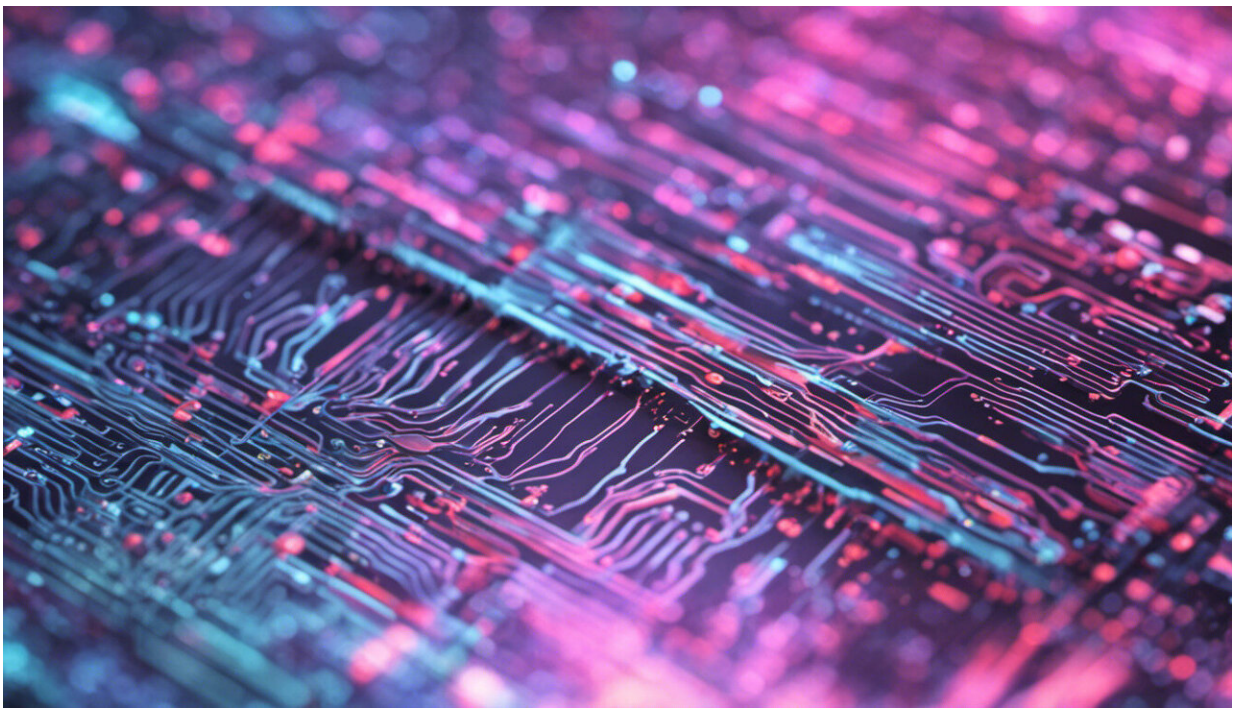
Cyber attacks are rewriting the 'rules' of modern warfare—and we aren't prepared for the consequences

May 17 2019, by Vasileios Karagiannopoulos And Mark Leiser



Credit: AI-generated image (disclaimer)

Governments are becoming ever more reliant on digital technology, making them more vulnerable to cyber attacks. In 2007, Estonia was attacked by pro-Russian hackers who crippled government servers, causing havoc. Cyber attacks in Ukraine targeted the country's electricity

grid, while Iran's nuclear power plants were infected by malware that could have led to a nuclear meltdown.

In the US, president Trump recently declared a "national emergency" to recognise the threat to US computer networks from "foreign adversaries".

Politically-motivated cyber attacks are becoming increasingly commonplace but unlike traditional warfare between two or more states, cyberwarfare can be launched by groups of individuals. On occasion, the state is actually caught in the crosshairs of competing hacking groups.

This doesn't mean that states don't actively prepare for such attacks. British defence officials have said they're prepared to conduct cyber attacks against Moscow's power grid, should Russia decide to launch an offensive.

In most cases, cyberwarfare operations have been conducted in the background, designed as scare tactics or displays of power. But the blending of traditional warfare and cyberwarfare seems inevitable and a recent incident added a new dimension.

How to respond to cyber attacks

Israeli Defence Forces bombed a building allegedly housing Hamas hackers, after they had attempted to, according to the IDF, attack "Israeli targets" online. This is the first time a cyber attack has been met with physical force by a state's military. But who is to blame and how should states respond when defending against cyber attacks?

Cyber attacks are a serious challenge for established laws of armed conflict. Determining the origin of an attack isn't impossible, but the process can take weeks. Even when the origin can be confirmed, it may

be difficult to establish that a state was responsible. This is especially true when cyber operations could be perpetrated by hackers in other countries routing their attacks through different jurisdictions.

NATO experts have highlighted the issue in the Tallinn Manual on International Law Applicable to Cyberwarfare. There is no consensus on whether a state is responsible for a cyber attack originating from its networks if it did not have explicit knowledge of the attack. Failure to take appropriate measures to prevent an attack by a host state could mean that the victim state is entitled to respond through proportionate use of force in self defence. But if there's uncertainty around who is to blame for the attack, any justification for a counter-attack is diminished.

Even if the problem of attribution is resolved, a state's right to respond with force to a cyber attack would normally be prohibited. Article 2(4) of the UN Charter protects the territorial integrity and political structures of states from attack. This can be lawfully bypassed if a state can claim they're defending themselves against an "armed attack".

The International Court of Justice explains that: "It will be necessary to distinguish between the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."

So a cyber-attack would justify force as self-defence if it could be considered an "armed attack". But is that possible? Only when the "scale" and "effect" of a cyber-attack are comparable to an offline "armed attack", such as attacks that lead to deaths and widespread damage to infrastructure. If so, self-defence is justified.

But what about when a cyber attack has been successfully defended against? Then, its effects can only be guessed at. This makes deciding a proportional response even trickier. Physical force used as self-defence after the cyber attack has already been successfully defended against

could be considered unnecessary and therefore, illegal. An exception, however, might be made for a preemptive defence against an imminent or possible attack.

When self-defence is considered reasonably necessary, the nature of the force permitted can vary. Proportionate counter-attacks with conventional military weapons can be acceptable responses to cyber operations under international law.

These issues are only the start of the challenges posed by cyberwarfare, which will get more complicated as technology develops. The intellectual challenges this will generate are numerous, but we still can't help but be fearful.

Societies face potentially devastating consequences from cyberwarfare as we become more reliant on information technologies and communication networks for everyday life – and we're only just starting to ask questions about it.

Provided by The Conversation