Edith Cowan University

Cyber 2020 Conference Reception

Welcome remarks by the Honourable Kim Beazley AC
Governor of Western Australia

Wednesday, 29th January 2020

I would firstly like to acknowledge the traditional owners of the land on which we meet – the Whadjuk Noongar people – and pay my respects to their elders past and present.

Welcome everyone. It is great to have Australia's cyber security thought leaders here this evening. You help to form the vanguard of our national security. Integral to the very foundation of our prosperity.

Western Australia is pivotal in helping to foster our nation's cyber capability; primarily through Edith Cowan University, home to the headquarters of Australia's Cyber Security Cooperative Research Centre.

ECU cyber security research and education is world leading. It has the most advanced cyber security research and education function of any university in Australia; with particular expertise including digital forensics, human security, and critical infrastructure security. Interpol has just six academic members of its Cyber Crime Experts Group internationally. Two of these work at ECU.

I heard that today [January 29], ECU opened its own Security Operations Centre – we are proud to have this capability at a Western Australian university. This is unique to the region and a coup for Australia.

The State Government has also made the digital economy a priority. One focus is to create a safe and secure digital place to do business. The WA Office of the Government Chief Information Officer is leading a substantial procurement process that will transform the digital platform for 140 agencies for the benefit of all West Australians. ECU's capability is vital to this and assists with the project.

It is remarkable to think that Australia is home to two former hackers, self-titled 'Electron' and 'Phoenix', who created the world's first politically motivated computer worm [virus] in the 1980's. I am informed that they were once regarded by the community as the most skilled hackers in the world. Only brought to justice because authorities in the United States were able to close in on them by realising they were from Australia [Melbourne], by way of their usage of lyrics from a Midnight Oil song.

Times certainly have changed. Cyber security was once seen as a novelty, of interest to a select few. The exponential increase in computer based dependency worldwide has changed this. In fact, in the earliest days [1943], the President of IBM said: "I think there is a world market for maybe five computers". Now, on average, every Australian home has more than five computer-based devices connected to the Internet. With one in every three Australian adults affected by cybercrime.

The number of unfilled cyber security jobs has grown by more than 50 per cent since 2015. By 2022, the global cyber security workforce shortage has been projected to reach upwards of 1.8 million unfilled positions. Over the next decade we will need another 60,000 specialists.

We are in the fourth industrial age. Government, industry and individuals seek to exploit the cyber domain in order to realise technological advances. It is ever so tempting to let cyber dependency privilege technical application over essential security needs. But we must not. In this current age, good cyber security is as essential to our prosperity as access to clean drinking water is to our society.

The old saying that 'all is fair in love and war' is now antiquated. Perhaps it should instead read 'all is fair in love, war and cyber operations'. After all, we cannot trust that so called 'gentlemen's agreements' will be upheld among adversaries and competitors. This has been demonstrated time and time again, including via a failed, albeit honourable attempt by President Obama, for countries to consider military-focussed cyber operations fair game, but to keep commercial activity off limits.

The sad truth is that if one country actually did refrain from offensive cyber operations, their adversaries and competitors would gain critical strategic advantages over them. This would see them on an 'unlevel' playing field that could shatter their military and economic interests, perhaps even their very survival. For example, by compromising sensitive government deliberations, multi-billion dollar trade deals, or even possibly, in effect, switching off a nation's defence force.

Cyber operations take plausible deniability and accessibility to a whole other level. Many of these operations are conducted by individuals yet to have had their first kiss. People who do it for the thrill, with or without sanction from their governments. This is not simply 'hacktivism'. Various exposés appear to show governments effectively outsourcing cyber operations to their citizens ['netizens'], or at least turning the other cheek where their ideals align, creating cyber armies en masse.

Your cyber event is a critical event in our defence against cyber criminality and our national security. You are assessing, analysing the results of the call for submissions on our cyber strategy. You are honing down propositions on defending against emerging cyber threats and vulnerabilities and how best to build cyber skills. This is the new domain of warfare and in it warfare is constant. In the other domains it is possible and we prepare expensive platforms to fight it, all highly dependent now on effectiveness in the cyber domain. I cannot think of a more important forum likely to take place in this State while I am Governor. We are lucky to have had in Edith Cowan devoted academics determined to produce national effectiveness.

Let us progress the debate and never 'play victim' whenever our institutions or industry is hacked. Let us instead accept the reality of our current age, including that prosecution across borders in nigh-on impossible. We must be utterly prepared to prevent and repel cyber intrusions.

We might build consensus in reprimanding perpetrators for their malicious work, to help keep their activities in check. And consistent with views suggested by the former Director General of the Australian Signals Directorate in a recent, rare public commentary, let us also keep our offensive capabilities honed – to disrupt, degrade or deny these adversaries offshore wherever extenuating circumstances apply.

Thank you.