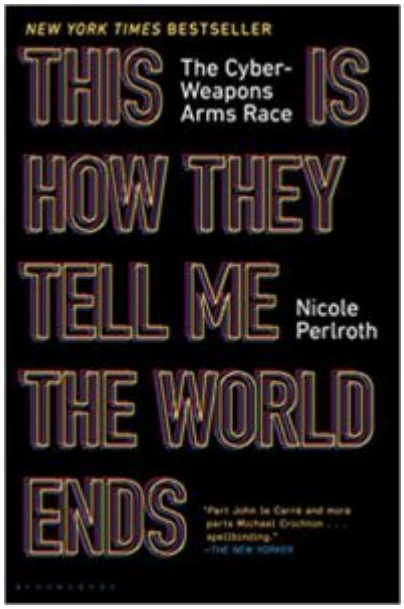
Book Review

Tim McQueen



***This is how they tell me the world ends* – the cyber weapons arms race**

Nicole Perlroth

Bloomsbury 491 pages

On 10 May 2021 The Age carried a story 'DarkSide, ransom group linked to Colonial Pipeline hack, new but not amateur'. This attack could, and should have been prevented. '*This is how they tell me the world ends* – the cyber weapons arms race' by Nicole Perlroth anticipated this and other aggression against American infrastructure. Perlroth is a staff writer for the New York Times covering cyber security and digital espionage. She previously covered Silicon Valley for Forbes.

She starts the story with Russia's cyber attack on the Ukraine in 2017 that shut down government services, railways, ATMs, the postal service and even the radiation monitors at Chernobyl. How did we come to that state?

Most Melb PC members will have at least some knowledge of zero day exploits and their use in hacking. What many may not know is that these may not be diligently reported to developers for patching, but collected by agencies for espionage and data collection or more nefarious activities. The early attitude of some developers was to attempt to sue hackers who discovered and reported bugs.

Nathaniel Borenstein, one of the inventors of the email attachment said: 'The most likely way for the world to be destroyed … is by accident. We're computer professionals. We cause accidents'.

After 9/11 American security services changed their emphasis. They acted against Huawei, suspecting backdoors for Chinese infiltration into American products. The National Security Administration (NSA) began to believe it was smarter than anyone else. In 2007, in apparent conjunction with Israel, Stuxnet (the Natanz worm) was developed. It worked well and apparently disrupted Iran's nuclear program. But it escaped and caused havoc in commercial installations throughout the world including the Cadbury factory in Hobart. (The worm, at 500 kb, was 100 times the size of the software used in the Apollo moon launch).

Michael Hayden, former NSA director said: ‘This has the whiff of August 1945 … Somebody just used a new weapon and [it] will not be put back in its box’.

Perlroth describes many exploits, the people who used them and some who tried to expose them. A problem is that exposing weaknesses can attract attention to them. Americans tried to work with ‘friendly’ nations; but some US allies (UAE, Saudi Arabia, Mexico) turned the tools against their own citizens.

Software security is only ever as good as its weakest link. And that weakest link is often the user who clicks on a phishing email.

Google set up in China, but soon found its tools being used against Chinese citizens and decided to abandon the attempt. (Later, the lure of the large market took it back.) In the meantime, China had hacked Google’s source code. Software developers had historically concentrated on the security of customer data rather than that of their own intellectual property. James Coney (FBI) stated: ‘there are two kinds of countries; those who’ve been hacked by the Chinese, and those who don’t know they’ve been hacked by the Chinese’.

In 2011 a whistleblower tipped off the Pentagon that its security software was riddled with Russian backdoors. The Pentagon had paid Computer Sciences Corporation $US613 million to secure its software. CSC subcontracted the job to a Massachusetts outfit which, in turn, farmed out the coding to programmers in Moscow. Why? Greed. The Russian contractors charged one third the price of their US peers.

In 2015, Apple resisted requests by the FBI to unencrypt an iPhone. (Apparently they eventually paid a hacker who found a way to access the information.)

Perlroth attended a hacker conference in Buenos Aires. Talking to a hacker she asked ‘will they only sell their exploits to good Western governments?’ The response was: ‘…who is good? Who is bad? The last country that bombed another country into oblivion was not China or Iran.’

The US (and Australia) are vulnerable. How secure is our IT infrastructure? How many systems are cobbled together with obsolete computers running outdated, unpatched software? How many default passwords have never been changed? How many staff can consistently recognise and avoid phishing attacks? How many staff have unsecured social media accounts (that may share passwords with office systems)?

In 2012, Russia proposed a cyberwar treaty; the US didn’t want one. President Trump refused to accept the concept of Russian interference in the 2016 election and scrapped the position of White House cybersecurity chief. Republican Senator Mitch McConnell (who has again been in the news recently because of his support for Trump’s rejection of the 2020 election results) prevented passage of an election security bill.

As long as we continue to design software with the aim of being first on the market, with no thought of security, using Open Source software that could be compromised, there is no solution in sight. There are moves to increase the security in chips (CHERI – Capabitiy Hardware Enhanced RISC instructions). But there is still the issue (and costs) of fixing all the old hardware and software. Read this book and weep.