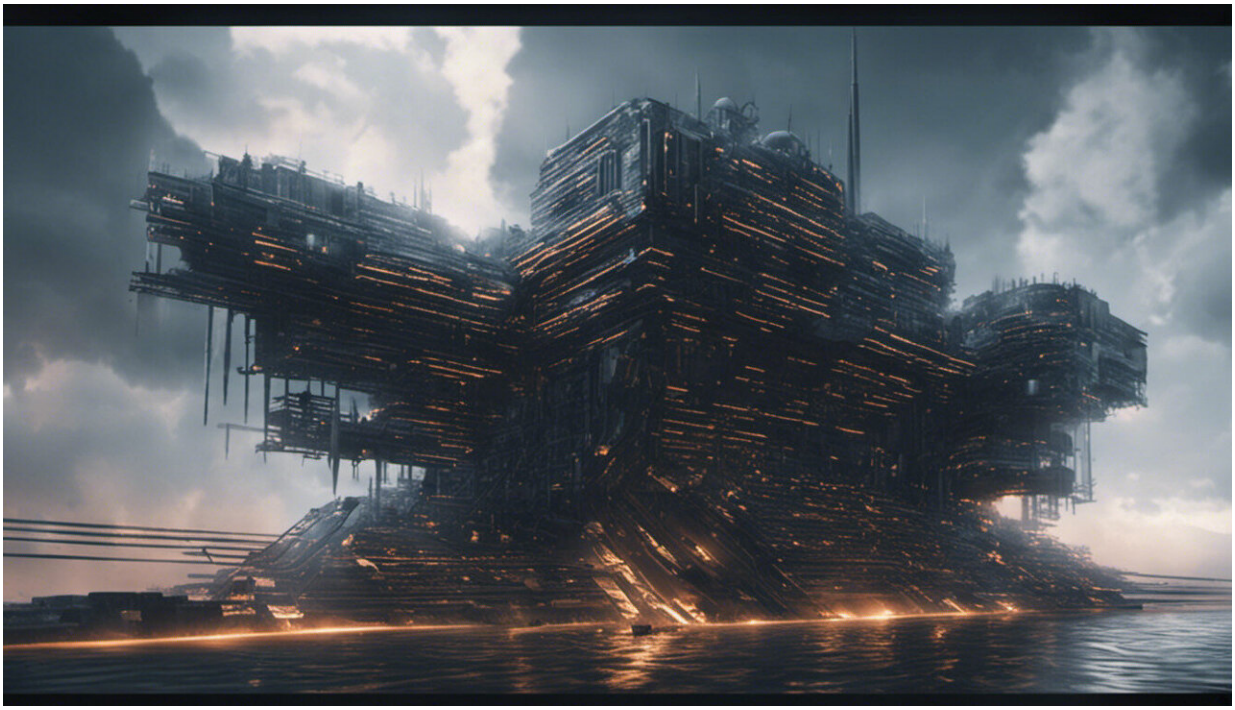
The public has a vital role to play in preventing future cyber attacks

April 17 2018, by Sandeep Gopalan



Credit: AI-generated image (disclaimer)

Up to 400 Australian organisations may have been snared in a massive hacking incident detailed today. The attack, allegedly engineered by the Russian government, targeted millions of government and private sector machines globally via devices such as routers, switches, and firewalls.

This follows a cyber attack orchestrated by Iranian hackers revealed last month, which targeted Australian universities.

A joint warning by the US and UK governments stated that the purpose of the most recent attack was to: "… support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations."

The Russians' modus operandi was to target end-of-life devices and those without encryption or authentication, thereby compromising routers and network infrastructure. In doing so, they secured legitimate credentials from individuals and organisations with weak password protections in order to take control of the infrastructure.

Cyber attacks are key to modern conflict

This is not the first instance of Russian aggression.

The US city of Atlanta last month was crippled by a cyber attack and many of its systems are yet to recover – including the court system. In that case, attackers used the SamSam ransomware, which also uses network infrastructure to infiltrate IT systems, and demanded a ransom payment in Bitcoin.

Baltimore was hit by a cyber attack on March 28 that disrupted its emergency 911 calling system. Russian hackers are suspected to have taken down the French TV station TV5Monde in 2015. The US Department of State was hacked in 2015 – and Ukraine's power grid and military infrastructure were also compromised in separate attacks in 2015 and 2017.

But Russia is not alone in committing these attacks.

In December 2017, North Korean hackers were blamed for the WannaCry attack that infected over 300,000 computers in 150 countries, affecting hospitals and banks. The UK's National Health Service was particularly bruised and patients had to be turned away from surgical procedures and appointments.

Iran has conducted cyber attacks against numerous targets in the US, Israel, UAE, and other countries. In turn, Iran was subjected to a cyber attack on April 7 that saw computer screens display the US flag with the warning "don't mess with our elections".

Prosecuting hackers is ineffective

The US government has launched prosecutions against hackers – most recently against nine Iranians for the cyber attacks on universities. However, prosecutions are of limited efficacy when hackers are beyond the reach of US law enforcement and unlikely to be surrendered by their home countries.

As I have written previously, countries such as Australia and the US cannot watch passively as rogue states conduct cyber attacks against targets within our jurisdiction.

Read more: Is counter-attack justified against a state-sponsored cyber attack? It's a legal grey area

Strong countermeasures must be taken in self defence against the perpetrators wherever they are located. If necessary, self defence must be preemptive – any potential perpetrators must be crippled before they are able to launch strikes on organisations here.

Reactive measures are a weak deterrent, and our response should include a first strike cyber attack option where there is credible intelligence

about imminent attacks. Notably, the UK has threatened to use conventional military strikes against cyber attacks. This may be an overreaction at this time.

Educating the public is essential

Numerous cyber attacks in recent years – including the current attack – have targeted common household devices, such as routers. As a result, the security of public infrastructure relies to some extent on the security practices of everyday Australians.

So, what role should the government play in ensuring Australians are securing their devices?

Unfortunately, cybersecurity isn't as simple as administering an annual flu shot. It's not feasible for the government to issue cybersecurity software to residents since security patches are likely to be out-of-date before the next attack.

But the government should play a role in educating the public about cyber attacks and securing public internet services.

The city of New York has provided a free app to all residents called NYC Secure that is aimed at educating people. It is also adding another layer of security to its free wifi services to protect users from downloading malicious software or accessing phishing websites. And the city of Jonesboro, Georgia is putting up a firewall to secure its services.

Australian city administrations must adopt similar strategies alongside a sustained public education effort. A vigilant public is a necessary component in our collective security strategy against cyber attacks.

This cannot be achieved without significant investment. In addition to

education campaigns, private organisations – banks, universities, online sellers, large employers – must be leveraged into ensuring their constituents do not enable attacks through end-of-life devices, unsupported software, poor password protection policies and lack of encryption.

Governments must also prioritise investment in their own IT and human resources infrastructure. Public sector IT talent has always lagged the private sector due to pay imbalances, and other structural reasons.

It is difficult for governments to attain parity of technical capabilities with Russian or North Korean hackers in the short term. The only solution is a strong partnership – in research, detection tools, and counter-response strategies – with the private sector.

The Atlanta attack illustrates the perils of inaction – an audit report shows the city was warned months in advance but did nothing. Australian cities must not make the same mistake.

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

Provided by The Conversation