

Why cyber security will be key issue in 2020s

Geopolitics and technological advances mean cyber deterrence is as important as the business cycle for financial, investment and economic decisions.

[Stirling Larkin](#) Columnist

Jan 15, 2020 — 12.00am

It was peculiar that so speedily after the drone [assassination of Iranian Qassem Soleimani](#) there were immediate warnings in the US, Europe, NATO members and allies, such as Australia and Canada, to expect Iranian cyber warfare counter-subterfuge.

Beyond cyber security being merely a commercial-industrial consideration, this was the first time on the international stage that it was recognised as an imminent likelihood.

Only weeks into this new era, already dubbed the “roaring 2020s”, geopolitics has conflated with technological advances and economic necessities to mean cyber deterrence is as important as the business cycle when considering financial, investment and economic decisions.

Top companies listed on the S&P 500 are speedily bolstering digital defences, stress-testing control systems (both internally across networks and ring-fencing access points), in the expectation of Iranian and proxy cyber strikes. The Islamic Revolutionary Guard cyber divisions have weaponry to leverage and deploy, which could cripple, “drop” and damage cloud and edge servers and even quantum “supercomputers” from the west coast of California all the way deep into Washington and Langley, Virginia.

Beyond the known drop attacks, malware and ransomware threads the Iranians, Russians, North Koreans and Chinese have levied over the past 15 years, it is thought the Iranians have lifted their game in pre-emptive and proactive attempts to circumvent industrial control systems across US, European and, by extension, Australian energy, transport and financial institutions.

Last year an Iranian group was thought to be responsible for compromising a Connecticut hydroelectric facility via denial-of-service (DoS) and zero-day belligerence, derailing the plant and opening the potential for real-world flooding, carnage and loss of life.

But beyond nuanced or isolated instances, Australian investment communities need an urgent wake-up call to this new epoch, especially with the hegemonic tussles between our two largest trading partners, the US and China.

As they vie for the coveted “quantum supremacy” – whereby one hegemonic power supersedes all others by mastering quantum computing and, by association, artificial intelligence and the likely future control of the human species – Australia and Australians are already cannon fodder for Sino-American commercial, financial and industrial tussles in this arena.

This clash suggests we are heading toward a more bipolar world, split between the US and its allies on one side and China and its allies on the other.

Such a shift will have serious consequences for global markets and decisive implications for investors, not to mention that [global growth](#) will likely slow in both scenarios.

Protectionism and deglobalisation have been key concerns for investors since Trump's election in November 2016. With [the near-certainty of Trump winning on November 3](#) this year and President Xi Jinping staying on near indefinitely, these concerns will only continue to mount and metastasise.

Another consequence for the global economy in this scenario is that supply chain shuffling will lead to less efficient use of economic resources – natural, capital or human – which will ultimately lead to upward price pressures, especially in the short run.

Lower productivity and therefore lower productive capacity are known sources of inflationary pressures.

The complex supply chains that power the global economy – and on which Australia as a mercantile powerhouse deeply relies – have been developed, refined and fine-tuned over decades and these may be compromised or destroyed within days of a successful cyber attack.

With all eyes on Iran, it should not be forgotten by Australians that it is China that has emerged as a major global contender in the field of AI, the apex technology of the information era. This has frustrated Australian mandarins at the World Trade Organisation (WTO) as China continued to demand developing economy status (affording it grants, subsidies and more leniencies), while bragging about its AI credentials and the likelihood of being the quantum and AI supremacist within the decade.

The commercialisation of "deep learning" has created a scarcity for AI talent as we see the tech giants opening research labs worldwide to attract talent. This should concern Australians who have both welcomed Chinese students and taken inadequate steps to protect home-grown IP, trade secrets and accrued acumen.

In the US, legislation passed this month to limit all exports of AI technologies, excluding to Canada, without both State and Commerce departments consent. This is an obvious step Canberra should follow.

While the "roaring 1920s" came to be known as a period of economic prosperity and later tumult, it is sanguine to foresee that the "roaring 2020s" will also welcome economic prosperity and will be enjoyed or challenged through cyber technologies.

[Stirling Larkin](#) writes on global investing and ultra high net worth wealth. He is chief investment officer of investment manager Australian Standfirst.

