# Get ready for a bumpy ride: Cybersecurity trends in 2020

January 7 2020, by Luisa Low



Credit: CC0 Public Domain

What will 2020 have in store for cybersecurity? Tighter regulation, increasingly sophisticated attacks on key infrastructure and AI-driven cyber warfare, according to Dr. Suranga Seneviratne from the School of

Computer Science.

## Internet of (Insecure) Things

"Internet-of-Things technology is becoming increasingly popular, with [smart home devices](link) on the rise in Australia," said cybersecurity expert from the University of Sydney's School of Computer Science, Dr. Suranga Seneviratne.

"Domestically, the household Internet of Things market reached $1.1 billion in 2018, which was a 57 percent increase compared to the previous year.

"We can't deny IoT's ubiquity, but are all these devices really secure? Are we opening up our houses to attackers to build botnets (ie: secretly using our smart home devices to attack other internet hosts), steal our data, or worse, control our houses?

"Perhaps it's time we looked at enforcing stricter regulations to make these devices more secure, which is already happening in the UK and US. The draft Australian [Voluntary Code of Practice: Securing the Internet of Things for Consumers](link) is definitely a step in the right direction."

## Tech giants under scrutiny: what to expect

"Under the European Union's General Data Protection Regulation (GDPR) framework we saw some big tech companies being held accountable for collecting personal data without proper consent," said Dr. Seneviratne.

"The [Cambridge Analytica](link) incident also generated a much-needed and

overdue discourse on how to collect and handle personal data.

"In California, where the majority of US tech-companies are based, the CCPA (California Consumer Privacy Act) will come into effect from January 2020.

"Yet, globally, we still don't have a proper framework on how to balance the trade-offs between privacy and consumer utility, particularly with data that's stored remotely. Will storing data on devices finally become trendy?"

## Cyberthreats on critical infrastructure—are we ready?

"This year we witnessed several global attack attempts on critical infrastructure, such as electrical grids and government services. These attacks are likely to become more frequent, more sophisticated and increasingly politically motivated," said Dr. Seneviratne.

"While it is important for governments and businesses to take all possible measures to detect and prevent these attacks, they must begin preparing for worst-case scenarios. In 2015 Ukraine bore the first ever attack of this kind. Attackers were able to disrupt the power supply of more than 200,000 people for a few hours.

"Do governments and large service providers have proper incident response protocols in place to prevent such attacks? Are employees well trained to handle such threats? In some cases, the way we react to an attack could make things far worse."

## AI-driven security and privacy threats

"Artificial intelligence is becoming pervasive: already we've witnessed demonstrations that have used AI to bypass [CAPTCHA](link) and facial-recognition software. For example, on one occasion, researchers showed how specially printed patterns on spectacle frames could trick state-of-the-art commercial facial recognition systems to think the wearer was someone else," said Dr. Seneviratne.

"It can be expected that these attacks will soon go beyond prototypes and into the real world, with hackers using AI to circumvent traditional antivirus solutions, such as malware detection systems and intrusion detection systems."

Provided by University of Sydney