Calling out China for cyberattacks is risky—but a lawless digital world is even riskier

20 July 2021, by Alexander Gillespie

Credit: www.shutterstock.com

Today's multi-country condemnation of cyber-attacks by Chinese state-sponsored agencies was a sign of increasing frustration at recent behavior. But it also masks the real problem—international law isn't strong or coherent enough to deal with this growing threat.

The coordinated announcement by several countries, including the US, UK, Australia and New Zealand, echoes the most recent threat assessment from the US intelligence community: cyber threats from nation states and their surrogates will remain acute for the foreseeable future.

Joining the chorus against China may be diplomatically risky for New Zealand and others, and China has already described the claims as "groundless and irresponsible". But there is no doubt the problem is real.

The latest report from New Zealand's Government Communications Security Bureau (GCSB) recorded 353 cyber security incidents in the 12 months to the middle of 2020, compared with 339 incidents in the previous year.

Given the focus is on potentially high-impact events targeting organizations of national significance, this is likely only a small proportion of the total. But the GCSB estimated state-sponsored attacks accounted for up to 30% of incidents recorded in 2019-20.

Since that report, more serious incidents have occurred, including attacks on the stock-exchange and Waikato hospital. The attacks are becoming more sophisticated and inflicting greater damage.

Globally, there are warnings that a major cyberattack could be as deadly as a weapon of mass destruction. The need to de-escalate is urgent.

> The government says it has uncovered evidence of Chinese state-sponsored cyber attacks in New Zealand.https://t.co/wB5Q8M4lwO
>
> — RNZ (@radionz) July 19, 2021

Global solutions missing

New Zealand would be relatively well-prepared to cope with domestic incidents using criminal, privacy and even harmful digital communications laws. But most cybercrime originates overseas, and global solutions don't really exist.

In theory, the attacks can be divided into two types—those by criminals and those by foreign governments. In reality, the line between the two is blurred.

Dealing with foreign criminals is slightly easier than

combating attacks by other governments, and Prime Minister Jacinda Ardern has recognized the need for a global effort to fight this kind of cybercrime.

To that end, the government recently announced New Zealand was joining the Council of Europe's Convention on Cybercrime, a global regime signed by 66 countries based on shared basic legal standards, mutual assistance and extradition rules.

Unfortunately, some of the countries most often suspected of allowing international cybercrime to be committed from within their borders have not signed, meaning they are not bound by its obligations.

That includes Russia, China and North Korea. Along with several other countries not known for their tolerance of an open, free and secure internet, they are trying to create an alternative international cybercrime regime, now entering a drafting process through the United Nations.

> 'Groundless, irresponsible': China fires back at NZ after cyber attack accusation https://t.co/oGSOMtFdXT
>
> — Newshub Politics (@NewshubPolitics) July 19, 2021

Cyberattacks as acts of war

Dealing with attacks by other governments (as opposed to criminals) is even harder.

Only broad principles exist, including that countries refrain from the threat or use of force against the territorial integrity or political independence of any state, and that they should behave in a friendly way towards one another. If one is attacked, it has an inherent right of self-defense.

Malicious state-sponsored cyber activity involving espionage, ransoms or breaches of privacy might qualify as unfriendly and in bad faith, but they are not acts of war.

However, cyberattacks directed by other governments could amount to acts of war if they cause death, serious injury or significant damage to the targeted state. Cyberattacks that meddle in foreign elections may, depending on their impact, dangerously undermine peace.

And yet, despite these extreme risks, there is no international convention governing state-based cyberattacks in the ways the Geneva Conventions cover the rules of warfare or arms control conventions limit weapons of mass destruction.

Risks of retaliation

The latest condemnation of Chinese-linked cyberattacks notwithstanding, the problem is not going away.

At their recent meeting in Geneva, US President Joe Biden told his Russian counterpart, Vladimir Putin, the US would retaliate against any attacks on its critical infrastructure. A new US agency aimed at countering ransomware attacks would respond in "unseen and seen ways", according to the administration.

Such responses would be legal under international law if there were no alternative means of resolution or reparation, and could be argued to be necessary and proportionate.

Also, the response can be unilateral or collective, meaning the US might call on its friends and allies to help. New Zealand has said it is open to the proposition that victim states can, in limited circumstances, request assistance from other states to apply proportionate countermeasures against someone acting in breach of international law.

A drift towards lawlessness

But only a month after Biden drew his red line with Putin, another massive ransomware attack crippled hundreds of service providers across 17 countries, including New Zealand schools and kindergartens.

The Russian-affiliated ransomware group REvil that was probably behind the attacks mysteriously

disappeared from the internet a few weeks later.

Things are moving fast and none of it is very reassuring. In an interconnected world facing a growing threat from cyberattacks, we appear to be drifting away from order, stability and safety and towards the darkness of increasing lawlessness.

The coordinated condemnation of China by New Zealand and others has considerably upped the ante. All parties should now be seeking a rules-based international solution or the risk will only grow.

Provided by The Conversation
APA citation: Calling out China for cyberattacks is risky—but a lawless digital world is even riskier (2021, July 20) retrieved 3 December 2021 from https://techxplore.com/news/2021-07-china-cyberattacks-riskybut-lawless-digital.html