

An Introduction to **National Security Research at Cranfield**

Who we are

Specialist postgraduate-only
as a **research-focused professional community**



100%
of our defence and security staff are **security cleared**



Our **Digital Forensics Unit** is one of the longest established forensic units in the world



81%
of our research is classed as **world-leading or internationally excellent**

Over 3,000
delegates and exhibitors, representing more than 700 companies, academic institutions and government agencies **attend our symposia annually**

UK No.1
for **research income from industry per academic**
(Higher Education Business and Community Interaction (HE-BCI) Survey (three year average between 2015 and 2018))

Working with over 1,500 industrial clients and partners across the globe

Six time
winner of the prestigious **Queen's Anniversary Prize**



THE QUEEN'S ANNIVERSARY PRIZES
FOR HIGHER AND FURTHER EDUCATION
2017

Over £100m
of investment in **new facilities over the past four years**

Cranfield University is taking the lead for the Academic Resilience and Security Community (A-RiSC), a network of 30 UK universities formed to help government and industry access academic experts and the latest research and knowledge in national security. It is recognised by the Home Office, other government departments and by industry as an important conduit to expertise in this field.

"The wealth of experience and expertise within Academic RiSC will continue to provide vital insights across the UK national security system."

Richard Alcock,
Chief Operating Officer for the Office for Security and Counter Terrorism, Home Office

What we offer

Cranfield University is a postgraduate specialist for research and teaching in science, technology, engineering and management. As one of the top five research-intensive universities in the UK, we are making a significant difference to industry by working with key UK and international government decision makers including AWE, BEIS, Defra, DfT, Dstl, EU, Home Office, Metropolitan Police Service, Ministry of Defence, Ministry of Justice and US DOD.

Through the applied way we undertake our research coupled with access to some world-class secure, industrial-scale test and evaluation facilities and subject matter experts we understand specific organisations' needs, making impact to the security sector of the UK and beyond.

Through our themes of Defence and Security, Aerospace, Energy and Power, Environment and Agrifood, Management, Manufacturing, Transport Systems and Water, we cover many of the UK's Critical National Infrastructure (CNI) sectors.



National Security at Cranfield

This guide gives an overview of some of the diverse areas of research we undertake that contribute to national security and how this aligns with the Government's Counter Terrorism Strategy CONTEST pillars.

Prevent

Pursue

Protect

Prepare

We breakdown each pillar to show how we're supporting the Government's strategy and how you can support us to do so too.

"Cranfield is well known for its pre-eminent defence capability, as such our security offering sometimes goes unnoticed. For decades Cranfield University's subject matter expertise, portfolio, customer relationships, specialist facilities and security cleared staff have been working closely across all related elements of the security sphere to reduce the risk to the UK and its citizens and interests overseas from terrorism, so that people can go about their lives freely and with confidence.

This brochure aims to demonstrate how our diverse areas of work address National Security concerns across all sectors of our [Critical National] infrastructure and services."

Dr Simon M Harwood,
Theme Director, Defence and Security and Co-chair of Academic RISC



Prevent

The purpose of **Prevent** is to stop people from becoming terrorists or supporting terrorism.

Pioneering research

Prison radicalisation

In recent years, the role of prisons in countering violent extremism has received growing attention. With prisons often viewed as 'hotbeds' of radicalisation, our research is examining the challenges and opportunities that arise with the presence of terrorism-related offenders within prison systems, including:

- understanding the risks and dynamics behind prisoner radicalisation,
- how risk assessment can be carried out,
- what management strategies are appropriate, critical issues around rehabilitation and reintegration.





Future of terrorism

A current project, within a wider series that's exploring similar issues, is being carried out in connection with Pool Re, the UK's leading terrorism reinsurer, to assess and model the major drivers of terrorist conflicts and what impact this will have in the coming decades.

The study is focused on better understanding the roles that emerging factors like climate change, population growth and immigration can play in driving future terrorism. Tied into this, the research is also exploring what potential policy initiatives and other measures can be taken to mitigate the risks and impact of terrorism in the future.

Understanding landscape change in support of opium monitoring in Afghanistan

The United Nations Office on Drugs and Crime estimates opium poppy cultivation in Afghanistan fell by 33% in 2018, but was the second highest ever recorded (263,000 ha). The heroin produced causes drug addiction, drug related crime and funds terrorism globally.

The spatial distribution of opium cultivation is constantly evolving due to varying environmental, social and economic pressures. The volume and variety of Earth observation data provides opportunities for assessing the agricultural dynamics associated with opium poppy to be extracted from legacy time-series datasets across Afghanistan.

The aim of this project is to derive information about seasonal and annual changes in opium poppy cultivation using Earth observation big data analytics. This project will also take advantage of emerging cloud technologies for timely image processing of associated vegetation dynamics.

“Cranfield University devised and applied an integrated remote-sensing approach to provide critical information on cereal and poppy cultivation and poppy eradication. The results and capacity building activities influenced international policy and counter-narcotics actions in Afghanistan. By applying the latest AI and machine learning techniques to satellite images of poppy growing areas, information is gathered faster, more accurately and with less reliance on ground survey – critical as field surveyors often work against a background of insecurity, coercion and corruption.”

Dr Toby Waine,
Senior Lecturer in Applied Remote Sensing



Pursue

The purpose of **Pursue** is to stop terrorist attacks by detecting, prosecuting and otherwise disrupting those who plot to carry out attacks against the UK or its interests overseas.

Pioneering research

Sifting through the ashes: Amazon Fire TV Stick acquisition and analysis (Digital Forensics)

The business for internet of things (IoT) is ever-growing, with new devices continually populating the market and technology becoming part and parcel of modern life. The increase of smart technology within our professional and personal lives has led to a great need for forensic investigation of such devices.

Our research analysed the popular Amazon Fire TV Stick in a forensically sound manner, meaning no alterations to data occurred and all was kept within ACPO guidelines. By populating the Fire TV Stick with data to understand the full capabilities of the device, we also created and were able to capture a relevant dataset, extracting this through removal of flash memory sticks to view the physical forensic image. The resulting image was analysed using a variety of digital forensic software to establish whether there are any artefacts stored on the device and to assess the forensic relevance of those artefacts.

“Forensic analysis of the Amazon Fire Stick is able to show information that may relate to criminal activity, such as viewing of illegal material, or communication data. It can also serve as an alibi by providing information about user activity on the device such as which apps were loaded, how long they were accessed for and what was done on them.

The chip-off method developed to obtain the data can also be generalised to other IoT devices to enable data to be extracted from many potential sources.

The research was part of a series of ongoing work on extracting data from IoT devices about how people have interacted with them.”

Dr Sarah Morris,
Head of Digital Forensics Unit Research Group



Human vulnerabilities in the face of cognitive hacking: an analytical process method

Cognitive hacking, through the manipulation of online content, intends to influence individual and group decision-making and subsequent behaviours for social, political or financial gain. The increasing research and understanding into human cognitive vulnerabilities has inevitably increased exploitation of cognitive hacking of individuals thought processes. This is why a theoretical model is being developed which maps information validity and context credibility features of online content to human cognitive vulnerabilities.

The model will be operationalised through the generation of a novel analytical process method, designed to support defence and/or security analysts in compartmentalising features of online content that may be exploiting cognitive vulnerabilities. This will enable the interpretation of nuanced verbal and non-verbal content and the identification of potential threats that machine algorithms cannot detect. It will also inform the prioritisation of counter-strategies, where required, for neutralising threats identified. The research is funded by the Defence Science and Technology Laboratory (DSTL) through the Defence and Security Accelerator (DASA) Phase 1 Behavioural Analytics Themed Competition.

Protect

The purpose of **Protect** is to strengthen protection against a terrorist attack in the UK or against its interests overseas, reducing vulnerability. The work focuses on border security, the transport system, national infrastructure and public places - initially recognising the threats to identify the measures to reduce risks.

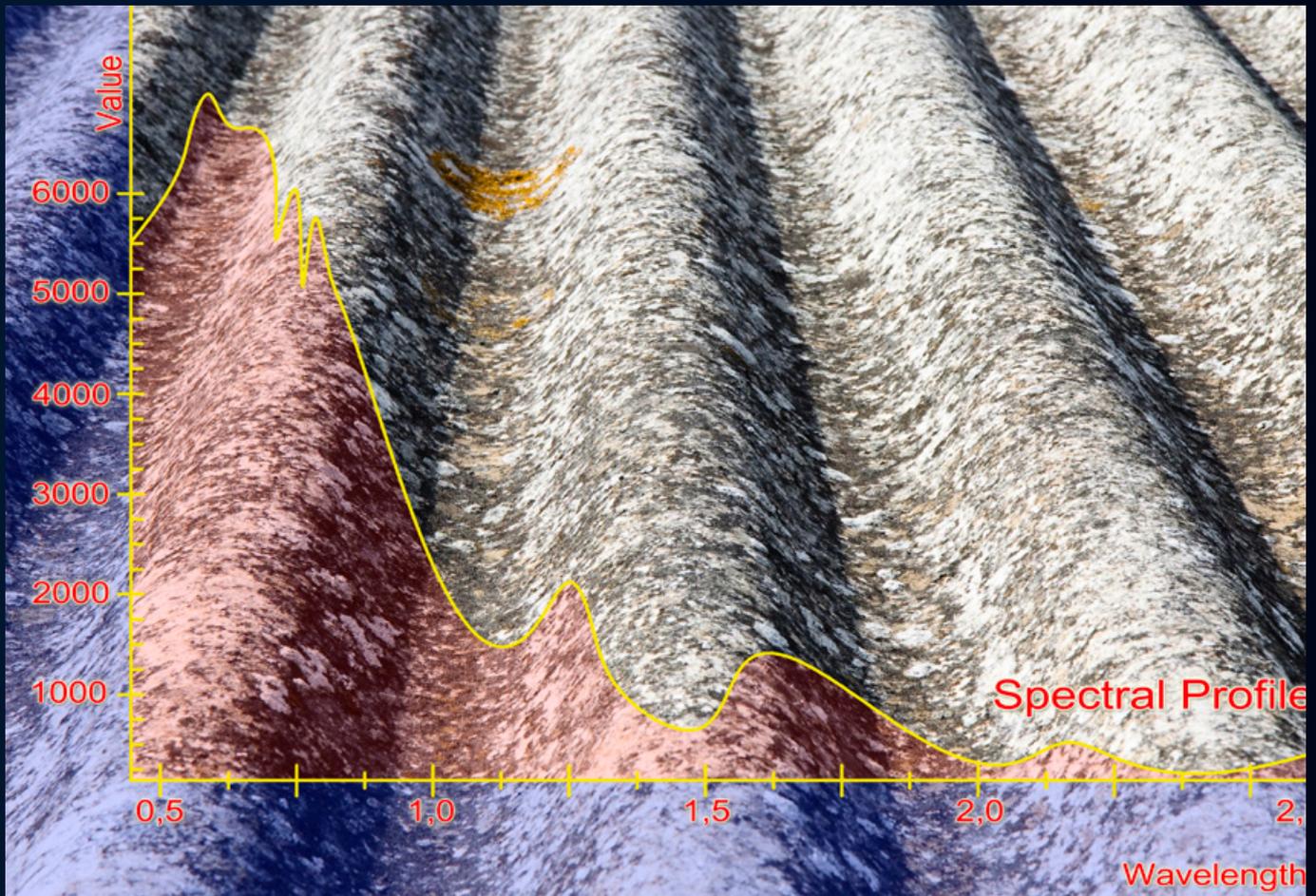
Pioneering research

Using X-rays to instantly identify illegal substances at airports

A joint venture being pioneered by Cranfield and Nottingham Trent University is investigating the use of X-ray signatures to identify illicit items such as drugs and explosives at airports. Halo, a new generation X-ray security scanner, will, for the first time, be able to quickly and precisely identify the material of any suspicious objects. It means weapons, explosives, contraband drugs and even illegal trade items such as ivory could be recognised in milliseconds.

The system will use scattered X-ray signals to identify materials via their unique signatures or chemical 'fingerprint', allowing items to be quickly and easily identified. Three-dimensional material specific images will also be produced to map the position of objects within luggage. Initially funded by a \$4.4 million grant from the US Department for Homeland Security, in June 2019 Halo was awarded further Homeland Security funding of \$1.6 million to secure the development and implementation of X-ray imagery of luggage.





Identifying potential terrorists through stress-levels

Hyperspectral imaging (HSI) is a technique that combines imaging and spectroscopy to extract detailed information from a specific scene - information unable to be acquired through human analysis alone. The discriminative capability in HSI allows the detection of a single pixel or even a single unresolved subpixel of a target. This is achieved through cross-checking the obtained spectra with known, unique spectral fingerprints to detect and identify chemical compositions, materials, liquids, activities or events attached to a precise location in a scene.

The HSI technique also has the ability to distinguish would-be terrorist suspects or extremely mentally stressed individuals from people with ordinary levels of stress. This is identified via the blood oxygenation variations over a person's facial region which can be sensed without direct contact of the subject.

Unlike the conventional machine vision technology which analyses broadband RGB images for target detections, HSI makes use of high spectral resolution images to allow highly camouflaged targets to be discriminated. The target discrimination abilities in HSI has been shown to be orders of magnitude more sensitive than that of the conventional technique. Subtle regional changes of blood oxygenation (SPO2) in the facial part of the subject can readily be diagnosed and the degree of stress can be quantified via precalibrated SPO2 data. Preliminary results obtained from ~100 volunteers have shown over 80% accuracy for the positive detections of medium to high levels of stress.

Hardware Trojan detection and prevention in integrated circuits

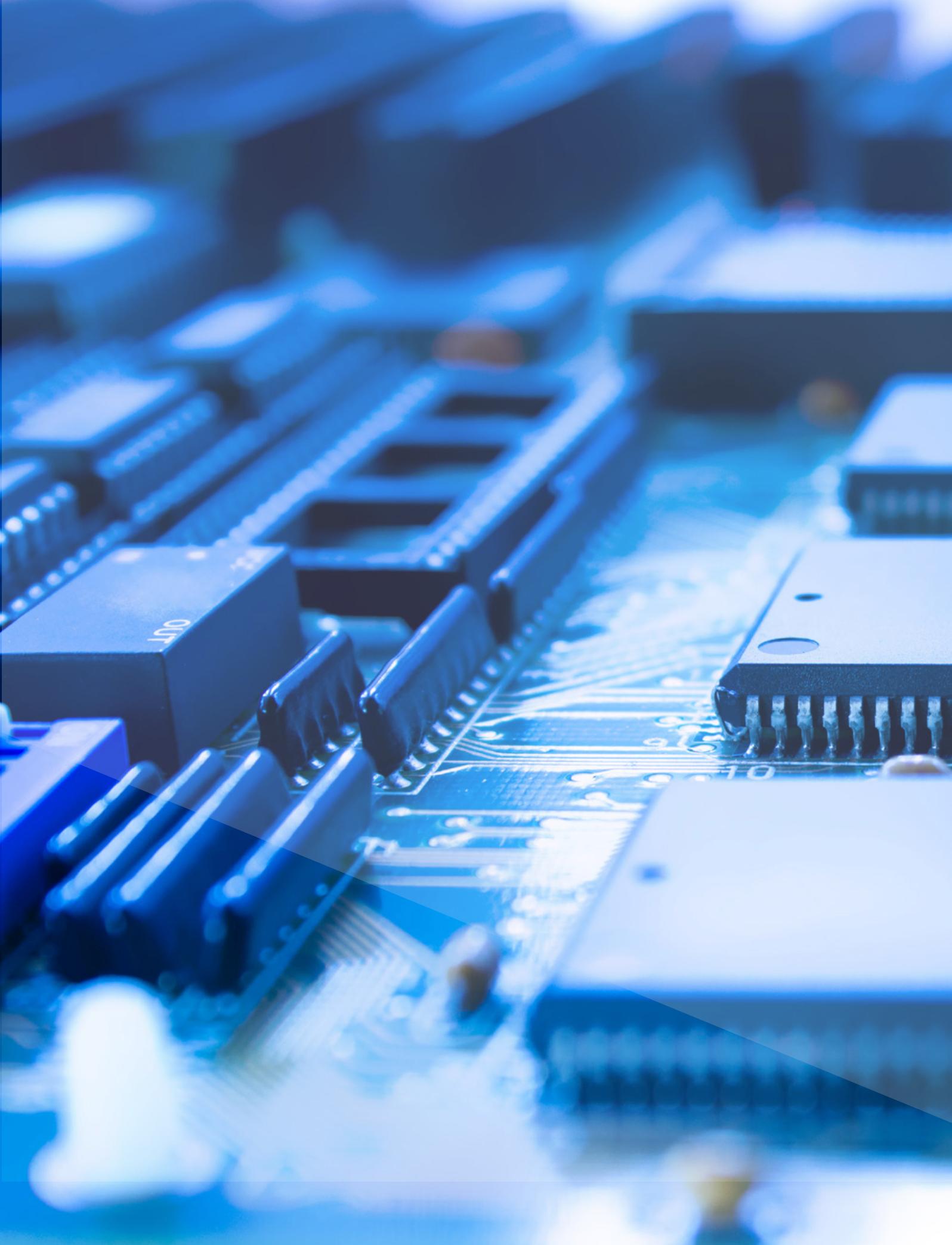
Embedded electronics are the weakest part of any smart system concerning security, privacy and trust. The problem occurs when the malicious electronic circuitry residing at the micro-architectural level of hardware exploits the side-channel information in addition to the exploitations of modern day software vulnerabilities. To detect and mitigate this type of threat we need to measure the performance of the device, develop electronic fingerprints and digital signatures, and upgrade the security when new threats are emerging.

Our research is aimed at developing design for prognostics and security in Field Programmable Gate Arrays (FPGAs). This uses kernel-based machine learning and path-delay based hardware, Trojan detection and ageing methods. The FPGAs are subjected to highly accelerated stress tests. This entails comprising the thermal and power cycling as well as stressing, all within a dedicated thermal chamber. From this healthy and hardware Trojan infected parameters are captured, collated and analysed for optimised design for prognostics and security.

“Military networks need a full spectrum military defence – existing civilian security approaches are simply not up to this task. Deception is all about creating errors in how our adversaries make sense of their world. It is about getting them to act in ways that suit our purposes, not theirs.

The use of cyber deception has to be adopted with rigorous intellectual professionalism.”

Darren Lawrence,
Director of the National Cyber Deception Laboratory



Prepare

The purpose of **Prepare** is to mitigate the impact of a terrorist attack where that attack cannot be stopped. This includes work to bring a terrorist attack to an end and to increase the UK's resilience so the country can recover from its aftermath.

Pioneering research

Organisational resilience

The Leading Complex Change Group helps organisations to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper. In today's volatile, uncertain and complex world, crises that threaten the reputation and operations of an organisation are becoming an everyday occurrence.

Our approach addresses the shortcomings of traditional risk management and shifts thinking beyond operational resilience, crisis and continuity by helping organisations move beyond the compliance-based, prescriptive rationale and logic that they have in the past been able to rely on. We recommend organisations use a strategic, performance-based approach to cope with the rapidly changing landscapes in which they are now operating. We help organisations embed resilience into their culture and core business operations to safeguard their financial performance and develop a robust company strategy; one that is strategic and proactive not tactical and reactive, while ensuring full organisational engagement from executive-level down, all playing an active role in setting the resilience agenda.





Computational blast-loading tool

Pool Re, a mutual reinsurer which underwrites over £2 trillion of exposure to terrorism risk in the UK, needs to undertake catastrophic and unconventional terrorism loss assessment so as to improve the UK's economic resilience. The aim of this work was to develop simulations on explosive blast in a complex city centre.

Ongoing work continues to support Pool Re's efforts to model the potential impact of a range of terrorist attacks, including those involving the use of chemical, biological and radiological weapons.

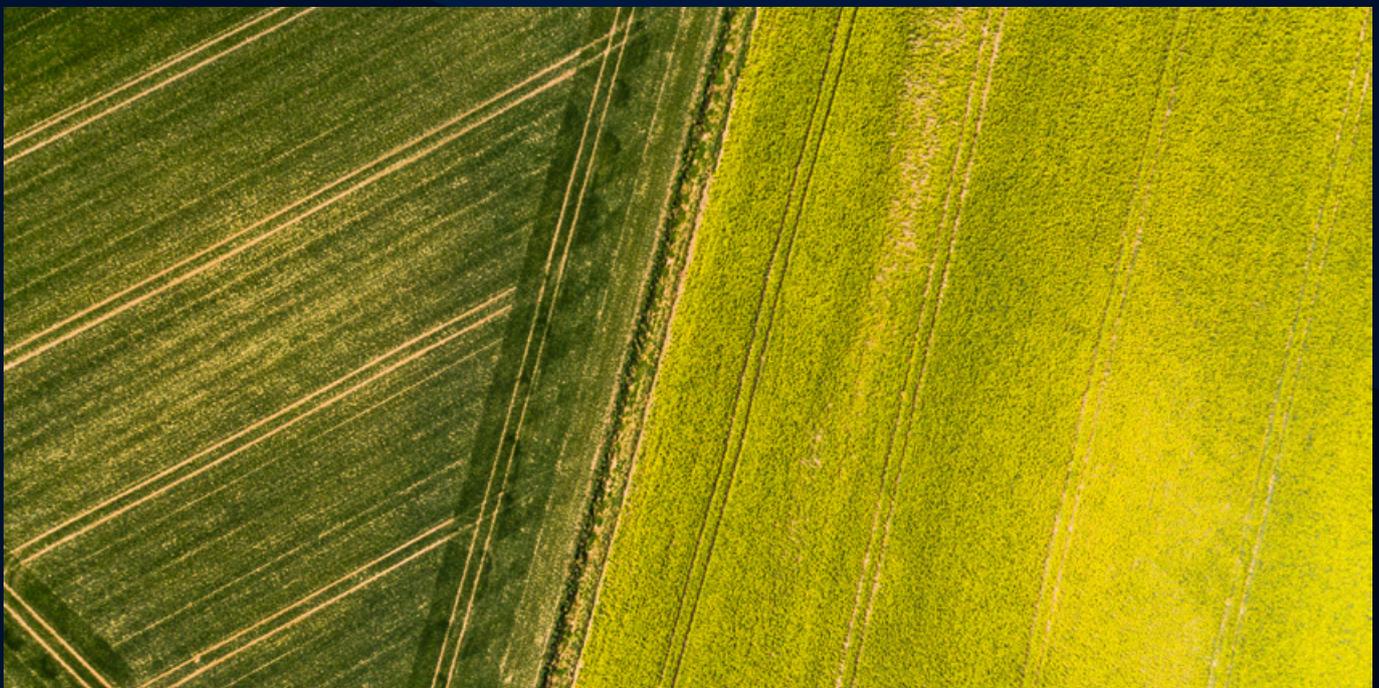
“We are fortunate to be able to work with Cranfield University whose leading academic experience in security issues is crucial in the model's development.”

Julian Enozi,
Chief Executive, Pool Re

Food Security

Closing the gap between food production, supply and reducing waste is an essential component of improving food security. However, the ability of the world food system to achieve this is under chronic pressure from numerous factors including conflict and terrorism.

Cranfield are exploring a range of mitigating factors in improving food security. For example, Agri-informatics, the increased use of big data analysis, and falling costs of sensors and data collection approaches - such as the use of satellite imagery - means we will have better information on agricultural practices, water and soil management. There will also be more opportunities for introducing technological solutions, data sharing and insights among farmers by national governments as well as across food supply chains in order to be able to pre-empt and react to market disruptions.



“History tells us that food insecurity and food shocks can lead to conflict and disruption. For 50 years, Cranfield has been contributing to enhancing natural capital and ensuring that global food systems are more resilient for the future. We believe that both immediate and long-term environmental pressures and threats to food security can be alleviated through technological innovation, data sharing and risk management.”

Professor Leon Terry,
Director of Environment and Agrifood



 @cranfielduni

 /cranfielduni

 Cranfielduni

 Cranfield University

For further information, please contact:

Dr Simon Harwood
Director of Defence and Security
T: +44 (0)1234 758175
E: s.harwood@cranfield.ac.uk

www.cranfield.ac.uk