INTERNATIONAL CONFERENCE:

REALIGNING CYBER SECURITY EDUCATION

Abstracts accepted as of 11 September

Education for Information Security in China: What Can We Learn?

This paper presents an overview of university-based information security education in China. It analyses the potential of education reforms since Xi Jinping declared in February 2014 the Communist Party's intent to turn the country into a cyber power. It compares university education programs with those in Chinese corporations. The dominance of engineering and cryptography in Chinese education programs visible before 2014 is proving hard to reverse, with social science, psychological and managerial studies so prevalent in Western approaches continuing to have almost no visibility. Moreover, the education ministry seems more susceptible than university academics to a hyper-nationalist approach that sees cyber sovereignty as achievable, while many scholars are inherently more comfortable with a globalised approach. The paper concludes that the university education system in China is proving to be as sclerotic and rigid in social science aspects of cyber security as it has been in other areas of social science, even as several Chinese universities rise in international rankings in the physical science and mathematics-based research areas associated with information security. Yet this is an opportunity for win-win cooperation between China and the globalised cyber security industry (an international division of labour), with foreign educators likely to have to offer to fill the gaps in university study options inside Chinese institutions. The paper builds on research for the author's books. *Cyber Policy in China* (Polity 2014) and *Cyber Security in China: The Next Wave* (Springer, forthcoming).

Cyber Security Formation: An Educational Maturity Model for Australia

This paper will be circulated to participants in the Cyber Security Education Policy Workshop on 28 November reviews ten public policy dilemmas—beyond curriculum content issues—which need to be addressed by Australia in 2017 in framing initial leap-frog strategies, new funding levels and execution plans for enhanced cyber security formation (CSF). Its recommendations include a proposal that Australian policy makers in government and industry would benefit from articulating separate strategies for each leg of the "cyber security formation" triad: education, cyber security literacy, and work force development. It suggests that scarce government resources might be best directed to very narrow and high priority needs at an advanced level, such as countering cyber crime or critical infrastructure protection, rather than to the ambition of providing general education for entry level cyber-security operations. It concludes that complexity of the cyber security education challenge speak to the need for a highly focused special program of cyber security education aimed at supporting the creation and sustainment of a Cyber Civil Reserve Corps of some kind.

Mastering the Cyber Security Skills Crisis

The cyber security skills crisis is a key policy issue in many countries, and governments look in part to universities to address it. This paper addresses one narrow question to see how it speaks to the broader challenges: are current Master of Cyber Security programs in Australia preparing students for the workforce? This research flags a new direction for further, much needed research rather than claim to be an exhaustive analysis. The paper outlines cyber

security education as being multi-faceted and multidisciplinary and then identifies current gaps in university-based offerings. It pursues several lines of investigation. The first approach is to scope the field. To do that, and following a brief literature review, the paper proposes a new multi-level matrix, the Cyberspace Education Framework. This framework allows a high-level comprehensive view of cyberspace education. The paper then investigates current generalist master's programs in Australia and the proposition that mission-specific and purpose-driven courses may better prepare students and address the skills crisis than generalist degrees. A survey of cyber security master's students at one university campus and subsequent discussions with other stakeholders revealed a contrast between expectations. The paper then compares the current educational learning outcomes of Master's programs in Australia with the knowledge, skills and abilities (KSA) set out in the U.S. Government's work standards document as a proxy for what would be required for five cyber work roles of high national importance to Australia. It reveals only modest alignment (around 50 per cent) between the several Australian Master's degrees reviewed and U.S. benchmark KSAs, compared with a 97 per cent alignment with them for a specialised Master's degree at University College Dublin. UNSW Canberra does score a 77 per cent alignment for one U.S. identified role with one of its more specialised degrees, and Edith Cowan scores a 67 per cent alignment in the same role (cyber defence incident investigator). The paper concludes that the requirement for purpose-driven and mission-specific cyber security education is increasing and recommends that this become a focus of new initiatives in cyber security education. Universities have an obligation to work with industry and government to ensure that cyber security programs are more directly preparing students for the workforce. That will give Australia more chance to become cyber resilient and an opportunity to become a global leader in cyber security education.