Cyber terrorism: fact or fiction?

By **ROBERT CHEW**
Council Member, SID

INNOVATION

An article in the June 2016 edition of New York Magazine described the scenario of how a massive, multi-pronged online attack on New York City could take place:

On December 4, 2017, at a little before nine in the morning, … a hired SUV suddenly swerved to the left, … pinning a sedan against a concrete median. A taxi ran into the SUV's rear fender and spun into the next lane, forcing a school-bus driver to slam on his brakes. Within minutes, nothing was moving … Moments later, on the George Washington Bridge, an SUV veered in front of an 18-wheeler, causing it to jackknife across all four lanes and block traffic heading into the city.

The crashes were not a coincidence. Within minutes, there were pileups … At the center of each accident was an SUV of the same make and model, but as the calls came in to the city's 911 centers in the Bronx and Brooklyn, the operators simply chalked them up to Monday-morning road rage. No one had yet realized that New York City had just been hit by a cyber attack.

A third-year resident in the emergency room at Columbia University Medical Center … walked through the hospital as a television was airing images from the accident on the George Washington Bridge; that meant several crash victims would soon be heading her way. When she got to her computer, she tried logging into the network to check on the patients who were already there, but she was greeted with an error message that read WE'RE NOT LOOKING FOR BITCOINS THIS TIME.

No longer the stuff of novels

What reads like a techno-thriller novel was meant to be a thought-provoking exercise, except the unnerving thing about it is that most, if not all, of what the article envisioned have already happened.

In July 2015, two researchers Chris Valasek and Charlie Miller demonstrated that they could launch attacks against the software systems that powered a 2014 Jeep Cherokee. They bombarded the passenger cabin with loud music, blurred the windshield with wiper fluid and, worryingly, forced the car to decelerate while on the Interstate Highway.

In March 2016, KrebsonSecurity.com, a site on internet security matters written by former *Washington Post* staffer Brian Krebs, reported that Kentucky's Methodist Hospital was on lockdown after an outbreak of the Locky ransomware encrypted data on a number of systems at the facility. At the same time, the BBC reported that two other Californian hospitals – Chino Valley Medical Center and Desert Valley Hospital – had also experienced ransomware attacks.

The *New York Magazine* article invoked high drama of a coordinated multi-vector attack on New York City to illustrate a point. As we move more and more things online, thinking we are moving into the future, we might one day be rudely awakenened by the very real possibility of a war zone instead.

Granted, we may not be in that war zone yet but we are certainly entering a new era of cyber security. With every bit of information getting digitalised, everything going the way of IoT (Internet of Things), vehicles becoming driver-less and autonomous, and medical devices getting implanted in our bodies, we create irresistible targets for those who want to spy and steal, disrupt and destruct, and a wide spectrum of illegal activities. Cyber threats are no longer just annoying but alarming, rendering both the information and physical world unsafe.

Fighting the invisible enemies

As Singapore steps up efforts to become a Smart Nation, the need to address the challenges of cyber security becomes ever greater. Foremost among these challenges is sourcing, developing and training information security professionals with the combination of business and technical savvy needed to combat the growing cyber threats. Unfortunately, this profession has evolved largely in reaction to threats and so, we are missing an entire generation.

We are not alone in this. In November 2015, the *Financial Times* reported that the global demand for cyber security experts is forecast to outstrip supply by a third before the end of the decade, with companies struggling against what one senior industry figure has called the "largest human capital shortage in the world".

In addition, traditional security methods are not keeping up with cyber attackers. As a result, researchers are now developing systems to automate the response – systems that tap Artificial Intelligence (AI) to create radically different and potentially far more sophisticated defence models. These techniques revolve around technologies such as big data, pattern mapping and matching, cognitive computing, and deep learning methods that simulate the way the human mind works. The goal is to better identify suspicious patterns and behaviour, and build security frameworks that are more resilient and adaptable.

At the recent hacker conference, DEFCON 2016, the US Defense Advanced Research Projects Agency (DARPA) ran its Cyber Grand Challenge. Seven teams competed to build AI "bots" to find, diagnose and fix software flaws. These "bots" also have to defend themselves against other teams attacking the vulnerable code on their own servers while trying to launch counterattacks.

DARPA has repeatedly delivered game-changing capabilities using such competitions, including icons of modern society such as the Internet, automated voice recognition and language translation, and the Global Positioning System receivers small enough to embed in our mobile phones.

The outcome of DARPA Cyber Grand Challenge could radically change the way we deal with software vulnerabilities and cyber threats. We may see here yet another case of digital disruption that is a work in progress. ■