Improving the relationship between National Security challenges and research

The Work of the CSaP/Global Uncertainties Visiting Fellow

CSaP Annual Conference 18 April 2013

Tristram Riley-Smith

tr356@cam.ac.uk

UNIVERSITY OF CAMBRIDGE

CSaP

Fellowship Objectives

What?

Explore, develop and test mechanisms to promote engagement between academia and the National Security (NS) domain.

Why?

Our research base has a vital contribution to make to the security of the UK and the wider world, but there’s a disconnect between NS stakeholders who own the challenges, and researchers with answers.

Who are the "NS stakeholders"?

This Fellowship has focused on the work of …

- Centre for Applied Science & Technology (CAST) & Office for Security & Counter Terrorism (OSCT) in the Home Office;
- Centre for Protection of National Infrastructure (CPNI);
- Defence Science & Technology Lab (Dstl) in the MOD;
- Office for Cyber-Security & Information Assurance (OCSIA) in the Cabinet Office;
- Security & Intelligence Agencies: MI5, MI6, GCHQ.

The Global Uncertainties Programme

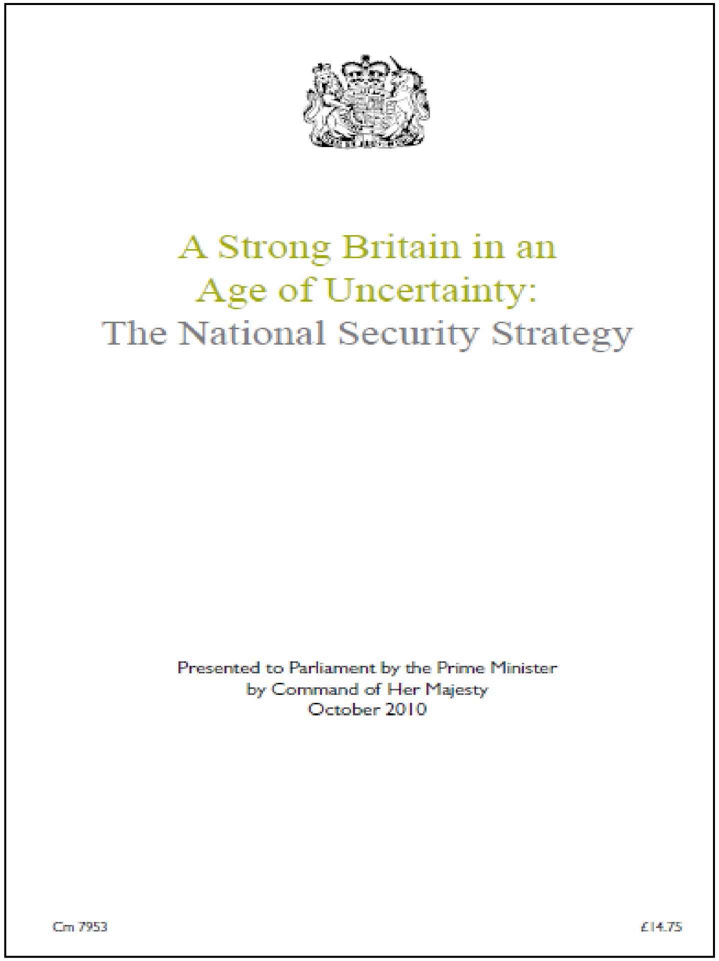
A major theme of RCUK addressing the cross-cutting, interdisciplinary and international nature of security challenge. There are six themes.

- **Terrorism;**
- **Cyber-security**
- **Threats to Infrastructures**
- **Countering CBRN Proliferation**
- **Transnational Organised Crime**
- **Ideologies & Beliefs.**

The NS Strategy

David Cameron and Nick Clegg, writing in the Foreword. October 2010

> “
>
> *Britain today is both more secure and more vulnerable than in most of her long history. We do not currently face a conventional threat of attack on our territory by a hostile power. But we are one of the most open societies, in a world that is more networked than ever before. All of this calls for a radical transformation in the way we think about national security and organise ourselves to protect it.*
>
> ”



A Strong Britain in an
Age of Uncertainty:
The National Security Strategy

Presented to Parliament by the Prime Minister
by Command of Her Majesty
October 2010

Cm 7953

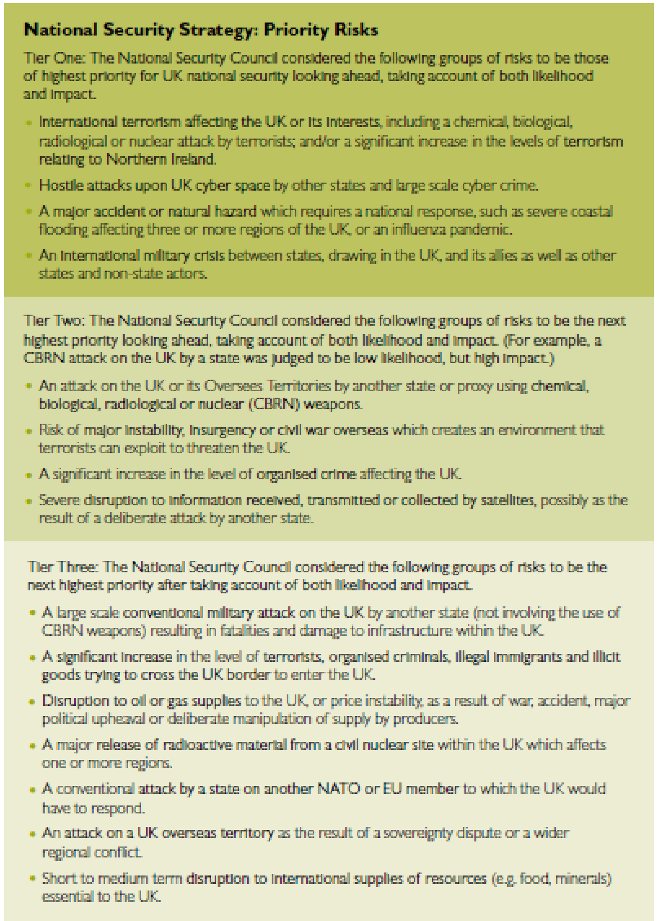
£14.75

National Security Risks

National Security Strategy: page 27

The four highest priority risks facing the UK until 2015 are:

- terrorism (including a CBRN attack);
- hostile attacks on UK cyber-space and/or large-scale cyber-crime;
- major accidents or natural hazards (e.g. coastal flooding or a 'flu epidemic);
- international military crises.



National Security Strategy: Priority Risks

Tier One: The National Security Council considered the following groups of risks to be those of highest priority for UK national security looking ahead, taking account of both likelihood and impact.

- International terrorism affecting the UK or its interests, including a chemical, biological, radiological or nuclear attack by terrorists; and/or a significant increase in the levels of terrorism relating to Northern Ireland.
- Hostile attacks upon UK cyber space by other states and large scale cyber crime.
- A major accident or natural hazard which requires a national response, such as severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic.
- An international military crisis between states, drawing in the UK, and its allies as well as other states and non-state actors.

Tier Two: The National Security Council considered the following groups of risks to be the next highest priority looking ahead, taking account of both likelihood and impact. (For example, a CBRN attack on the UK by a state was judged to be low likelihood, but high impact.)

- An attack on the UK or its Oversees Territories by another state or proxy using chemical, biological, radiological or nuclear (CBRN) weapons.
- Risk of major instability, insurgency or civil war overseas which creates an environment that terrorists can exploit to threaten the UK.
- A significant increase in the level of organised crime affecting the UK.
- Severe disruption to information received, transmitted or collected by satellites, possibly as the result of a deliberate attack by another state.

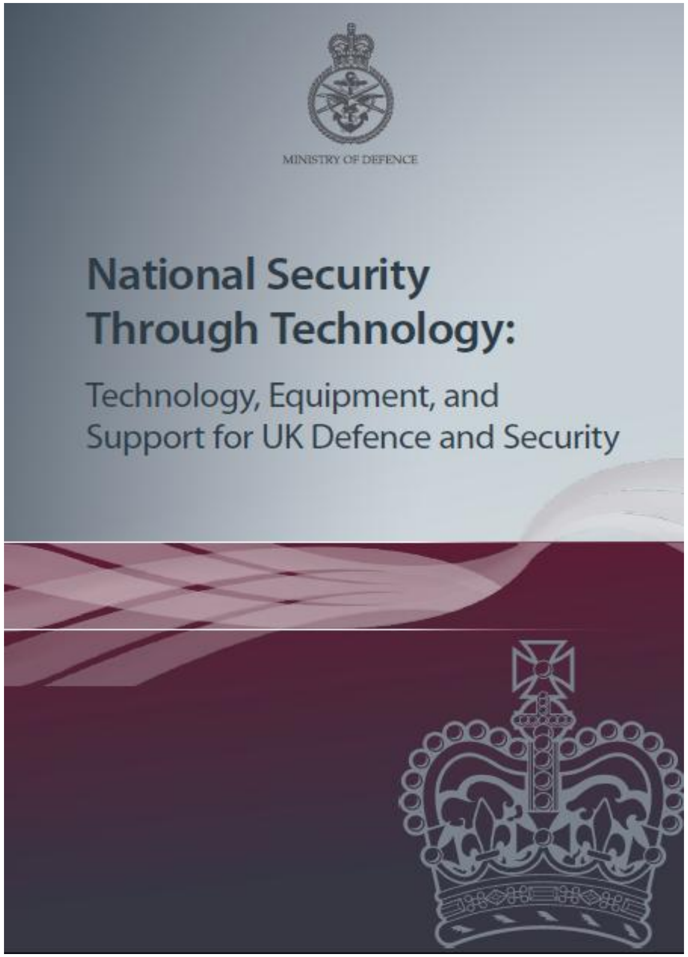
Tier Three: The National Security Council considered the following groups of risks to be the next highest priority after taking account of both likelihood and impact.

- A large scale conventional military attack on the UK by another state (not involving the use of CBRN weapons) resulting in fatalities and damage to infrastructure within the UK.
- A significant increase in the level of terrorists, organised criminals, illegal immigrants and illicit goods trying to cross the UK border to enter the UK.
- Disruption to oil or gas supplies to the UK, or price instability, as a result of war, accident, major political upheaval or deliberate manipulation of supply by producers.
- A major release of radioactive material from a civil nuclear site within the UK which affects one or more regions.
- A conventional attack by a state on another NATO or EU member to which the UK would have to respond.
- An attack on a UK overseas territory as the result of a sovereignty dispute or a wider regional conflict.
- Short to medium term disruption to international supplies of resources (e.g. food, minerals) essential to the UK.

Seven Priority NS Challenges

Source: HMG White Paper *National Security through Technology* (February 2012) p 38

- protect from IEDs
- Identify/mitigate CBRN threats
- protect from cyber threats
- understand human & social dynamics
- communicate rapidly/effectively including data from sensors in challenging environments
- extract value from complex, multiple data sources, media and streams
- identify/assess future risks & threats.



MINISTRY OF DEFENCE

National Security Through Technology:

Technology, Equipment, and Support for UK Defence and Security

The CSaP Project: 76 Interviews

Research Discipline		*Behav’al & Social*	*Bio-science*	*Business*	*Chemistry/ Materials*	*Computer Science*	*Engineering*	*Maths*
Academia	**39**	**9**	**3**	**5**	**4**	**6**	**9**	**3**
Industry	**11**	**3**	**0**	**0**	**0**	**1**	**5**	**2**
Total	***50***	***12***	***3***	***5***	***4***	***7***	***14***	***5***
Government Departments			*GO Science*	*Home Office*	*MOD*	*OCS IA*	*SIA*	
HMG	**26**		**1**	**7**	**5**	**1**	**12**	
Grand Total	**76**							

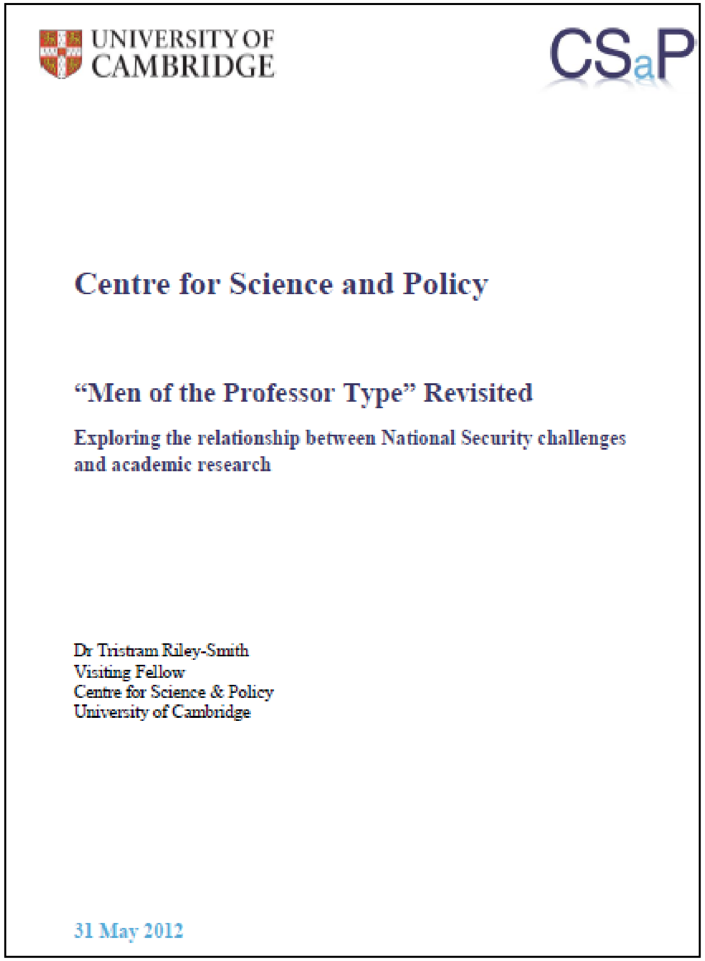
UNIVERSITY OF CAMBRIDGE

CSaP

The Phase 1 Report

Key findings –

- Many instances of successful, often tactical, interaction but …
- Cultural and logistical differences hamper effective engagement;
- We need to nurture relationships of trust;
- We need to accommodate and join up fundamental research and applied science and technology;
- We can experiment with practical mechanisms, and test strategic ideas, for achieving these goals.



UNIVERSITY OF CAMBRIDGE

CSaP

Centre for Science and Policy

"Men of the Professor Type" Revisited

Exploring the relationship between National Security challenges and academic research

Dr Tristram Riley-Smith
Visiting Fellow
Centre for Science & Policy
University of Cambridge

31 May 2012

Obstacles to Engagement

Clash of Cultures

Stereotypes around “Ivory Tower” academics and public servants devoted to saying “Yes Minister”.

Resources and Red Tape

Complaints about bureaucracy on both sides; and significant concern about the approach agencies take to commissioning research (“Fire and Forget” and a “Procurement Mind-Set”).

Trust and Communication

Issues of security/secrets constraining collaboration, with communications challenges of docking and translation.

Key Conclusions

Three inter-related principles
underpin engagement between the two worlds

- The Merits of Variety
- The Value of Intermediaries
- The Importance of a *Whole-Life* Plan, with <u>four</u> stages …
    - **Access**
    - **Exchange**
    - **Commitment**
    - **Delivery.**

Building Engagement

1. Access

Make requirements of NS customers and capabilities of researchers visible and available for scrutiny.

Examples

- A portal managed by the Centre for Defence Enterprise, focussing on a call -"Finding the Threat" - where MI5 and GCHQ can reach out to sources of innovation;
- The Security & Resilience Industry Suppliers' Council (RISC), and plans to create an Academic RISC.
- Gateway to Research - http://gtr.rcuk.ac.uk/ - being trialled by the Research Councils and BIS.

2. Exchange

Develop trusting relationships: requirements and capabilities are better understood, identifying opportunities for research.

Examples

- In-house Summer Schools – SWAMP
- National Security Professors of Practice
- EPSRC/CPNI Sandpits and Ideas Factories
- Trial a National Security Fellowship Scheme.

3. Commitment

Establish longer-term, strategic relationships, where both partners invest time and effort in collaborative research.

Examples

- CSAs and SACs;
- Data-Release Facilities;
- NS Research Institutes;
- Strategic Research Programmes.

4. Delivery

Turn research into capabilities, often with the help of capital markets &industry, to generate new products and services

Examples

- IP/IPR agreements;
- Accelerators/Incubators;
- Security Growth Partnership;
- Technology Strategy Board Programmes.

The Message to Take Away

Remember the Importance of a *Whole-Life* Plan

aka

THE FOUR-ACT PLAY

- Access: put the players on the stage
- Exchange: let the characters get to know one another
- Commitment: establish lasting relationships of trust
- Delivery: reap the rewards of partnership.

And plan all four acts from the get-go!

What Next?

Professor Derek Smith

To discuss the challenge of building relationships of trust in researching and countering flu epidemics … *including the National Security challenge.*

Mark Phillips

To discuss the work of RISC and ideas for a Security Growth Partnership … *including proposals for an "Academic RISC"*.