INFORMATION WARFARE

CAPABILITY PROSPECTUS AND EXPRESSION-OF-INTEREST
TO DEVELOP AN INFORMATION WARFARE CENTRE
IN COLLABORATION WITH
THE AUSTRALIAN DEFENCE FORCE

OCTOBER 2019 V 1.0
A preliminary proposal to establish a world-class information warfare research centre as joint collaboration between the Australian Defence Forces and The University of Queensland.

**CONTENTS**

<table>
<thead>
<tr>
<th>CONTENT</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Teaching &amp; research</td>
<td>8</td>
</tr>
<tr>
<td>BreakerSpace</td>
<td>10</td>
</tr>
<tr>
<td>Teaching &amp; Research</td>
<td>12</td>
</tr>
<tr>
<td>School of Political Science and International Studies</td>
<td>15</td>
</tr>
<tr>
<td>Leadership and organisational innovation research and teaching capabilities - UQ Business School</td>
<td>16</td>
</tr>
<tr>
<td>AusCERT</td>
<td>19</td>
</tr>
<tr>
<td>Joint research innovation hub</td>
<td>20</td>
</tr>
<tr>
<td>Collaboration</td>
<td>21</td>
</tr>
</tbody>
</table>
INTRODUCTION

Information warfare research collaboration proposal

The University of Queensland is pleased to submit a proposal to collaborate with the Australian Army’s Information Warfare division to develop a dedicated Information Warfare centre for teaching and research.

UQ is one of Australia’s leading research organisations, consistently rated in the global top 50. Moreover UQ has an international reputation for the quality and impact of its research. With six faculties and eight research institutes across 30 teaching and research sites and three campuses, the University is recognised for the scale of its operations and breadth of its cross-disciplinary expertise.

Integrating complex systems for IW research or preparedness is a task UQ is well qualified to deliver.

Our proven record of working collaboratively with international corporates such as Boeing and DOW demonstrate the University’s capacity to perform to exacting international standards.

UQ-ADF INFORMATION WARFARE CENTRE

We propose a three-pronged collaboration with the ADF.

UQ’s skilled teaching staff are ready to train and upskill ADF personnel in the latest cyber micro-credentials.

The creation of a complementary BreakerSpace will be an immediate focal point for co-design and rapid roll-out.

We also envisage the establishment of a Research Innovation Hub as the capstone of our collaboration. The hub will be co-designed and tailored to meet with the ADF’s unique strategic and operational priorities in the Information Warfare space.

UQ’s researchers have established experience in cooperating with Australian Government agencies to deliver executive education targeted specifically to meet the needs of its partners.

UQ delivers world-class, research innovation, as evidenced by the Boeing Research and Technology Australia-UQ Technology Centre – Boeing’s first such research hub in the Asia-Pacific.

More than 30 engineers have been hosted at the Boeing centre since 2017. The centre serves as a focal point for aerospace research innovation and training, including the development of specific technologies (e.g. unmanned vehicles and...
The University is eager to direct its world-class research and education strengths to meet the needs of organisations working in competitive domains at the cutting-edge of technological change.

autonomous systems) of immediate relevance to the ADF.
All told, UQ collaboration and engagement with Boeing has extended over 13 years, including cumulative research funding from Boeing of more than $10.5 million.
UQ has collaborated with Boeing in information technology and electronic engineering research, as well studies in human behaviours and systems management. Boeing also provides a wide range of support for undergraduate training and PhD programs.
The success of the centre illustrates UQ’s experience in working with industry partners for mutual benefit.
The University is eager to direct its world-class research and education strengths to meet the needs of organisations working in competitive domains at the cutting-edge of technological change.
Another showcase partnership is UQ’s relationship with the Dow Chemical Company.
Dow’s donation of $US10 million towards the UQ Dow Centre has enabled commitment to delivering solutions to globally significant challenges by generating and communicating new knowledge and analysis.

RESEARCH PARTNERS
UQ is a global top-50 university with the expertise and infrastructure to help partners find solutions to compelling technical, economic and environmental challenges.
Our expanding range of external partners includes many levels of government, private industry, community groups, industry associations, not-for-profits, foundations, and other sectors.
In terms of information warfare research, however, UQ has advanced capability across three key areas, namely: education/training, a bespoke breakerlab, and collaborative research.
The following document outlines what UQ would bring to a joint ADF-UQ Information Warfare research centre.
ADF-UQ Information Warfare Research Centre

The proposed centre will be accomplished through three pillars of activity —

1. **Training programs**
   Defence personnel can undertake a variety of short UQ courses, distance learning, executive education, online micro credential activities and more, with a view to refreshing their training.

2. **BreakerSpace**
   The opposite of a ‘maker’s lab’, BreakerSpace is a state-of-the-art facility where students, interns and other researchers work alongside ADF personnel engaging in training exercises and challenges aimed at breaking, penetrating and proofing cyber security defences.

3. **Collaborative research innovation**
   A jointly run lab where UQ’s best researchers work with Defence personnel on research and innovation challenges.

- Office of the Deputy Vice-Chancellor (Research)
- School of Political Science and International Studies
- Faculty of Engineering Architecture and IT
Australia's strategic environment is being revolutionised by the growing salience of the cyber-domain. At a strategic level, Australia’s critical infrastructure is increasingly susceptible to targeting and disruption from a plethora of sophisticated state-based and non-state adversaries. Domestically, the rise of digital media has left Australia and other western democracies vulnerable to hostile information operations, that aim to inflame political polarisation and undermine public faith in the integrity of our electoral institutions.

Revolutionary advances in cryptography and communication technologies have meanwhile strengthened organised criminals’ opportunities for illicit profit, while also radically enhancing terrorists’ capacities for recruitment, financing and operational coordination at a global level. The growing cyber-warfare capacities of key regional states threaten the integrity of the Australian Defence Force’s command and control systems, and jeopardise the combat capabilities of an increasingly ‘networked’ Australian Army, fighting in joint operations with both other elements of the ADF and also with other equally ‘networked’ allies.

Working together to strengthen IW resilience and capability

... the centre will also build on UQ’s established experience and track-record of success working with industry partners to create and deploy cutting-edge dual-use technologies.

The proposed centre would leverage UQ’s full spectrum teaching and research capabilities, which encompass deep expertise in the technological as well as geopolitical dimensions of information warfare. Additionally, the centre would also build on UQ’s established...
UQ’s relative proximity to existing key elements of Army’s combat, command, instruction and training infrastructure provides strengthens its claims to co-host an information warfare centre with the ADF.

experience and track-record of success working with industry partners to create and deploy cutting-edge dual-use technologies. UQ’s relative proximity to existing key elements of Army’s combat, command, instruction and training infrastructure strengthens its claims to co-host an information warfare centre with the Australian Army. Queensland hosts two of Australia’s three combat brigades (3rd Brigade headquarter in Townsville as well as 7th Brigade headquartered in Brisbane), as well as the 1st Division Headquarters (Brisbane) and the Land Warfare Centre (headquarter in Kokoda barracks Canungra, less than 90 minutes from UQ’s St Lucia campus).

SHOALWATER BAY TRAINING AREA

Further afield, the Shoalwater Bay Military Training Area is a key site for training in joint warfare, both for the ADF and with key allies such as the United States. The proximity to high concentrations of serving personnel will facilitate the training and education dimension of the proposed partnership, as well as providing on-the-ground opportunities for efficiently testing and refining technologies developed in the proposed research innovation hub.
UQ’s **teaching** and **research** capabilities in the information warfare domain

UQ offers holistic capabilities for teaching and research in the information warfare space, uniquely positioning it as a preferred partner for the ADF.

Specifically, UQ offers research and teaching strengths in both the technical as well as the political and strategic aspects of information warfare.

UQ moreover has an established track-record of success in partnering with industry to deliver world-class, cutting edge research innovation, as evidenced by UQ’s hosting of the Boeing Research and Technology Centre, the first industry-university research hub of its kind that Boeing has undertaken in the Asia-Pacific.

UQ’s researchers have established experience in cooperating with both Australian Government agencies and the Australian military to deliver executive education and micro-credentials targeted specifically to meet the needs of these industry partners.

A core mission of the UQ-Australian Army Information Warfare Centre will be the delivery of relevant training, short courses and micro-credentials to students in the domain of information warfare, broadly defined.

The training program and accompanying micro-credentials will be customised to meet the Australian Army’s specific needs, but will build upon UQ’s established and broad-ranging strengths in this area.

UQ offers a custom-built master’s program in cyber security, with a common inter-disciplinary core taken by all students, followed by specialisation streams in cyber defence, leadership, cyber criminology and cryptography, and completed with a research or industry-based capstone project.
This program can be readily adapted to the defence context, perhaps through the creation of a dedicated specialisation available only to defence personnel.

At the undergraduate level, UQ’s Bachelor of Computer Science has a cyber security major, which contains study on technical fundamentals as well as topics such as vulnerability analysis and penetration testing. The program is currently under review and the opportunity exists for influence in the major content and design.

Beyond traditional teaching offerings, UQ Cyber Security in partnership with AusCERT (see page X) is working to offer a growing portfolio of professional certifications ...

Meanwhile, UQ’s School of Political Science and International Studies (POLSIS) has extensive experience in designing and delivering micro-credentials to government partners, both in Australia and overseas.

POLSIS has worked extensively with the Department of Foreign Affairs and Trade (DFAT) to deliver training to diplomats and high level civil servants from key African and Pacific Island states, while the Asia-Pacific Centre for the Responsibility to Protect (co-funded by DFAT) also has extensive experience in delivering micro-credentials on atrocity prevention to government partners in the Asia-Pacific.

CYBER MOOC

POLSIS’ Dr Sebastian Kaempf has designed and delivered a Massive Open Online Course (‘Global Media, War, and Technology’) dedicated specifically to examining the intersection between digital media, information warfare and the evolving cyber-security landscape. Elements of this course could be customised to meet the ADF’s educational needs in this space.
INFORMATION WARFARE RESEARCH
COLLABORATION PROPOSAL

TEACHING & RESEARCH

SECURE SOFTWARE ENGINEERING

Together with partners such as the Defence Science and Technology (DST), researchers in formal methods and secure software engineering from ITEE are working on solutions which enable the detection and reduction of security vulnerabilities arising in complex, interconnected software systems, and developing interactive and automated tools to assist with identifying and analysing such vulnerabilities. This work includes enabling secure software development via the use of programming languages customised for analysis with fully automatic tools.

NATIONAL SECURITY AND CYBER POLICIES

Engaging with leading think tanks, policy advisors, legislators and key government agencies, experts from the Centre for Policy Futures, ITEE, HASS and the School of Law are quantitatively and qualitatively researching the impact and effectiveness of policies addressing national security, foreign affairs, cyber security, regional and international coordination, and the global cyber security skills shortage.

MICROMASTERS PROGRAM

UQ Business School (UQBS) already offers the ground breaking MicroMasters Program in Business Leadership, a tailored online program drawing from elements of the flagship UQ MBA program, and serves as foundational coursework for numerous UQ programs. The MicroMasters program was recently selected as a finalist for the international 2019 edX prize for exceptional contributions to online teaching and learning.

The program has also been tailored into a series of blended leadership courses (combined online and face-to-face delivery) in executive education that specifically targets technical teams and feed into UQ’s MBA program; these executive-level courses recently won a gold award for leadership capability development at the 2019 LearnX Live awards.

More broadly, UQ is an industry leader and innovator in high-quality online education, with the facilities, staff, and experience to design, develop, and produce world-class online coursework.

CYBER CRIMINOLOGY

Together with leading Australian and international law enforcement agencies, experts from HASS (Criminology), TC Beirne School of Law, and ITEE are researching crime prevention and intervention techniques, policies and building crime fighting tools (e.g. visualization, cyber crime attribution) which can be applied into cyber and cyber-enabled crime. The group is also focused on addressing the skills gaps faced by frontline officers, and researching into the understanding and de-anonymising criminal activities on social media platforms and the Dark Web.

More broadly, UQ is an industry leader and innovator in high-quality online education, with the facilities, staff, and experience to design, develop, and produce world-class online coursework.
The UQ Information Warfare BreakerSpace will form a critical node in our IW teaching and learning infrastructure.

The BreakerSpace is envisaged as a hands-on lab where students will have the opportunity to ‘stress test’ information systems and refine their defensive and offensive cyber warfare skills in a secure environment.

More broadly, the BreakerSpace will provide students with direct hands-on experience in understanding, manipulating and modifying relevant hardware and software pertaining to Information Warfare. The BreakerSpace will serve as an incubator for the Army’s next generation of cyber warriors, providing them with the practical skills and experience necessary to defend Australia’s cyber assets and critical infrastructure, and as well as to develop the offensive cyber capabilities necessary to deter attacks from both sophisticated state-based adversaries as well as non-state cyber threats.

In the technical domain, UQ hosts researchers who enjoy world-leading research expertise in cyber security.
Along with AusCERT and energy and critical infrastructure sectors, experts from UQ’s cyber security, cyber physical systems and power and energy systems groups, UQ humanities researchers and industry partners, Siemens and Redback Technologies, are working on addressing cyber security risks and challenges, and proposing new solutions and resilient communication protocols across the energy, industrial control systems, industrial internet of things (IIoT), internet of things (IoT), drones and wireless sensor networks.

DATA PRIVACY AND USER DATA CONTROL

Experts from the School of ITEE and Faculty of Humanities and Social Sciences (HASS) (Criminology, Political Science) are working on the technical, ethical and policy challenges around data control and privacy. Researchers are working with international partners on data accountability, data provenance tracking, cyber attack attribution, privacy-preserving algorithms, homomorphic encryption, encrypted search, and a data ‘kill switch’ for online and cloud computing users. Researchers are also working with indigenous data sovereignty experts from Australia and New Zealand.
UQ offers a custom-built master’s program in cyber security, with a common inter-disciplinary core taken by all students, followed by specialisation streams in cyber defence, leadership, cyber criminology and cryptography, and completed with a research or industry-based capstone project. This program can be readily adapted to the defence context, perhaps through the creation of a dedicated specialisation available only to defence personnel.

**Professor Ryan Ko**  
Chair and Director of UQ Cyber Security at The University of Queensland  
Prof. Ko’s applied research in cyber security focuses on ‘returning control of data to cloud computing users’. His research reduces users’ reliance on trusting third-parties and focusses on (1) provenance logging and reconstruction, and (2) privacy-preserving data processing (homomorphic encryption). Prof. Ko has a strong record in establishing university-wide, multi-disciplinary academic research and education programs, including NZ’s first cyber security graduate research program and lab (CROW) in 2012, NZ’s first Master of Cyber Security (encompassing technical and law courses), the NZ Cyber Security Challenge since 2014, and the New Zealand Institute for Security and Crime Science – Te Puna Haumaru, the Evidence Based Policing Centre (at Wellington with NZ Police and ESR), and Master of Security and Crime Science in 2017.

**A/Prof. John Williams**  
Deputy Director of the UQ Cyber Security initiative  
Dr Williams was responsible for developing the UQ Cyber Security initiative and led development of the new UQ Master of Cyber Security. He has an extensive track-record in industry and external partnership and entrepreneurship, including a successful spinout of a technology company from UQ in 2007, and its subsequent acquisition by a major semiconductor vendor in 2012.

**Dr Mahsa Baktashmotlagh**  
Dr Baktashmotlagh is a UQ lecturer with a research focus on developing machine learning and data mining techniques applied in visual data analysis (visual domain adaptation, video classification, and animal’s foraging behavioural analysis), road traffic networks (mining large-scale road traffic networks and building a road load balancing tool to predict congestion on any road in the city), biomedical data (prediction of neonatal sepsis), and finance (hedging foreign exchange trading risks).
Prof. Benjamin Burton
Benjamin Burton’s research interests include computational geometry and topology, combinatorics, and information security. Prof. Burton’s research involves a blend of techniques from pure mathematics and computer science. His main interest is in computational geometry and topology in three and four dimensions, looking at problems such as how a computer can recognise whether a loop of string is knotted, or how it can identify large-scale geometric structures in a three-dimensional space. He is the primary author of the open source software package Regina, which implements state-of-the-art algorithms in this field. His multi-disciplinary background includes a PhD in geometry and topology, an honours degree in combinatorics, research experience in information security, and three years as a research analyst in the finance industry. He has worked at several universities in Australia and overseas.

A/Prof. Dan Kim
Dr Dan Kim’s research interests include cyber security and dependability for various systems and networks:
- Cyber security modelling and analysis: models, metrics and measurement
- Cloud computing security
- Internet of Things/Edge security
- Software defined networking security
- Artificial intelligence and big data analytics for security
- Interpretable, dependable and secure machine learning/deep learning

Dr Larissa Meinicke
Dr Meinicke’s research interests include mathematical notations and techniques for the formal specification and development of computing systems; probabilistic systems; computer security; abstract algebra and refinement algebra; real-time and fault-tolerant systems.
A/Prof. Marius Portmann
Dr Marius Portmann was awarded his PhD in Electrical Engineering from the Swiss Federal Institute of Technology (ETH) in Zurich in 2003. His research interests are in overlay and peer-to-peer networks, wireless mesh networks, network protocols, software-defined networking, cyber security and blockchain technology.

Prof. Timothy Ralph
Professor Timothy Ralph obtained a BSc Hons from Macquarie University in 1989 and a PhD in Physics from The Australian National University in 1993. He has held three Australian Research Council Fellowships – Postdoctoral, QEII and Professorial. He is currently Node Director for the ARC Centre of Excellence for Quantum Computation and Communication Technology at UQ. His research interests include linear optics quantum computation, quantum communication with lasers, and relativistic quantum information.

Dr Jacqui Romero
Dr Romero was awarded her PhD at the University of Glasgow. Her research interests cover opto-mechanical quantum measurements, building nodes for an entangled quantum network, and quantum causality.

Dr David Ross
UQ Adjunct Associate Professor Information Security Specialist
Dr David Ross is one of Australia’s leading information security experts. A managing consultant for security practice with Australian telco Telstra, Dr Ross was awarded his PhD by investigating how to secure wireless Local Area Networks. He has worked with the Australian Defence force since 1979 and was the Chief Information Security Officer for Bridge Point Communications (2008–2015).

A/Prof. Graeme Smith
Dr Graeme Smith’s research interests are in formal methods: mathematical notations for modelling software systems; automated tool-support for analysing such models; and development of software systems from such models. He received his PhD from The University of Queensland in 1993. Since then he has worked at universities and research institutes in France, Australia and Germany. His past research has focused on the development of the object-oriented formal specification language Object-Z, and its integration with other formal specification languages and techniques to facilitate the modelling of concurrent and real-time systems. Currently he is investigating the use of formal methods for verifying lock-free algorithms running on modern multi-core architectures.

Prof. Shazia Sadiq
Professor Shazia Sadiq is based at UQ’s School of Information Technology and Electrical Engineering where she is part of the Data and Knowledge Engineering research group involved in teaching and researching databases and information systems. Professor Sadiq holds a PhD in Information Systems and a Masters Degree in Computer Science from the Asian Institute of Technology, Bangkok, Thailand. Her main research interests are innovative solutions for business information systems that span several areas including business process management, governance, risk and compliance, data quality management, workflow systems, and service science.
School of Political Science and International Studies

The UQ School of Political Science and International Studies (POLSIS) hosts a cluster of world-class researchers with expertise in examining new and emerging security challenges, including threats and challenges in the cyber-domain.

POLSIS’ researchers with relevant teaching and research expertise include:

**Prof. Alex Bellamy**

Prof. Bellamy leads the Asia-Pacific Centre on the Responsibility to Protect, a joint UQ-DFAT-funded research centre responsible for researching ‘new’ wars and atrocity prevention, and for training civil servants in Asia-Pacific countries on the prevention of mass atrocity crimes and genocide. Prof. Bellamy has also taught humanitarian operations and International Humanitarian Law at the Special Air Service annual executive course, as well as entry level short courses at Royal Military Academy Sandhurst. In Australia, he has also taught into the Australian Command and Staff Course at what was then the Australian Defence College (now the Australian War College), and was also previously on the College’s academic advisory board. The Asia-Pacific Centre for the Responsibility to Protect, which Professor Bellamy leads, also designed DFAT’s training package on Conflict/atrocity early warning and reporting, and now trains their trainers on how to deliver this training package.

**Dr Sebastian Kaempf**

Dr Kaempf an expert on asymmetric warfare and the intersection between digital media and cyber security, designed and taught ‘Global Media, War and Technology’, the first Massive Open Online Course (with 10,000 students and counting) dedicated to this topic. Dr Kaempf also hosts a semi-annual ‘media lab’ in his course ‘Global Media, War, and Peace’, which provides students with hands-on experience in making sense of digital media’s transformative impact on war-fighting in the contemporary context.

**A/Prof. Sarah Percy**

Dr Percy’s research focuses on transnational security challenges and unconventional combatants in the Indo-Pacific. She has previously worked extensively with the Australian military as a non-resident Fellow in the Royal Australian Navy Seapower Centre.

**A/Prof. Andrew Phillips**

Dr Phillips is an expert on international orders and ‘great transformations’ in world politics, who has written extensively on the intersection between disruptive military innovation and ideological extremism as a catalyst for international orders’ breakdown, and has previously served as the Visiting Fellow for International Order and Transnational Security Challenges at the Australian War College.

Beyond their regional expertise, Bellamy, Percy and Phillips also have experience in designing and delivering short courses to serving military personnel...

**Leadership and organisational innovation research and teaching capabilities**

The UQ Business School has more than 200 world-class academics, with existing research and teaching strengths in the areas of business information systems, innovation, and leadership.

The breadth of expertise in these areas is broad, including the following academics specifically...
Dr Clutterbuck teaches in the areas of Internet security and infrastructure. Awarded his PhD (Theoretical Computing Science) in 2005, his PhD research focused on the measurement and management of the availability of distributed software services.

conducting research and teaching in the area of information security, governance and leadership:

**Dr Micheal Axelsen**

Dr Axelsen is an experienced Information Systems (IS) professional and accountant (FCPA of CPA Australia) with 15 years’ experience in IS consulting. His career includes the evaluation of IS projects, IS audit and IT management and governance. Micheal’s published research is in the areas of the use of intelligent decision aids, Information Systems (IS) audit, and Information Technology (IT) governance. Before receiving his PhD, Micheal chaired the IT & Management Centre of Excellence for CPA Australia.

**Dr Peter Clutterbuck**

Dr Clutterbuck teaches in the areas of Internet security and infrastructure. Awarded his PhD (Theoretical Computing Science) in 2005, his PhD research focused on the measurement and management of the availability of distributed software services. This research spanned the areas of IT security architectures and IT networking protocols. Peter’s current research direction is within the area of IT security auditing. Peter has held positions within the public and private sectors in personnel, project, and technology management capacities. Ongoing consultancy activities include applications programming and secure network configuration.

**Prof. Nicole Gillespie**

Professor Gillespie is the KPMG Chair in Organisational Trust and Professor of Management at the UQ Business School, and an International Research Fellow at the Centre for Corporate Reputation, Oxford University. Trained as an organisational psychologist, Nicole’s research focuses on trust development and repair in organisational contexts, and in contexts where trust is challenged. Current research projects focus on understanding stakeholder trust in organisations and industries, organisational trust repair, designing trustworthy organisations, trust in Artificial Intelligence, and stakeholder trust and uptake of telemedicine. Nicole has more than
Dr Liivoja recently produced a joint-research report on autonomous cyber capabilities with the NATO Cooperative Cyber Defence Centre of Excellence.

15 years' experience in designing and delivering MBA, Executive MBA, specialist masters and undergraduate courses. She is the recipient of five teaching excellence awards and, together with her PhD student, two best paper awards from the Academy of Management.

A/Prof. Tyler Okimoto
Dr Okimoto teaches courses on leadership, human resources, conflict/negotiation, and decision-making in the undergraduate, MBA, and executive levels, including online and blended deliveries. In particular, he has developed and delivered award-winning programs on leadership within the context of technical teams. Prior to joining UQ in 2011, he received his PhD in Social and Organisational Psychology from New York University in 2005, and worked as a Postdoctoral Researcher in the School of Psychology at Flinders University in Australia, and in the School of Management at Yale University. His research focuses on how diverse viewpoints devolve into conflict, as well as how that diversity can be bridged to overcome conflict and achieve greater levels of problem-solving and collaboration.

A/Prof. Rain Liivoja
Dr Rain Liivoja is an Associate Professor at the TC Beirne School of Law, The University of Queensland. He also holds the title of Adjunct Professor of International Law at the University of Helsinki, where he is affiliated with the Erik Castrén Institute of International Law and Human Rights. Rain’s current research focuses on the legal challenges associated with the military applications of science and technology generally and biosciences specifically. His broader research and teaching interests include the law of armed conflict, human rights law and the law of treaties, as well as international and comparative criminal law. He is the author of Criminal Jurisdiction over Armed Forces Abroad (Cambridge University Press 2017), and a co-editor of the Routledge Handbook of the Law of Armed Conflict (Routledge 2016) and International Law-making: Essays in Honour of Jan Klabbers (Routledge 2013).
Australia’s Pioneer Cyber Emergency Response Team — AusCERT

UQ-based AusCERT helps members prevent, detect, respond to and mitigate cyber- and internet-based attacks.

AusCERT is Australia’s leading Cyber Emergency Response Team, providing information security advice to its members – including the higher education sector.

AusCERT is the single point of contact for dealing with cyber security incidents affecting or involving member networks.

As a not-for-profit security group based at The University of Queensland, AusCERT helps members prevent, detect, respond to and mitigate cyber- and internet-based attacks.

Formed in 1993, AusCERT is one of the oldest CERTs in the world and was the first CERT in Australia to operate as the national CERT, which it did until 2010.

AusCERT monitors and evaluates global cyber network threats and vulnerabilities, and remains on-call for members after hours.

AusCERT publishes the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.

AusCERT’s Incident Management Service can be an effective way to halt an ongoing cyber attack or, provide practical advice to assist in responding to and recovering from an attack.

Within UQ, AusCERT is part of Information Technology Services (ITS). AusCERT is self-funded and covers its operating costs through a variety of sources including member subscriptions, the annual AusCERT conference and service contracts.

AusCERT has more than 500 corporate members across Australia and Oceania.

As an active member of the Forum for Incident Response and Security Teams (FIRST) and Asia Pacific Computer Emergency Response Team (APCERT), AusCERT has access to accurate, timely and reliable information about emerging computer network threats and vulnerabilities on a regional and global basis.

Additionally, AusCERT maintains a large network of trusted CERT contacts in North America, the United Kingdom, Europe and throughout Asia. AusCERT uses these contacts to receive early warning of global threats and to assist in responding to incidents which span jurisdictions.

Incident Management

The AusCERT Incident Management Service assists organisations to detect, interpret and respond to attacks from around the world. AusCERT acts as a trusted intermediary, coordinating communication about incidents between affected parties.

The AusCERT team provides proactive and reactive incident response assistance actively seeking information from various sources to help find data relevant to you. They take immediate action and follow well-defined protocols to obtain a resolution and satisfactory outcome.

Information Sharing & Analysis Centre (ISAC)

Over the past few years, AusCERT has coordinated and run a highly-successful information sharing group for the tertiary education sector (CAUDIT-ISAC), and established an Information Sharing and Analysis Center (AusISAC); now available to general members.

Phishing Take-Down

AusCERT’s Phishing Take-down service works to reduce brand damage by requesting the removal of fraudulent websites. The service puts the safety of your brand at the forefront by detecting and acting immediately if your organisation is affected.
A joint UQ-ADF research innovation hub

The capstone of UQ’s collaboration with the ADF will be the UQ-ADF Information Warfare Research Innovation Hub.

This research innovation hub will build on UQ’s established record of success in collaborating with outside partners to develop cutting-edge technological innovations tailored to the latter’s needs. UQ will leverage its world-class research in cybersecurity to develop the information warfare applications most suited to the Australian Army’s needs in a rapidly evolving and increasingly complex and contested strategic environment.

SECURITY AND FOREIGN INFLUENCE

Clearly in such a collaboration, careful attention must be paid to matters of defence sensitive training, capacity building and partnered research.

The University of Queensland is in the early stages of preparing for membership in DISP (Defence Industry Security Program), and involved in round-table discussions with Defence and other Group of Eight and the broader university sector on the best ways to approach this capability.

All joint activities undertaken between IWD and UQ will be assessed for their sensitivity, and appropriate boundaries on personnel, physical and cyber security will be instituted in consultation with Defence.

The UQ Long Pocket site is a potential location for these activities, with the opportunity to create dedicated and secure teaching, workshop and laboratory spaces as required.

WORKSHOP OCTOBER 2019

UQ would be pleased to present a more comprehensive pitch, as well as a cross-faculty demonstration of our research and teaching capabilities in the Information Warfare space, in the form of a workshop hosting key decision-makers from the Australian Army’s Information Warfare division at a time of the latter’s convenience, ideally in Oct or Nov 2019.
COLLABORATION

SECURE QUANTUM COMMUNICATIONS
Experts from the School of Mathematics and Physics (SMP) and School of Information Technology and Electrical Engineering (ITEE) are addressing the fundamental and applied scientific challenges of quantum key distribution, error correction protocols, quantum alphabets, security in higher-dimensional quantum systems and post-quantum cryptography.

CYBER AUTONOMY AND AUTOMATION
Together with AusCERT, large IT multinationals, and cloud service providers, researchers are working on next-generation solutions that teach computers how to discover their own vulnerabilities, and automatically patch or heal themselves. This involves application of artificial intelligence (machine learning and AI planning) techniques, and automating cyber security tools and incident response workflows. The goal is to be able to equip human administrators with the tools they need to reduce the time taken between discovering and remediating vulnerabilities in critical infrastructure.

SECURE COMMUNICATIONS FOR SPACE
Experts from SMP, Faculty of Engineering Architecture and IT (EAIT), and the Centre for Policy Futures are working on the policy and technical aspects of cyber security and secure communications for space systems. From mission control centres to satellites, we are understanding and addressing the cyber security risks for the sector and implications for national security. We are also engineering next-generation resilient, secure communication protocols and systems suitable for space deployments.

CYBER LAW AND ETHICS
Experts from the HASS, TC Beirne School of Law, ITEE and the Criminology Department are researching on domestic and international laws and ethical norms addressing cyber security, cyber crime, data privacy, mandatory data breach disclosures, encryption, social media, bots and the application of artificial intelligence. Researchers analyse and evaluate the effectiveness of legislative frameworks and identify gaps in the domestic and international settings.

UQ ENERGY TESTLAB
As part of a national $5 million pilot program, UQ is building an Industry 4.0 Energy Testlab led by Professor Tapan Saha of the Power and Energy Systems Group.

The lab, which will be completed by the end of 2019, will provide a physical space for businesses and researchers to trial, explore and showcase Industry 4.0 technologies and processes in the energy and cyber-physical security domain, enable educational institutions and industry, particularly small-to-medium enterprises, to collaborate, and develop skills needed to take full advantage of opportunities presented by Industry 4.0. In partnership with Siemens Australia, Testlab will focus on energy management. A major theme of this program is the security of industrial control systems in the energy sector.
Since the launch of the world’s first artificial satellite in 1957, there has been a global fascination in flight and space exploration, particularly hypersonic flight.

At UQ’s Centre for Hypersonics, researchers have been conducting research for more than 20 years into all aspects of hypersonic flight.

School of Mechanical and Mining Engineering researcher and Chair of Hypersonic Propulsion Professor Michael Smart leads UQ’s research into scramjet technology, a sustainable engine alternative to rockets. A scramjet is a high-speed plane with air-breathing engines able to fly long distances across the Earth very quickly, making it lighter and more fuel-efficient.

“A scramjet is like a plane. When it has accelerated to its maximum velocity, the upper-stage rocket carrying the satellite blasts off its back, and the scramjet simply turns around and flies back to base. We can then re-fuel and launch it again,” Professor Smart says.

He and his team have developed scramjet engines to the point where they can be used in a space-launch system. Professor Smart and the centre are also investigating the means of flying at hypersonic speed — or travelling faster than five times the speed of sound.

This research is being undertaken with the Defence Science and Technology Group of Australia, the US Air Force Research Laboratory, and Boeing as part of the HiFiRE (Hypersonic International Flight Research Experimentation) Program.

In May 2016, the program successfully launched a hypersonic test rocket from the Woomera Test Range in South Australia, achieving Mach 7.5 (9200 km/h) and reaching 278 kilometres above Earth.
**WORLD’S FIRST BIOFUEL FLIGHT BETWEEN THE UNITED STATES AND AUSTRALIA**

In January 2018, Australian airline Qantas piloted the world’s first biofuel flight between the United States and Australia, with UQ researchers helping to provide the fuel.

The historic trans-Pacific 15-hour flight from Los Angeles to Melbourne operated with about 24,000 kg of blended biofuel, saving 18,000 kg in carbon emissions.

The plane was powered by *Brassica carinata* (carinata), a non-food, industrial type of mustard seed — fields of which are being trialled at UQ Gatton.

Faculty of Science researcher Dr Anthony van Herwaarden led the seed crop trials in collaboration with Agrisoma BioSciences, a Canadian based agricultural-technology company that has partnered with Qantas.

According to data from the US Energy Information Administration (EIA), Australia consumes about 125,000 barrels of jet fuel each day.

Qantas has also reported that jet fuel accounts for up to 95 per cent of emissions related to flying.

Across its life-cycle, using carinata-derived biofuel can reduce carbon emissions by 80 per cent compared to traditional jet fuel.

As a ‘drop-in’ crop, it requires no specialised production nor processing techniques. Carinata is also water efficient and field trials have demonstrated it should do very well in the Australian climate.

The Australian field trials were conducted with UQ’s Dr Christopher Lambrides, University of Melbourne Associate Professor Phillip Salisbury and Trent Potter of Yeruga Crop Research.

**SOLAR POWERED DESALINATION PROJECT IN CHILE**

An agreement between UQ’s Sustainable Minerals Institute Centre of Excellence in Chile (SMI-ICE-Chile) and TRENDS Industrial paves the way for collaboration on an integrated multi-user desalination supply system in Chile’s Atacama region.

TRENDS Industrial is the company behind the Energías y Aguas del Pacífico project (ENAPAC) a solar powered desalination project in the Atacama Region which aims to ensure the stability of the industrial water supply.