Australian National University | National Security College

Australian Government | Department of Defence

Technology Surprise Forum | May 2022

In May 2022, the National Security College Futures Hub at the Australian National University hosted, in partnership with the Defence Science and Technology Group (DSTG), a Technology Surprise Forum. The Forum aimed to highlight a range of high impact future technologies that could influence the Australian national security landscape over the next 5 to 10 years.

The Forum brought together science and technology practitioners and researchers from across academia and government to build communities of interest that would generate further research on technology and national security issues.

Papers presented at the Forum addressed the following questions:

- What emerging technological innovations and convergences could surprise government in the medium to long term?
- How can government harness emerging civilian and military technologies to support national security?

Researchers focused on problems they anticipated would be faced by the national security community, and put forward novel ideas and concepts to foster solutions to these problems. For the purposes of this Forum, national security was understood to cover non-defence-related protection of Australia's borders, the threat of terrorism, espionage and foreign interference, and major organised crime.

Suggested topics included (but were not restricted to) technologies and issues such as: the metaverse as a vector for population or political manipulation; brain-machine interfaces; intelligence in the age of deep fakes (including identifying fakes and defeating biometric recognition); quantum computing, cryptography and sensing.

Papers were expected to relate to at least one of the current National Security Science and Technology Priorities:

1. ***Technology Foresight***: The ability to monitor, analyse and evaluate the implications of scientific and technological developments to prevent strategic and tactical surprise.

2. ***Intelligence***: The ability to collect, analyse, integrate, assess and disseminate intelligence with the accuracy, scale and speed required to support timely national security and intelligence decision making.

3. ***Preparedness, Protection, Prevention & Incident Response***: The ability to appropriately equip and prepare Australian agencies to effectively address national security threats and natural or man-made destructive events, including mass-harm and mass-damage incidents, either by preventing their occurrence, or responding and recovering effectively if they have occurred.

4. ***Cyber Security***: The ability to strengthen the cyber security and resilience of critical infrastructure and systems of national significance through the conduct of research and development, and the delivery of advanced cyber technologies, tools, techniques and education.

5. ***Border Security and Identity Management***: The national security community's ability to protect and secure Australia's borders from disease outbreaks, hazardous material and threats to our community, including maximum disruption effect on illegal activity and migration with projected growth in people and cargo movement across Australian borders.

6. ***Investigative Support and Forensic Science***: Law enforcement's ability to prevent, disrupt and prosecute terrorist and criminal activities in a complex transnational and evolving digital environment.

Due to the topics concerned, only proposals from Australian citizens and permanent residents were considered.