Preface

Sir Keith O’Nions
Former President & Rector of Imperial College London

Ten years ago the security challenges facing individuals, the wider population and our digital and physical infrastructures were receiving increasing attention. The UK government was developing a comprehensive National Security Framework and it was clear that universities with their capacity for interdisciplinary research had a much bigger role to play.

Imperial had recognised this opportunity and in mid-2008 I was invited, following more than eight years in government roles, to join the College and establish a security institute. I was delighted to accept. The formation of the Institute of Security Science and Technology thus became Imperial’s response to this need and opportunity. The Institute’s initial strategy was straightforward – to become a portal for accessing world-leading interdisciplinary research and also a trusted interface for Government and industry.

From its inception ISST was an interdisciplinary institute drawing participation and interest from across Imperial’s faculties, and building cross-cutting programmes. It drew on one of Imperial’s great and enduring strengths – a willingness of researchers to cross the boundaries of departments and faculties and bring their talents to bear on new opportunities and challenges. It also developed a series of international connections from the outset using both the networks of its founding members and the help and generosity of its board of advisors.

Today, a decade on, the need for multidisciplinary research in security science and technology within universities is as great as ever. It is a pleasure to see ISST continuing to grow and flourish with increasingly ambitious programmes in both research and teaching.

Furthermore it has become a tribute to the role that universities such as Imperial College are able to play in addressing major societal challenges.

Introduction to the ISST

The Institute for Security Science and Technology is Imperial College London’s hub for security research and engagement.

We coordinate interdisciplinary research in security across Imperial College London. We further act as a security science, technology and innovation interface for academia, government and industry.

The Institute was founded in 2008 as one of Imperial College’s Global Challenge Institutes. Each Institute has been formed to promote interdisciplinary working to meet the greatest challenges faced by society, to become a focal point for multidisciplinary activities and an interface to stakeholders, and to formulate and apply new areas of knowledge and technology solutions, as well as providing independent scientific advice.

Our vision

Geo-political uncertainties, climate change and changing cyber and physical attack methods give rise to a constantly evolving security landscape. We envisage, design and coordinate the application of science and technology to answer the grand security challenges raised.
Some words from our Co-Directors and Deputy Director

Professor Chris Hankin  
Co-Director, ISST  
Professor of Computing Science, Department of Computing

The academic year of 2008/2009 was something of a watershed for me; it was the last time that I had sabbatical leave. I had just stepped down as Deputy Principal of the Faculty of Engineering (Vice Dean in today’s currency) and I was preparing myself for return to the Department of Computing as a full-time academic. I was aware that Sir Keith, followed by Andrew Burton, had joined the College to establish a new Institute and, since my research had moved towards cyber security, I enthusiastically engaged with the new enterprise. Keith and Andrew encouraged me to attend my first EPSRC sandpit, about Detecting Acts of Terrorism, and that led to me becoming Principal Investigator of the Making Sense project. Making Sense was a multi-disciplinary project using visual analytics to support analysts in investigating acts of terrorism, and I led a team from nine universities.

Up until that point, my research had focussed on an area known as “Language-based Security”. This involved the analysis of computer programs to understand the way in which they processed data. The work built on my expertise in static analysis of computer programs to understand the way in which they processed data. The work built on my expertise in static analysis. Language-based security aimed to ensure that “secret” information was not leaked to the outside world. Making Sense opened a new area of work for me; at Imperial we concentrated on the analysis of data and, surprisingly, some of the analysis techniques were not so different from my earlier work.

Soon after I finished my sabbatical, Sir Keith was elevated to the position of Rector and invited me to take over as Director of ISST, which I did in January 2010. The last eight years have been an exciting mix of policy work, building research programmes in ISST and supporting security researchers across the College. The two main research programmes to date have been in cyber security and data analytics. ISST holds the GCHQ Academic Centre of Excellence in Cyber Security Research (ACE-CSR) status for the College, has led our involvement in the Research Hub for security, privacy and trust in the Internet-of-Things (PETRAS) and has been involved in two of the national cyber security research institutes, leading one of them The Research Institute in Trustworthy Inter-connected Cyber-Physical Systems (RITICS). The data analytics programme has conducted a variety of projects for UK and overseas governments and has recently specialised in social media analytics. The policy work has contributed to important publications across a number of UK Government Departments.

At this point in the Institute’s history, there are a number of exciting new opportunities on the horizon. The two that are likely to have the most impact are the new Centre for Financial Engineering and Artificial Intelligence and our plans to launch education programmes at both the doctoral and Masters levels. We are also beginning to collaborate much more actively with the other Imperial College Institutes, particularly with medical colleagues.

Unfortunately, the world is no more secure now than it was 10 years ago – in fact, it could be argued that political instability and the effects of climate change and other factors are making it less secure. The security threat may change but the Imperial academic community is well-placed to contribute to solutions to whatever problems may arise in future. I expect the next ten years to be an even more successful period for ISST.

Professor Bill Lee  
Co-Director, ISST  
Professor in Ceramic Science and Engineering, Department of Materials

My association with the ISST began when I joined as Co-Director in July 2017, to work with Chris Hankin on a remit to expand the portfolio of research and develop our training programmes.

For the former, Jane Lac our outstanding Manager, has helped us make appointments in key areas including Laurence Williams FREng OBE in nuclear security, Washington Ochieng FREng in transport security and PJ Beaghton in finance security. Sir Keith O’Nions also joined our team as a Distinguished Research Fellow. With Jane’s assistance we’ve also initiated an ISST Champion’s Group with a representative from each Department (with knowledge of security issues), meeting monthly to discuss potential collaborations across College.

In the training domain and working with the whole ISST team, Jane and Bill Proud (Associate Director) have developed the MSc Security and Resilience: Science and Technology which will start its first cohort of students in October 2019. We plan to make an Introduction to Security Science course available for undergraduates.

In addition, initiatives to support cohorts of PhD students across the broad field of security science, in collaboration with other UK universities and supported by Government and industry, are planned.

Largely through Deeph Chana we have been working closely with David Gann CBE (Imperial’s Vice-President for Innovation) on developments at Imperial’s White City campus. We’ve recently seen Airbus take space at White City, as well as DSTL’s Defence and Security Accelerator (DASA), and this along with all these initiatives makes the future exciting, and busy, for us! Finally, Max Swinscow-Hall, our Communications and Outreach Officer, will ensure you are aware of all these developments.
In 2012 I joined the ISST to help develop and grow its programme, and connect it to stakeholders outside of academia. This was a welcomed step following various research positions in both academia and industry, as well as security-relevant roles in UK Government.

Jumping back to September 11th, 2001, over a decade prior to me joining ISST, I was in the final days of writing up my physics PhD thesis when the terrorist attacks in New York took place. The weeks and months that followed were filled with discussions on everything from geopolitics, to the resilience of cities and buildings, and the measures needed to prevent airlines from being hijacked. It seemed to me that many of the emerging debates could be better informed by an improved consideration of evidence. I became interested in how society copes with low probability, high consequence events, and the role science plays in shaping the politics around them.

For the next few years I worked as a post-doctoral researcher, getting involved with a range of research projects. All the while my interest in science and policymaking grew, and I became increasingly focussed on the particularly thorny problems in security.

Shortly after the London Tube bombings in 2005, I took a role in the UK Government working within the team responsible for setting national security policy for transport. Over the next five years in the civil service, I ended up leading a large programme of science and technology projects, and coordinating the work of other government departments through a role in the Home Office. My other key responsibilities included briefing Secretaries of State in the aftermath of national incidents and developing international partnerships.

In 2010 I decided to leave the civil service and transition to the private sector as I wanted to connect with technology development more directly. I joined an exciting quantum cascade laser technology company in Scotland and then got involved in numerous entrepreneurial style STEM projects ranging from trace detection, crowd analysis, cyber security, autonomous vehicles, material science and infrastructure security and resilience.

Since taking up the Deputy Director role at ISST in 2012, I co-founded the Institute’s ongoing activity in the cyber security of industrial control systems, RITICS, and have undertaken research on the vulnerability and protection of cyber-physical systems using machine-learning. Working closely with Prof PJ Beaghton, I am currently working on exciting initiatives to develop the College’s engagement with the finance industry and am also working with Prof W Ochieng on developing research projects on the security of future mobility. I believe that bringing academia closer to industry and government is a solid model for innovation and is key for developing the UK’s future technology economy. The ISST is playing its part through initiatives such as its partnership with the MoD’s Defence and Security Accelerator (DASA), currently located at our new White City campus, and through my involvement with the Business School. I’m looking forward to working towards making this innovation model a reality at Imperial.
Some words from our Associate Directors

Professor Emil Lupu
Associate Director, ISST
Professor Computer Systems, Department of Computing

I joined ISST in 2011 as one of its first Associate Directors. The security and resilience challenges, the inter-disciplinarity and the opportunity to contribute to Imperial’s broader activities motivated me most. I was also aiming to do something new, and venture beyond the traditional academic concerns.

The first call for recognition of Academic Centres of Excellence in Cyber Security Research (ACE-CSR) offered the first opportunity. I led Imperial’s successful application, which brought together 15 academics across 4 College departments, described their collective achievements and characterised our specificity and strengths in Engineering Secure Software System, including major themes in System Analysis and Verification, and Operational Systems and Information Assurance. Our recognition as an ACE-CSR proved an important milestone for everybody involved. It gave us an opportunity to grow, to establish new partnerships to obtain further funding for PhD students and to engage in new collaborations. Even our students went on to win the Inter-ACE capture the flag competition in 2017.

The overall research in cyber security strengthened and by 2016, when our ACE-CSR status was renewed, our application included 25 academics and showed an increase in research funding exceeding 42%. Our ranks are still growing and many new exciting projects are being developed. See the website for more information: http://www.imperial.ac.uk/cyber-security

John Hassard PhD
Associate Director, ISST
Reader in Physics, Department of Physics

I played a minor role in setting up the ISST and was then appointed by Sir Keith O’Nions as the first Associate Director, with special remit to guide CBRNE research.

Within a year, I was seconded to the State of Qatar, on an Imperial College-led initiative, namely to establish biomedical and biotechnological research facilities within the Qatar Science and Technology Park, sponsored by Her Royal Highness Sheikh Moazah. Whilst this reduced my contributions to the ISST, I remained engaged with security science and global issues of security.

I returned to the UK, and full-time Imperial College operations, in 2016, and subsequently resumed my Associate Directorship. While I am still extremely involved with and concerned by CBRNE affairs, I have refocused somewhat to look at a more fundamental problem; the relationship between climate change, societal unrest, mass migrations, their implications for the cooler North, and the use of unconventional warfare agents by both national and subnational groups.

Leading the ACE-CSR has also marked a personal milestone. Somewhat shifting my own research area, I have established a new research group in Resilient Information Systems Security, which is now pursuing a range of research activities in systems security, risk assessment, cyber-physical security, attribution, adversarial machine learning and resilience (http://rissgroup.org).

Another important development was Imperial’s participation in the PETRAS IoT Research Hub – Cyber security of the Internet of Things where the College contributed to over 12 streams and project activities totalling over £1.7M funding. These involved academics from four Departments across a broad range of areas ranging from healthcare to transport and tracking works of art, as well as more traditional blockchain and risk management activities. On behalf of the Institute, I had the opportunity to not only lead Imperial’s participation in the Hub but also to act as Deputy Director of the Hub and contribute to its broader activities and outcomes.

The Internet of Things is only one of the terms representing the merger between the digital, the physical and the social spaces, which will continue in the years to come. It will enable us to leverage progress in data analytics and AI to improve efficiency, personalisation and quality of life. It touches all industry sectors from healthcare to manufacturing, from agriculture to the creative arts. Yet at the same time this merger brings new security challenges and opportunities which the College, with its science and technology focus is in a good position to address.

Outside of wealthy enclaves, the Middle East and North Africa region will be largely uninhabitable in any reasonable Business As Usual scenario within a 20 to 70 year timescale. This could result in over 300 million people seeking to relocate. If we look at the Central Africa region, we can double that figure. IPCC targets of a maximum 1.5°C global average temperature rise are now extremely unlikely to be met. A 2°C rise in temperature, also likely to be very optimistic, will disproportionately affect the Middle East and North Africa regions. The problem is highly cross disciplinary, and the solution must also draw on many areas of expertise.

My main interests include establishment of new technologies which contribute to carbon mitigation, and in particular the so-called Solar Cyclone Tower, which has many implications for security not least the potential for copious amounts of water produced with little or no environmental impact. I am also working on strategies and technologies for hydrocarbon substitution, and advanced recycling technologies. And clearly, the threat of CBRNE and other lower-technology threats such as vehicles, has not gone away.
My first interaction with the ISST occurred on my first day in Imperial – 1st October 2009. I had been promised an office would be ready for me as Reader in Shock Physics and Technical Director of the Institute of Shock Physics (ISP). When I arrived I discovered that my office walls on the 4th floor of the Royal School of Mines, had not been completed. So I decided to sit in the large open plan office dedicated to the ISP, adjacent to the ISST office. Furthermore, I seemed to vaguely recognise one of the occupants, Andrew Burton and also the name ‘K O’Nions’ on one of the doors. It was soon clear that I had met Andrew several times while he was in DSTL and I had met Sir Keith during his time as Chief Scientific Advisor at the MoD.

A shared interest, with Andrew, in energetic materials (explosives) and the effect of their use rapidly led onto a more wide-ranging discussion about security, threats, mitigation and outcomes. This is probably when I first said ‘Guns, bombs, knives and sharp sticks’, a phrase which has followed me around in my interactions with ISST ever since.

It was clear that some aspects of my research – home-made explosives and their defeat, trigger mechanisms and material supply – overlapped strongly with some ISST interests. Soon I found myself regularly invited to ISST meetings with a range of representatives from the USA and other nations. As well as ISST, I also found myself sought out by ImperialBlast, who were the precursor to the current Royal British Legion Centre for Blast Injury Studies at Imperial College London (CBIS). Their interest was in high-speed diagnostics and loading platforms to simulate the effect on soft biological materials of explosive loading.

These two initial interactions with ISST and CBIS have defined a significant part of my research in Imperial College London. My interest in explosives and ballistics as areas of applied science and technology have been augmented to include aspects of security and resilience (ISST) as well as medical outcomes and rehabilitation (CBIS).

I was delighted when Professor Chris Hankin asked me to become an Associate Director of the ISST in 2013. This allowed me, via a formal role, to devote long-term, strategic time to the ISST.

The result of this is the setting up of an MSc course in Security and Resilience to address a wide – sweep of Science and Technology approaches in this area. It has been wonderful to see the ISST grow from its original scope of being a ‘portal for defence related areas in Imperial’ to becoming a well-recognised centre for research which is both cross-department and cross-faculty.

I have met many interesting and stimulating people through the ISST. Also, I have been given the opportunity to say ‘Guns, bombs…..’ on many technically relevant occasions.

Throughout my career in trading and fund management, I was involved in all aspects of high-volume electronic/automated trading, ranging from statistical/ mathematical modelling to algorithmic order generation and two-way high-speed interaction with multiple trading venues. I was thus motivated to engage with government, regulators, and law enforcement to leverage this experience and help identify and defend against security threats to the financial markets. In parallel, and more recently, I have become Associate Director of the ISST and Professor of Practice in the Department of Computing, focusing on “FinSec”, i.e. security of financial systems, processes, and institutions. I am particularly interested in studying the vulnerabilities of trading exchanges, banks, and brokerage houses to both external and internal attacks and to accidental generation of large number of electronic orders, that can result in contagion across exchanges, products and regions.

Another area that interests me is researching the increasing use of non-cash financial instruments for money laundering and other illegal activities. The growing sophistication of the complex structures implemented by criminals makes it almost impossible to identify and reverse-engineer them without the application of algorithmic forensic analysis. The combination of financial knowhow in securities and derivatives with anomaly detection algorithms deploying machine learning/AI techniques can be put to good use in this arms race between investigators and criminals.

Working in a cross-disciplinary institute, with connections and affiliations to most departments and faculties at Imperial College, and with a cross-industry approach to all security, whether cyber or physical, has been very exciting for me, especially given the plethora of common features in the security threats facing financial institutions and other industries (e.g. source, methods of attack, detection, prevention, etc.).

The other major advantage of working in London in a top STEM university with a world-class business school at this point in time is the transformation and disruption of the banking industry caused by FinTech SMEs. Drawing from my banking and hedge fund management background and my FinSec expertise, I have co-led the establishment of an Imperial College Network of Excellence in FinTech, with participation of 50 academics representing many departments from all of the faculties. This Network, although only in its first year, has already been successful in not only bringing together Imperial College academics from different disciplines, but in energising interaction with banks, hedge funds, and FinTech start-ups.
Professor Nick Jennings is Vice Provost for Research and Enterprise at Imperial College London. In his role he has oversight of the six global institutes, including ISST, and has long been a champion of their work.

Nick’s own research has many applications in security, and in 2010 he was appointed the first ever Chief Scientific Advisor (CSA) to the UK Government on national security.

Max Swinscow-Hall, the ISST’s communications and engagement officer, caught up with Nick to learn more about his experiences and what the future holds for national security and the ISST.
What are your research areas, and how are these linked to security?
My research expertise is broadly in artificial intelligence, autonomous systems, cyber security and agent-based computing. My research touches on security but has not generally been security-specific.
For example, some of my research has looked at disaster response. When responding to a disaster there is a lot of information received by the response team, who need to be able to deploy resources to best resolve the issues. This is not that different to the requirements of a response team to a national security incident, such as a cyber attack or a chemical attack.

What is the general role of a Chief Scientific Advisor in national security and was your research expertise particularly suitable?
In 2010 I was appointed Chief Scientific Advisor to the UK Government for national security. Whilst science and technology has long played a role in national security, a CSA post had never existed before.
As CSA my primary responsibility was to provide advice to the national security department on the science and technology relevant to national security, and to develop new research capabilities. To do this you need to traverse all science, social science, technology and engineering disciplines, and so having broad expertise helps.
For national security, having a background of computer science was particularly useful. During my tenure cyber security became a big and serious issue. I don’t think it’s a coincidence that my successor as CSA, Professor Anthony Finkelstein, also has a background in computer science.

What were some of the biggest challenges and achievements?
One of my proudest achievements from my time as CSA was increasing the openness of Government national security agencies to outside collaborations and partnerships. These collaborations are highly valuable to solving the grand challenges, as Government doesn’t have the time or resources to do so alone.
Open calls and collaborations between academia, industry and the security agencies are now commonplace, but this was not the case when I started as CSA.

What role should universities play in national security?
The short answer is a lot. I would break it down into three main areas where universities can and should play a role.
First, research. Government departments are not set up for long-term, sustained research, but this is what universities do best.
Second, talent. Universities can help train and build interest in talented people to get them involved in national security. The ISST’s new MSc Security and Resilience course is a great example of this.
Cyber security has emerged as a major security theme over the last 10-15 years, as society has become increasingly reliant on interconnected computers to run systems. This is an area where ISST has developed significant expertise, and lead local, national and international research programmes.

Academic Centre of Excellence in Cyber Security Research (ACE-CSR)
Imperial College London, led by the Institute for Security Science and Technology, was among the first UK universities to be recognised as an Academic Centre of Excellence in Cyber Security Research by the UK’s Government Communication Headquarters (GCHQ). The ACE-CSR accreditation officially recognises a critical mass of cyber security expertise and world-leading research in cyber security.

In 2017, Imperial College’s ACE-CSR accreditation was officially renewed.

RITICS
The Research Institute in Trustworthy Inter-connected Cyber-Physical Systems is one of the UK’s three national cyber security institutes. It was founded in 2014 by Professor Chris Hankin (ISST Co-Director) and Dr Deeph Chana (ISST Deputy Director), and has been coordinated by ISST since, with Chris Hankin serving as the Director. Funding comes from the Engineering and Physical Sciences Research Council (EPSRC) and the National Cyber Security Centre (NCSC).

The prestigious research programme started off as five academically led, industry linked cyber security projects, addressing threats to industrial control systems and the business risks these pose. The programme managed to leverage over £40mm in additional funding, published 35 research papers, and engaged over 20 further industry and academic partners, kick-starting a national community.

In 2018, additional funding was secured from EPSRC and NCSC to continue building on this success. The current programme has expanded its scope to focus on the cyber security of cyber-physical systems, and is pushing the further development of a community of interest, bringing in more academic and industry partners.

PETRAS Internet of Things Research Hub
Imperial College London is part of the PETRAS Internet of Things Research Hub, led by Professor Emil Lupu (Department of Computing, and ISST Associate Director) on behalf of the College. PETRAS is a consortium of nine leading UK universities, led by UCL, which work together to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security. Funding for the Hub totals approximately £43 million, including a £9.8 million grant from the Engineering and Physical Sciences Research Council (EPSRC), and partner contributions.

www.petrashub.org

Data Analytics has become hugely important, impacting many, if not all industries. Over the years we have used our expertise to apply data analytics to security issues, including cyber security, biosecurity, and counter terrorism.

Making Sense
Making Sense was funded by EPSRC and Centre for the Protection of National Infrastructure (CPNI) from 2010 to 2013. The key challenge that this project addressed was the analysis and visualization of multiple sources of multi-modal data that may be partial, unreliable and contradictory.

To tackle this we developed an interactive visualization-based decision support assistant which collects data, fuses it, analyses it and visualizes the results in a way which can be shared by analysts.

The underlying analysis tools we developed during this project can be adopted for different circumstances. This led us to secure two grants from the Defence Science and Technology Laboratory, one of which is highlighted below.

Defender / Sentinel
These projects have focussed on applying tools of data analytics and machine learning to detecting disease outbreaks.

In our most recent project, Sentinel, we use social media (e.g. Twitter) as a public data feed to track people mentioning symptoms of some well-known diseases (e.g. flu, malaria, salmonella, etc.) in their tweets. This data is compared with the official data sources from the national health authorities such as the U.S. Center for Disease Control and the UK’s National Health Service.

These reporting authorities have a lag of a few weeks for getting their data from local hospitals, but social media reports are real-time. Our innovative technique aggregates these tweets along with local news in order to build a confidence score that an outbreak reported on social media is genuine. The end goal of this project is to decrease this “reporting gap”, while using more innovative data sources, such as social media, news and crowdsourcing.
Policy work

Informing and influencing policy has been at the heart of the ISST’s remit since its launch. Over the years, the ISST’s Co-Directors, Associate Directors and Affiliates have sat on many advisory boards to Government Departments, presented written and oral evidence to committees, and helped set the national agenda in key security topics. Here are a few recent highlights.

**Future Identities**
Professor Chris Hankin chaired the expert group that oversaw the production of the Future Identities report, from the UK Government Office for Science. The 2013 report was a horizon scan of how technologies will affect views of identity in the UK, over the next 10 years.


**U.S. Department of Energy nuclear weapons clean-up programme**
Professor Bill Lee is one of only two non-American scientists who were invited to join an advisory committee, which will evaluate and advise on the technology used in the clean-up of U.S. nuclear weapons testing sites. The scale of the clean-up programme is enormous and covers many sites, including the one at Nevada, where nuclear weapons were tested underground in the 1950’s and 60’s. It will cost a total of $300 billion U.S. dollars, and take around 50 years to complete.

[www.imperial.ac.uk/news/184508/imperial-professor-advise-300b-us-nuclear](http://www.imperial.ac.uk/news/184508/imperial-professor-advise-300b-us-nuclear)

**Cyber Security Regulation and Incentives Review, UK Government Department for Culture, Media and Sport**
Professor Chris Hankin chaired the senior expert advisory group, which advised the review team, for this 2016 report. The report was produced by the UK Government Department for Culture, Media and Sport, as part of a £1.9 billion strategy to make the UK more cyber secure.


**AI in the UK: ready, willing and able? House of Lords Select Committee on Artificial Intelligence**
The House of Lords appointed this Committee in 2017 to answer key questions on artificial intelligence relating to opportunities and risks for the UK, as well as issues relating to ethics and how it will change people’s lives. Professor Chris Hankin gave oral evidence to the Committee in November 2017 and answered questions relating to the potential for AI to assist in cybersecurity.


**UK Research Institute in Trustworthy Industrial Systems**
RITICS was founded by Dr Deeph Chana and Professor Chris Hankin back in 2014. The two co-founders had successfully raised the profile of the threats to UK industry through cyber-physical systems, shaped the debate on cyber security, spurring key funding agencies to finance the project. This is now one of the UK’s flagship programmes in cyber security research which was extended in 2018 with further funding.

[www.ritics.org](http://www.ritics.org)
Having spent 10 years in the defence government sector I was ready for a change. I applied to the research position at ISST because the topic offered was highly aligned with my experience and interests. I also considered the opportunity to earn a PhD in a STEM topic from a top university as a big plus.

My research addresses predicting strategic national intention from observations of national industrial bases using web-based data. To do this I employ cutting-edge web scraping and machine learning techniques as part of a flexible framework inspired by my experience in capability development and quantitative analysis.

The work has been very stretching, taking me out of my comfort zone and allowing me to gain many valued skills. Now approaching the end of my research, I am in an excellent position for the next step in my career, the PhD having opened up additional opportunities in data science and academia.

Overall my experience has been extremely positive and I am very glad to have taken the leap to becoming a full-time student again.

Ovidiu Serban
Research Associate

My current work at the ISST is in biosecurity and biosurveillance. This is incredibly interesting and challenging, and involves developing new Natural Language Processing and Machine Learning models for syndromic surveillance and health classification. In our most recent project, we use social media (e.g. Twitter) as a real-time public data feed to track people mentioning symptoms of some well-known diseases (e.g. flu, malaria, salmonella, etc.). This data is compared with the official data sources from the national health authorities (e.g. CDC, NHS, etc.), which typically have a lag of a few weeks in collecting data from hospitals.

It is very satisfying to know that your research contribution carries such a high social impact. It’s also great to be able to work with a multidisciplinary team and government agencies, as this helps you understand all the practical aspects of your ideas faster than anywhere else.

Maria Vigliotti
Technical and Business Partner, Gradbase

I worked at the Institute for Security Science and Technology at Imperial College London for about two years. During my time there I had the privilege to carry out ground-breaking work on the use of big data for security purposes. At the time I joined, the Institute was undertaking a push to make research more relevant to industry; this gave me the chance to carry out research driven by industrial and Government stakeholders and provided me with the chance to improve my communication and management stakeholders skills, both which turned out to be very valuable after I left academia.

My relationship with the Institute continued after I left; in fact, when I was writing the UK Railway Cyber Security Strategy, and the participation of an academic partner was needed, I could not think of a better choice than the Institute for Security Science and Technology Institute at Imperial College London.

MSc Security and Resilience: Science and Technology

2019 will mark a new chapter in education at the Institute for Security Science and Technology. October 2019 will see the first cohort of the new MSc Security and Resilience course enter Imperial College.

The course has been developed responding to the skills gap in security and resilience, and the need for STEM graduates with a broad understanding of security and resilience as a subject.

More information can be found at www.imperial.ac.uk/security-institute/education/msc
The Vincent Briscoe Lecture series

Part of our remit as a Global Challenges Institute is to engage with wider society. As part of this, each year since 2009 we have run an annual security science lecture named after Professor Vincent Briscoe. Professor Briscoe was an inorganic chemist at Imperial College London from 1932 to 1954. He is credited with providing the first independent scientific advice to the British Security Service (MI5), in 1915, on the subject of secret German writing.

All of the lectures have been recorded and made available on our website at: www.imperial.ac.uk/security-institute/media/videos/

2010

Science, Technology and Secret Intelligence. Delivered by Christopher Andrew.

MI5’s first official historian, Christopher Andrew, delivered the inaugural Vincent Briscoe annual security lecture. In it he explores the interaction between science, technology and secret intelligence over the last century, from the world wars to the era of transnational terrorism.

2011


Author of the first official history of MI6, Keith Jeffery (Queens University Belfast) investigates the extent to which the profession of intelligence might be described as a science, and also explores the role of science itself in both the working and the targeting of British intelligence operations in peace and war.

2012

Legal and Ethical Boundaries at the Cyber Frontier. Delivered by Michael Chertoff.

Former US Secretary of Homeland Security, Michael Chertoff asks when is a cyber attack a genuine act of war? What is the line between the development of offensive versus defensive cyber capabilities? How can law enforcement most effectively combat cyber crime and cyber terrorism while maintaining civil liberties and privacy?

2013

Modern Terrorism’s Technological Trajectory. Delivered by Bruce Hoffman.

Terrorist success depends not only on an ability to keep one step ahead of the authorities, but also one step ahead of counter-terrorist technology. But curiously, as radical or fanatical as terrorists may be, both politically and ideologically, they are technologically conservative. Bruce Hoffman (Georgetown University) explores this paradox and assesses terrorism’s ongoing technological trajectory.
Jamie Bartlett (Demos) explores dark internet subcultures, hidden encrypted websites and the people behind them. He covers the rise of citizen-led encryption systems, the cryptocurrency bitcoin, the anonymous browser ‘Tor’, online drugs markets, and how extremist groups and criminals use the internet. Jamie explains how this world operates, and what it means for public safety and security.

Former UK Science Minister David Willetts considers ways in which a safe and secure space environment can be sustained and how we must work with international partners and the industrial and academic community to safeguard this ‘global commons’ which is so important to our critical infrastructure.

60 Years of Nuclear Nonproliferation: Who’s The Adversary Now? Delivered by Anne Harrington.
In this lecture, NNSA Deputy Administrator Anne Harrington describes the historical development of nuclear nonproliferation, whether our technical and dialogue-based means for nonproliferation are still appropriate, and what the international policy and science community must do to maintain and further advance efforts towards nuclear threat reduction.

This talk explores the contribution that the social sciences ought to be making to every aspect of security science and technology. The achievements and authority of the latter are truly remarkable. But they form just one element of our human pursuit of purpose and meaning.

Obstructing those we oppose is not the same as articulating what we are for. Addressing risks is a means to an end, not the end in itself. The biggest threat we face may be an emerging cultural disconnect within society. Engaging the human dimension has never been more vital.

Digital policing – the changing role of technology in law enforcement. Delivered by Commissioner Cressida Dick.
Commissioner of the London Metropolitan Police Service, Cressida Dick, discusses effective digital policing and the need for careful, ethical application of technology in law enforcement in the 2018 Vincent Briscoe lecture.
Engage with us

imperial.ac.uk/security-institute
securityscience@imperial.ac.uk
@imperial_isst
linkedin.com/showcase/institute-for-security-science-and-technology

Jane Lac
Institute Manager

Denise McGurk
Institute Administrator

Max Swinscow-Hall
Communications and Policy Outreach Officer