

**Session II Discussion Paper**

**Are there risks for Australia in engaging with Chinese tech and innovation?**Jemma Xu

Privately-owned Chinese companies, SOEs (state-owned enterprises) and government-funded public institutions are seeking international collaborators in technology research and development. Australia is an ideal partner given the quality of its educational institutions, skilled workforce and pre-existing linkages with the PRC due to its significant number of citizens of Chinese heritage. However, one must be mindful of the risks of working with the PRC in science and technology.

Collaboration would mean Australia could benefit in areas where the PRC has a scientific competitive advantage. The PRC is investing immense capital and human resources into science and technology, this year accounting for 26% of the global total spend on research and development. It already leads the world in areas such as drones, facial recognition technology, big data analytics, mobile payments and renewable energy.

With 1.4 billion people, the PRC can also provide product feedback and inputs into training algorithms on a scale and speed that is unmatched elsewhere in the world. This is critical not just to advance technological developments, but also because product feedback is inevitably much slower in a country with a small population like Australia. Australia’s ability to access and use this quantity of data through collaboration with the PRC will be advantageous for developing technology in areas that require big data to train algorithms such as machine learning, facial recognition and artificial intelligence.

On the downside, there are a number of risks, from both a national security and commercial perspective.

Australian companies looking to enter the PRC market regularly express concerns over intellectual property theft. Contractual recourse to intellectual property infringements can become costly and longwinded. Consequently, legal pursuits are often not commercially viable, particularly for startups with limited resources. However, some commercially sound methods to minimise this risk already exist. The advent of cloud computing and reduced costs in cloud storage mean that Australian companies can conduct and store research and development outside of the PRC and only license the usage in the PRC. To comply with PRC laws, any data collected in the PRC must be stored onshore in the PRC. However, aspects such as data inputs, algorithms and analytics that go into forming the core intellectual property can be easily and cheaply stored offshore and be used in the PRC.

There has been public debate about the extent to which PRC private companies should be involved in Australia’s critical infrastructure. For example, Huawei was banned from participating in Australia’s national broadband network (NBN). This was due to Huawei’s alleged ties to the PRC government as well as founder and Chairman Ren Zhengfei’s previous role as an engineer in the People’s Liberation Army (PLA). If Huawei were to manage Australia’s network, the company would have access to technical information which could potentially be used to instigate a cyberattack.

Australia has also expressed reservations about institutional collaboration on tech due to potential military use. The best example of this is the $100m partnership between the University of New South Wales (UNSW) and the PRC government’s Torch program. Twenty-nine PRC partners have signed on, including at least seven companies working in sectors with both civilian and potential military use, such as aerospace, GPS navigation, underwater technology and nanotechnology. Australian universities have a strict risk assessment framework for research partnerships, including detailed due diligence on any overseas collaborations with national security implications.

Nonetheless, it is now widely known that the PLA’s National University of Defense Technology (NUDT) has extensive collaborations with Australian researchers at institutions such as Commonwealth Scientific and Industrial Research Organisation (CSIRO), UNSW, ANU, University of Technology Sydney, and Curtin University. These technologies when further developed will be valuable in a range of military and intelligence operations such as improving the PRC’s military aircraft, secure voice communications and battle management. While the research is funded by the companies themselves, not directly by the PRC government, there is concern that PRC companies would share their research with the PRC government. This could put Australia at a disadvantage should military conflicts arise.

The Australian and PRC governments, as well as various private companies, have made substantial efforts and devoted significant resources to facilitate increased cross border collaboration. The benefits and risks must be carefully evaluated to ensure commercially sound outcomes that do not forgo strategic considerations. Ultimately, risks appear to be the greatest in dual-use technology. However, by adhering to rigorous assessment standards, Australia-China cross border technology collaboration should provide benefits whilst limiting the risks.

**Questions**

* Are there instances of tech and innovation collaboration with the PRC where risk outweights potential benefit for Australia?
* Is there a need for stronger regulation and oversight in projects which include sensitive technology with potential military application, such as the Torch Innovation Precinct collaboration between the University of New South Wales and the PRC government?
* Are there trends in tech and innovation growth where Australian inaction now significantly limits opportunity later?
* Is the issue of sharing intellectual property a cause for concern or optimism for Australian businesses in the PRC?