a massively destructive cyberattack—targeting several electricity utilities, water treatment facilities or industrial plants at once, or in combination with each other to compound the damage.

Perhaps the most concerning possibility, though, is that it might happen by mistake. On several occasions, human and mechanical errors very nearly destroyed the world during the Cold War; something analogous could happen in the software and hardware of the digital realm.

Defending against disaster

Just as there is no way to completely protect against a nuclear attack, there are only ways to make devastating cyberattacks less likely.

The first is that governments, businesses and regular people need to secure their systems to prevent outside intruders from finding their way in, and then exploiting their connections and access to dive deeper.

Critical systems, like those at public utilities, transportation companies and firms that use hazardous chemicals, need to be much more secure. One analysis found that only about one-fifth of companies that use computers to control industrial machinery in the U.S. even monitor their equipment to detect potential attacks—and that in 40% of the attacks they did catch, the intruder had been accessing the system for more than a year. Another survey found that nearly three-quarters of energy companies had experienced some sort of network intrusion in the previous year.

But all those systems can't be protected without skilled cybersecurity staffs to handle the work. At present, nearly a quarter of all cybersecurity jobs in the U.S. are vacant, with more positions opening up than there are people to fill them. One recruiter has expressed concern that even some of the jobs that are filled are held by people who aren't qualified to do them. The solution is more training and education, to teach people the skills they need to do cybersecurity work, and to keep existing workers up to date on the latest threats and defense strategies.

If the world is to hold off major cyberattacks—including some with the potential to be as damaging as a nuclear strike—it will be up to each person, each company, each government agency to work on its own and together to secure the vital systems on which people's lives depend.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: A cyberattack could wreak destruction comparable to a nuclear weapon (2019, August 19) retrieved 25 April 2024 from https://techxplore.com/news/2019-08-cyberattack-wreak-destruction-nuclear-weapon.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.