Intelligent Security

Development of intelligent methods—such as adversarial machine learning and cyber threat intelligence—for automatically detecting, responding to, and preventing advanced persistent threats.

Competitive advantage

- Development of Cyber threat intelligence models such as intrusion detection, privacy-preserving, and digital forensics-based statistics, machine and deep learning models
- Development of automated penetration testing methods based on AI planning
- Design of new testbed architectures for Industry 4.0 networks
- Leading analysis of how AI could develop automated cyber applications, for the Australian Army, Australian Federal Police (AFP), and the Cyber Security Cooperative Research Centre (CSCRC)
- Advanced threat intelligence models for deterring cyber threats and reducing financial losses and critic infrastructure damages

More Information

Dr Nour Moustafa

School of Engineering and Information Technology

T: +61 (0) 416 817 811
E: nour.moustafa@unsw.edu.au

UNSW Knowledge Exchange

knowledge.exchange@unsw.edu.au

www.capabilities.unsw.edu.au

+61 (2) 9385 5008

Impact

- The increase in everything-connected, online systems that both sense from and interact with the physical world poses a security risk. The extent to which countries such as Australia are already dependent on cyber-physical systems – which is projected to increase – means that the impact of any disruption is potentially catastrophic.

Successful applications

- Evaluating Network Intrusion Detection based Deep Learning and Graph Models
- A Collaborative Host-Network Anomaly Detection Framework for Internet of Things
- A new intelligent wargaming web service-based Machine Learning for the Australian Army to understand human influences and behaviours

Capabilities and facilities

- Cyber Range Labs
- Digital Forensics Lab
- IoT Lab