



UNSW
SYDNEY



Complex Systems Security

Delivering a better understanding of the security of future networks and platforms; these networks include the Internet of Things, Industry 4.0, Industrial Control Systems that run Australia's critical infrastructure, and resilience of social networks against coercion and soft influence.

Competitive advantage

- Expertise in next-generation networks, critical infrastructure security, cyber-resilience and simulation
- World class experimentation development platforms and lab facilities
- Strong industry links to develop usable outcomes

Impact

- Development of new processes and techniques to discover vulnerabilities in large scale systems
- A holistic perspective on network development and security analysis
- Increasing resiliency of future networks against cyber threat
- Running wargames and scenario-based learning opportunities to understand future threats
- Cyber influence and security simulation platforms for decision support and situational awareness

Successful applications

- Social Media Dataset Generation, Australian Army
- An Intelligent Risk Evaluation Tool for Safeguarding IoT Smart Airports, Cyber Cooperative Research Centre (Cyber CRC)
- Cyber Supply Chain Mission Assurance, Australian Army
- Cyber Impact Analysis Towards Mission Assurance, Defence Science and Technology
- Secure Software Defined Networking for Multi-Bearer Time-Sensitive Distributed Systems, Defence Science and Technology

Capabilities and facilities

- UNSW Canberra Cyber Rang

More Information

Associate Professor Frank den Hartog
UNSW Canberra Cyber

T: +61 (0) 2 6268 8816
E: frank.den.hartog@unsw.edu.au

UNSW Knowledge Exchange

knowledge.exchange@unsw.edu.au

www.capabilities.unsw.edu.au

+61(2) 9385 5008