Transcript: Stuxnet

Stuxnet is a new type of weapon, a digital worm. And it was used in the first cyberattack known to have caused physical damage in the real world.

While they have not admitted to it, the United States and Israel allegedly created Stuxnet in order to slow Iran's effort to build nuclear weapons.

The worm targeted the computers that ran the machines used to turn uranium into nuclear fuel. The Stuxnet worm spun many of the centrifuges out of control, blowing them up—all without the Iranians figuring out what was causing the explosions.

Eventually, though, Stuxnet got loose and spread across the world, infecting computers in more than 100 countries. The worm was quickly noticed—and the operation publicly exposed.

Cyber experts were alarmed by Stuxnet and feared its potential for destruction. While this worm only attacked specific equipment related to Iran's centrifuges, experts feared that the same digital technology could be used to manipulate the computers that run a huge swath of industrial activity and infrastructure projects like factories, dams, and electrical grids. Disrupting or destroying any of them could cause enormous physical damage and could potentially kill large numbers of people.

This has led some to suggest that cyberweapons have the potential to be weapons of mass destruction. And just as international treaties were created to control nuclear weapons, many countries and individuals are calling for treaties to control the use of cyberweapons. But that is unlikely to happen anytime soon because cyberweapons pose unique challenges.

They're often designed to be covert, so victims may not even realize that they were hit by a cyberattack. For example, while the Stuxnet worm was destroying the centrifuges, it sent false information to the Iranian scientists' equipment, pretending that everything was operating normally.

Even if victims do discover that they were attacked, they may not be able to determine who attacked them because hackers can mask their identities and cover their digital tracks. This makes it harder to enforce potential cyberweapon rules because countries may not know whom to attribute a violation to and as a result may not know who to punish.

On top of these challenges, there's no international consensus on what the cyber rules would even be. And so, without any rules, countries are

building up their cyber defenses, making it harder for cyberattacks to succeed.

But there's no perfect defense against a cyberattack. For example, the Iranian nuclear facility was underground and air-gapped, completely cut off from the internet. So those who wanted to damage the Iranian program couldn't sneak Stuxnet into the facility online. Nevertheless, they targeted the hardware suppliers for the facility and put it on their electronic equipment, which eventually made its way into the nuclear facility. This infiltration tactic makes it near impossible to completely protect any system from cyberattacks.

With globalized supply chains, every country is vulnerable to foreign cyberweapons. So many focus on building resiliency, making sure that important systems and infrastructure can quickly recover after a cyberattack.

And countries are also racing to develop stronger cyberweapons hoping to deter other countries from attacking out of fear of retaliation. They are also seen as a new tool to respond to extreme security threats like terrorist attacks or even to counterattack sanctions. More countries than ever are armed with cyb er weapons.

And every country—rich, poor, big, and small—is vulnerable.