As surveillance gets smart, hackers get smarter

July 28 2016, by Monique Mann And Michael Wilson

Credit: AI-generated image (disclaimer)

There is an escalating technological arms race underway between governments and hacktivists. As governments step up their surveillance, the hacktivists find new ways to subvert it.

This cat and mouse game has been described as a crypto war and it's

been going on for decades.

Top secret documents released by Edward Snowden confirmed the extent of global internet surveillance by government agencies. For example, the United States National Security Agency (NSA) obtained access to systems maintained by tech companies and intercepted undersea cables to monitor global internet traffic.

New laws, new powers

The motivation behind the expansion of surveillance powers is to use intelligence gathering to improve security. We see this in recent Australian legislative developments.

Australian laws allow the Australian Security Intelligence Organisation (ASIO) to infiltrate computer networks. Other new laws require internet service providers (ISPs) to retain metadata for two years.

A range of government agencies enjoy access without warrant, including many unrelated to criminal justice or national security.

But past experience shows how online surveillance can provoke hacktivists to develop and disseminate technologies that enhance privacy.

The Cypherpunk movement arose in direct opposition to state surveillance. They promoted privacy online and released cryptographic code to thwart prying eyes.

Contemporary advocates for surveillance self-defence include the Electronic Frontier Foundation and Australian Greens Senator Scott Ludlam.

Public figures like Snowden continue to raise awareness and provide advice on how to evade surveillance. Use of TOR, a network that allows people to browse the internet anonymously, increased dramatically following Snowden's revelations about NSA snooping.

The US Director of National Intelligence said Snowden's disclosures accelerated the uptake of encryption by seven years. Just last week it was reported that Snowden is developing a new tool to show when mobile phone communications are being monitored.

What all this means is that technologies that enhance privacy are now readily available and widely used. There has already been a marked increase in encrypted internet traffic.

Even Australian Prime Minister Malcolm Turnbull admitted he used Wickr to encrypt communications.

Hacktivists have also launched cyber-attacks in protest to government activities and surveillance. Distributed denial-of-service attacks have been targeted at both government and corporate websites in response to email surveillance and extradition and the banking blocks against WikiLeaks.

Encryption facilitates crime online

Although arising from benevolent motives, these same tools can be used for more sinister purposes. Illicit marketplaces abound in the dark web. Anyone can anonymously buy drugs, firearms, stolen identification or distribute child pornography online.

Hackers are now using encryption to defeat firewalls and overcome anti-virus protection. This has resulted in an upsurge in malware attacks around the world.

The ability to conceal identities, communications and locations poses more challenges for law enforcement and security agencies. It makes identifying offenders and accessing evidence even harder.

This means additional resources and new technical skills are needed. Earlier this year the Australian Government announced A$230 million in funding to implement the Cyber Security Strategy. This outlines plans for increased intelligence and offensive cyber capabilities.

And so the arms race in the crypto-war continues.

Security through surveillance?

Despite all this, questions remain about the success of blanket surveillance programs. There is currently no evidence to indicate this actually increases security.

We know surveillance can be effective under narrow conditions, but only for specific crimes. Collecting too much information can also be a barrier to effective intelligence systems.

Recent terrorist attacks in Paris reveal how data retention programs that attempt to identify every possible threat are not failsafe. Security agencies become overwhelmed with data. Collecting as much information as possible about as many people as possible may be positively harmful.

Significant resources are being spent on strategies with questionable efficacy. These strategies impact privacy, provoke opposition and create new challenges to overcome.

The privacy-security paradox

Governments are seeking to detect threats through surveillance. But hacktivists are responding to a perceived injustice. Namely, the invasion of the privacy of all internet users.

Successive governments have argued for the need to balance security and privacy. But there are both political and practical problems with this approach.

Leading academics argue security interests will always outweigh individual rights. But encroaching on the privacy of all internet users just antagonises hacktivists and inspires further development and use of tools to enhance privacy.

The security versus privacy trade-off becomes a self-defeating paradox.

So we need to rethink this balancing act in a way that respects the rights of internet users. The public needs to have confidence that their privacy is respected and that governments are collecting and using information appropriately.

Certainly governments have a responsibility for countering threats like terrorism. But it is important to realise that mass indiscriminate surveillance, and the development of technologies to circumvent it, are evolving together.

Governments may think they are smart in surveillance, but those evading it are even smarter.

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

Source: The Conversation