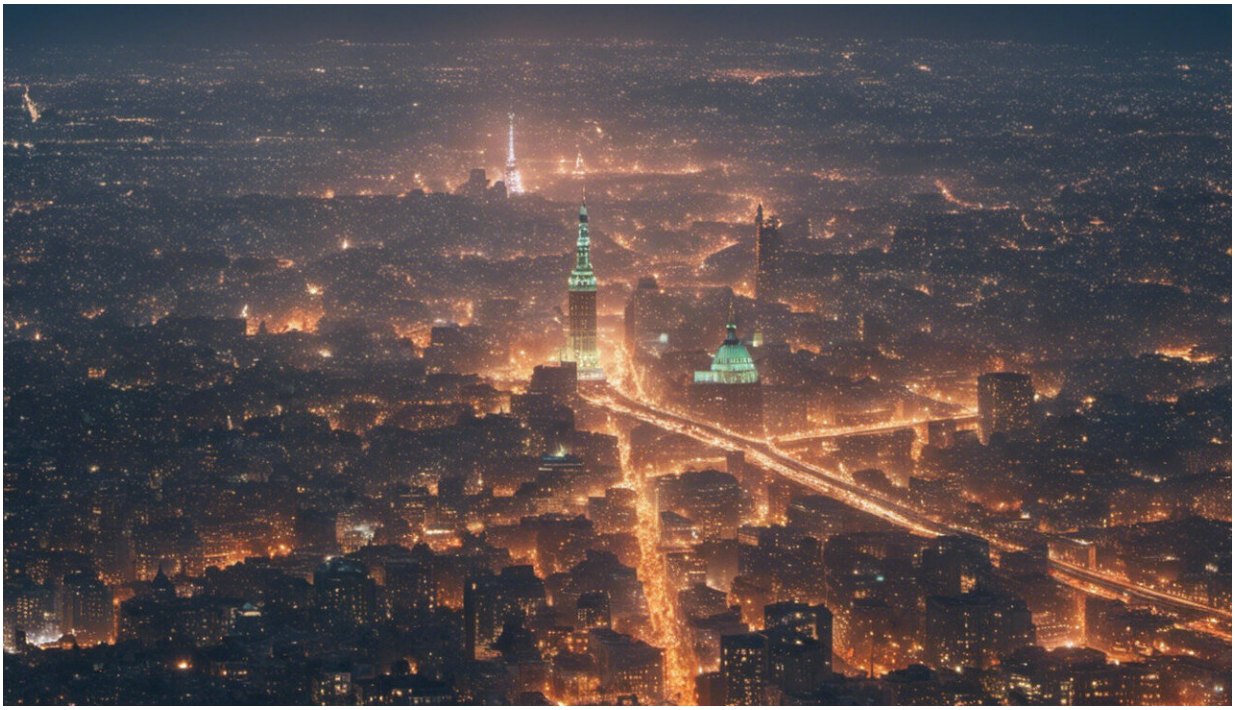
The next Cold War has already begun – in cyberspace

April 7 2016, by Conor Deane-Mckenna, University Of Birmingham



Credit: AI-generated image (disclaimer)

The world is fighting a hidden war thanks to a massive shift in the technologies countries can use to attack each other. Much like the Cold War, the conflict is being fought indirectly rather than through open declarations of hostility. It has so far been fought without casualties but has the potential to cause suffering similar to that of any bomb blast. It is

the Cyber War.

When we think of cyber attacks, we often think of terrorists or criminals hacking their way into our bank accounts or damaging government websites. But they have now been joined by agents of different governments that are launching cyber attacks against one another.

They aren't officially at war, but the tension between the US and Russia – and to a lesser degree China – remains high over a number of disputed decisions. Cyber attacks allow these countries to exert their power against each other in an often anonymous way. They can secretly make small gains but a wrong move could spell disaster, much like the operations of nuclear submarines during the Cold War.

There are numerous forms of cyber attacks that can be used. Malware, typically in the form of a Trojan horse or a worm, installs itself on a computer and takes control, often without the knowledge of the victim. Other attacks can disrupt computer systems through brute force. For example, distributed denial of service (DDOS) attacks involve flooding a system with so many requests to access a website that it crashes the site's server.

Countries are also trying to build up their cyber defences. Many infrastructural systems connected to power plants, for example, have been physically disconnected or "air-gapped" from the internet. Other defences such as firewalls and security programs are in place in all government systems to prevent their hacking by outside sources.

Just as dangerous as "real war"

Some argue that the idea of cyber warfare has been overhyped because cyber attacks don't have the physical consequences that "real" wars do. But the cyber weapons being used and developed could cause a large

degree of economic as well as infrastructural damage – and this could endanger property and even human life. In 2007, scientists at the Idaho National Laboratory in the US were able to show how a cyber attack on an electricity generator could cause an explosion. This shows the real danger that cyber attacks can pose, not simply to national security infrastructure but also to hospitals, schools and homes.

The year 2007 was actually crucial in the history of cyber warfare, marking the point when several major states began putting cyber weapons to use in a well-documented way. After Estonia attempted to relocate a Soviet war memorial, Russia was accused of launching a series of DDOS attacks on Estonian websites including government and banking sites. Such action was not just embarrassing but damaging to both the power of the Estonian state and the economic activity of the country.

Although it wasn't discovered until 2010, the Stuxnet worm was the first prominent cyber weapon to be used by the US, and was originally deployed against Iran in 2007. The worm, part of the wider "Operation Olympic Games", was designed to prevent Iran from producing uranium that could be used in nuclear weapons. The software was hidden on a USB stick and uploaded to the control systems of the enrichment plant, causing its centrifuges to operate outside of safe parameters and leading to a series of breakdowns.

The Israeli cyber section, Unit 8200, which had a hand in the Stuxnet design, was also involved in the blackout of air radar during an attack on nuclear facilities in Syria in Operation Orchard, 2007. Shutting down the ageing Soviet-era radar through a mixture of cyber attacks allowed Israeli jets to bomb the site in the Deir-ez-Zor region of Syria.

The Israeli example shows how cyber attacks will start to become part of standard military operations. Both the US and Chinese cyber warfare

divisions are parts of the countries' conventional military structures. And both states have made it clear that they will not rule out using cyber attacks for the sake of maintaining national security interests.

Acting with impunity

These capabilities pose a danger to everyone, not just governments, and not just because they could lead to infrastructure being blown up. Stuxnet was discovered because the worm found its way onto the global internet and caused problems for tens of thousands of PCs across the world. It's not hard to imagine the widespread economic and personal damage that could be done with an even more malicious program. Stuxnet also shows why simply keeping critical infrastructure disconnected from the internet is not enough to protect it.

The other particularly worrying aspect of cyber warfare is that it allows states to act with relative impunity. Advanced encryption technologies make it almost impossible to prove exactly who is responsible for a specific cyber attack. As a result, states can now act unilaterally with little fear of open retaliation. For example, despite a bilateral agreement between the US and China to refrain from hacking for economic benefit, Chinese hackers have continued to infiltrate secure systems in the United States. There are few real consequences for this outright breach of sovereignty.

On the positive side, some have argued that cyber attacks allow states to pursue their foreign policy goals without using conventional military action, and could even dissuade superpowers from doing so. Disabling Iran's nuclear programme, for example, reduced the short-term likelihood the US would feel the need to make a military attack on the country. With tensions between superpowers high, but the risk of full-scale world war still relatively low, cyber attacks are likely to become an increasingly common way for countries to gain at their competitors'

expense.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation