UNIVERSITY OF CAMBRIDGE

CSaP

Centre for Science and Policy

Improving the relationship between National Security challenges and academic research.

The CSaP/GU Visiting Fellowship 2012:
Summary of Findings and Outcomes.

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

28 February 2013

Contents

* * * * *

Supporting Material

Folder I (Mid-Term Report):
"Men of the Professor Type" Revisited

Folder II (Chicheley Hall Conference)
Record of Proceedings of CSaP/GU Conference, 11/12 December 2012

Folder III (Work-Stream Reports)
National Security Data Release: A Feasibility Study
National Security Fellowship Scheme: A Trial

Acknowledgements. This project was supported by a generous award from ESRC under their Knowledge Exchange Scheme, for which I am very grateful. I also want to thank: all those interviewed in the Inquiry Phase of the project; the Government officials and academics who supported the Feasibility Study into NS Data Release and trial of an NS Fellowship Scheme; and all of those who participated in the June Workshop at the Royal Society and the December Conference at Chicheley Hall. Special thanks go to: Professor Nick Jennings (Chief Scientific Advisor at CPNI); the Master & Fellows of Pembroke College, Cambridge; the Master & Fellows of Worcester College, Oxford; Professor Brian Collins and his team at UCL; the Bursar of New College, Oxford (upholding the spirit of *Amicabilis Concordia*); and the Centre for Science and Policy (CSaP): this project was only made possible thanks to contributions from Dr Robert Doubleday (Director), Mrs Jackie Ouchikh (Head of Programmes), Dr Nick Gray (Associate Adviser), Henry Rex (Administrator) and Ms Julia Graham (who took the record of our Global Uncertainties Workshop in the Royal Society). I am particularly grateful to Dr David Cleevely (Founding Director of CSaP) and Dr Chris Tyler (former Director of CSaP) for welcoming me into the Centre as a Visiting Fellow.

The CSaP/GU Visiting Fellowship, 2012

Introduction

1. This report is the final output from a project that has explored, developed and tested mechanisms to promote engagement between academia and the National Security (NS) domain[i]. It is aligned to RCUK's Global Uncertainties Programme and has taken, as points of reference, the NS Strategy and the White Paper - *National Security through Technology* - which identifies research challenges. I have sought, in this Fellowship, to combine strategic insight with the application of practical solutions, exploring the interplay between them.

2. The Inquiry Phase (January-June 2012) identified cultural and practical differences that make it difficult to establish effective communications between the two domains; there is a need to nurture conditions where relationships of trust can be established between NS stakeholders and academic researchers. The detailed findings are set out in a Mid-Term Report – *"Men of the Professor Type" Revisited* (see Annex 1 for the Executive Summary, and Folder I, attached, for the full report).

3. The programme for the second half of the Fellowship was shaped by a workshop at the Royal Society in June 2012, which recommended that five work-streams should be pursued. Progress with each of these was reported and discussed at a Closing Conference (see Folder II), and is summarised in the table below:

i	**Trial the Feasibility of a National Security Data Release Scheme** A speech corpus, comprising both unclassified and classified material (from telephone intercept operations) was selected as the candidate data-set. The data-owners reviewed legal, ethical, security and operational issues; academic researchers reviewed the intellectual, technical and logistical challenges. Crucially, there are statutory obligations imposed on the authority owning data like this: it can only be disclosed in so far as this is necessary for the proper discharge of its functions; but we have established that this can include research to improve efficiency and/or effectiveness. There are also operational (security) and reputational risks, but these can be mitigated through careful editing and selection of the data. A provisional ruling from the authority's Deputy Senior Information Risk Officer endorsed the release of the unclassified data-set to a research repository, and identified a way forward for making the data available to researchers. The creation of new Data Centres, recommended by the Administrative Data Taskforce (ADT), could facilitate this. **This judgement demonstrated that - in principle, and probably in practice - sensitive NS data can be released for research, where this supports the statutory function of the data-owners**. *See Session IV in the Conference Notes for discussion of the issues and details of the ADT's proposals. The Feasibility Study is to be found in Folder III.*
ii	**Improve Access to Information on the Research-Base** With the help of the Research Councils, we put in place – in August 2012 - arrangements to support NS stakeholder inquiries into on-going research, using the Research Outcomes System. This was communicated to relevant teams in six Government Departments and Agencies, but none made use of the facilities. Feedback gathered in November suggested that either there were established workarounds to perceived obstacles (e.g. use of existing, informal networks) and/or that this was not regarded as a sufficiently high priority to justify action. With the help of RCUK, we also raised awareness among stakeholders of the *Gateway to Research* project: ***Gateway to Research*** **provides an opportunity to transform access to, and knowledge of, research in the UK.** *See the record of the discussion in Session I of our Closing Conference in the Record of Proceedings.*
iii	**Issue Guidelines for IP/IPR** A consultation exercise conducted with the SIA and HOCAST revealed a growing interest in understanding IP/IPR issues, although departments are moving along parallel tracks and at different speeds. I engaged with an IPO initiative to review the Lambert Tool-Kit: the IPO is taking account of the needs of Government Departments engaged in collaborative research with universities and the Independent Reviewer addressed our Chicheley Hall Conference. **A key conclusion is that NS Departments must develop the capacity to understand complex IP issues (e.g. making the right choice from a range of IPR options available; and resolving tensions between national prosperity, product delivery and national security).** This is likely to require new training and/or recruitment programmes. *See the record of the discussion in Session II of our Closing Conference, in the Record of Proceedings.*
iv	**Trial a Knowledge Exchange Scheme** I organised a National Security Fellowship Scheme, with three officials from departments with interest in cyber-security issues meeting over 40 academics from 13 different academic institutions. The officials identified four major themes that they wanted to explore: Threats, Vulnerabilities & Mitigations; the Nature of the Cyber World; the Partnership between Academic Research, Government & Industry; and the Economics, Management & Communication of Cyber-Security. Feedback afterwards produced high scores from the Fellows in terms of impact on their attitude to engagement with academic research, with the prospect for follow-up research; they are communicating what they learnt through internal blogs, briefing colleagues and written reports. We have already seen evidence of follow-up action. **This has proved to be an effective, if small-scale, method for sharing knowledge and starting to build relationships of trust.** *The Knowledge Exchange Report is to be found in Folder III.*
v	**Explore Options for a National Security Portal for Research Proposals** I was able to monitor progress with an innovative call, entitled *Finding the Threat*[ii], conducted by the Centre for Defence Enterprise on behalf of MI5 and GCHQ. This was launched in September 2012, and elicited a record number of responses from Small and Medium-Sized Enterprises and Universities; over 30 proposals have been funded. The number of academic researchers applying was relatively small (at c 15%), but this reflects CDE's traditional focus on industry and the challenge of communicating with researchers. **This problem could be significantly overcome if we could construct more effective channels for researchers to receive requirements, supporting processes like CDE's with the idea of an Academic RISC** (the Security and Resilience Industry Suppliers' Community). *See the record of the discussion in Session I of our Closing Conference in the Record of Proceedings.*

The Chicheley Hall Conference: 11-12 December 2012

4. We drew the year's work to a conclusion with a CSaP/Global Uncertainties Conference at Chicheley Hall on 11/12 December 2012. This was intended to achieve an impact in its own right, by creating a space where forty officials and researchers could meet together, and by encouraging some commitment to changing attitudes and behaviour in relation to collaborative research in the NS sphere. Sir David Omand's concluding remarks are included in Annex 2 to this document, and the full Record of Proceedings is available in Folder II or through this link. Furthermore, the Conclusions and Recommendations, overleaf, draw on the key points to emerge from Conference.

5. There are early indications that this small-scale, shorter-term, goal will deliver impact, based on the feedback received from participants (see Appendix to the Record of Proceedings). For instance, we collected the following responses from participants, at the end of the Conference, when we asked them to give examples of opportunities you might now take to foster engagement between National Security stakeholders and researchers:

Industry Participants

- RISC to make efforts to linking industry and academia in support of HMG, supporting to idea of an Academic RISC and linking this to a Security Growth Partnership;
- The Smith Institute to consider establishing a collaborative workshop for young researchers working on unclassified data, with the incentive of future work on classified data if successful.

Academic Participants

- Cambridge University Intelligence Seminars to establish new links with participants;
- Briefing of Chicheley Hall Conference to be given to the Director of Centre for the Study of Terrorism and Political Violence (CSTPV) at St Andrew's;
- Commitments have been made by CSaP and CSTPV and CSaP for a second and possibly third NS Fellowship Scheme, supported by the Airey Neave Trust;
- Imperial College participants to consider follow-up research initiatives around Tier 1 priorities including cyber-security (and "lessons learned" of relevance to wider engagement with Government);
- Director of Imperial College's Institute for Security Science & Technology to pursue proposal for an Academic RISC;
- Edinburgh University to look for opportunities for follow-up research based on NS speech data
- Cambridge University's Computer Labs to develop research proposals relating to a) accurate indoor location systems technology and b) privacy-preserving advertising technology (which allows Online Behavioural Tracking to support targeted adverts without breaching people's privacy);
- The University of East London to hold an internal 'sandpit' event to discuss NS opportunities;
- Oxford University's Cyber-Security Centre of Excellence to explore new instruments for cross-sector, cross-discipline interaction around security.

Government Participants

- SOCA to explore with Home Office opportunities for the CDE process to be used to support Law Enforcement Agencies;
- Insights from Conference to be fed into on-going work at Home Office on academic engagement, innovation, horizon scanning and IP policies (with a paper going to OSCT Directors and the Home Office Chief Scientific Advisor);
- Dstl to consider follow-up work on a) Advanced Manufacturing, b) IP Exploitation and c) promoting Security and Defence 'Communities of Practice';
- OSCT will take proactive steps to engage with academia on topics of OSCT Open Calls and also consider running sandpits and seminars on specific themed issues;
- CPNI, Dstl and HO CAST to participate in a second NS Fellowship Scheme, focused on detecting/countering Improvised Explosive Devices and Home-Made Explosives;
- HO CAST participants to consider changing their academic engagement strategy to take account of "lessons learned"; to include bringing in academics to discuss areas which are new to Government;
- Individual NS agencies will consider the use of joint programmes and closer collaboration with funding bodies; they will also specifically review the UKVAC partnership (to ensure it is progressing as originally planned).

6. It is particularly pleasing to report, within two months of the Chicheley Hall event, evidence of follow-on action by delegates which is informed, if not directly inspired, by the discussions at the conference:

- CSaP has been commissioned by the Airey Neave Trust to run a second NS Fellowship Scheme, with Fellows nominated by Dstl, HOCAST and CPNI to meet researchers with relevant expertise in the detection and countering of Improvised Exposive Devices and Home Made Explosives;
- RISC has submitted a formal proposal to Ministers recommending the establishment of a Security Growth Partnership;
- CSaP is exploring, with the FCO, options for inviting academics to engage in "horizon-scanning" discussions to consider future proliferation threats over the next 20-30 years.

Conclusions and Recommendations

7. After a year spent exploring the boundaries between the NS community (with its diverse challenges), and the UK's research-base (representing a fragmented but remarkable talent-pool), I have been able to condense the knowledge gleaned through this Fellowship into a small number of conclusions and recommendations; the latter are divided between specific recommendations that have fallen out from this work (which I treat, therefore, as *secondary*) and **one primary recommendation** relating to underpinning principles.

Conclusions

8. Two overarching conclusions have emerged from this work:

- both the National Security and the academic research communities find it difficult to engage with one another, for cultural and structural reasons; a long-standing security culture, formed and hardened during the Cold War, exacerbates an already difficult situation; the importance of building trust, in order to overcome these barriers, cannot be overstated; (see Chapter 2 of the Mid-Term Report); but …
- there is a willingness among opinion-formers and leaders on both sides to effect change; we have seen positive moves on the part of Government through the CDE Call, *Finding the Threat*, and through the work on releasing sensitive data; the academic domain is changing its incentives through a greater commitment to impact, and proposals for an Academic RISC indicate efforts to overcome the fragmentary nature of the research-base; and the active participation of both communities in the NS Fellowship Trial is encouraging; (see the Proceedings of the Chicheley Hall Conference).

Secondary Recommendations

9. A small number of **secondary recommendations** emerge from this project. I have identified where responsibility for taking these forward could suitably reside; senior stakeholders and strategic groups are invited to support their implementation:

i. Consider the merits of producing a concordat between the NS community and academia, based on *The Principles of Scientific Advice*[iii], reflecting the need to accommodate security sensitivities and with an reflecting the need for research to contribute capabilities as well as advice to NS end-users. *See Sir David Omand's comments in Annex 2, para 13*. **Action: NSC (Officials) S&T Committee**

ii. Support the establishment of an Academic RISC. *See Conference Proceedings, Session I, paras 14-17 and feedback from breakout groups.* **Action: RISC/Home Office**

iii. Seek evidence-based advice on how to make NS calls (like "Finding the Threat") work better for academic researchers, and develop guidance on how to improve such bids). *See Conference Proceedings, Session I, including feedback from breakout groups.* **Action: RCUK/CDE**

iv. Institute a regular NS Fellowship Scheme (twice a year?) as a low-cost, small-scale way of building relationships and exchanging information; include some commitment to support follow-up research. *See "NS Fellowship Scheme Report".* **Action: NSC (Officials) S&T Committee**

v. Commission a strategic study into the merits of new NS Research Centres: identify factors behind success & failure of models, testing the vision against capability needs. *See Mid-Term Report: pp 26-27.* **Action: NSC (Officials) S&T Committee.**

vi. Support a work-stream, linked to the ADT initiative, to ensure NS needs are taken into account in the design and implementation of new Government Data Centres. *See Conference Proceedings, Session IV, including feedback from breakout groups; and the Feasibility Study.* **Action: RCUK and NSC (Officials) S&T Committee.**

vii. Consider steps to improve understanding of IP/IPR issues within NS departments and agencies (to include use of the Lambert Toolkit, training and/or recruitment of expertise). *See Conference Proceedings, Session II including feedback from breakout groups.* **Action: RCUK and NSC (Officials) S&T Committee.**

viii. Work with the TSB on engagement with academic research partners & Tech Transfer teams to nurture the development of IP through SMEs and university-focused Accelerators and Incubators. *See Mid-Term Report: pp 22-23.* **Action: NSC (Officials) S&T Committee.**

Primary Recommendation

10. **My primary recommendation** aims to advance – and seek support - for three inter-related principles that need be borne in mind when taking any initiative (however small) to advance engagement between these two worlds. These are set out below.

Principles Underpinning Effective Collaboration

The Importance of a *Whole-Life* Plan

Any exercise to build engagement between NS stakeholders and academic researchers, in order to achieve impact, needs to adopt a "whole-life" approach. I recommend this addresses four different activities, which can be seen as phases encompassing:

- Access: where requirements (of NS customers) and capabilities (of academic researchers) are visible and available for scrutiny;
- Exchange: where trusting relationships can be established, allowing these requirements and capabilities to be better understood, in order to identify opportunities for productive and innovative research;
- Commitment: where longer-term, strategic relationships can be established, with both partners making an investment of time and effort in order to support successful collaborative research;
- Delivery: where research is turned into capabilities (often with the help of capital markets and industry) in order to generate new products, services, tools, techniques, advice and guidance.

Comment.
Each of these four phases needs to be planned for and anticipated, in order to avoid the disappointment of squandered *ad hoc* initiatives. Relationship Maturity Models provide an established approach, but it is a mistake to be overly mechanistic about managing such a process: it is less like a staged production line, more like an eco-system with feedback loops etc.

The Merits of Variety

Variety is to be welcomed. There are many different methods and models for delivering engagement, some operating at a tactical level, others applied more strategically. Examples, using the phases identified above, include:

- Access:
  - *To requirements* - Research Calls; Briefings (to conferences, Learned Societies, Think-Tanks, etc); Grand Challenges;
  - *To capabilities* - Gateway-to-Research; Systematic Reviews; RCUK Consultation.
- Exchange: Sandpits/Ideas Factories; PhD Scholarships; Internships; In-house Summer Schools; NS Fellowship Schemes; Professors of Practice; Guest Lectures;
- Commitment: Blackett Groups; Scientific Advisory Panels/Committees; Chief Scientific Advisors; NS Research Institutes; Strategic Research Programmes; Data-Release Facilities; Catapult Centres.
- Delivery: IP/IPR agreements; Accelerators/Incubators; Venture Catalyst Initiatives; Security Growth Partnership(s); TSB Programmes.

Comment.
It is a mistake to be overly prescriptive. Stakeholders and researchers should be encouraged to trial different approaches.

The Value of Intermediaries

Intermediaries have an important part to play bringing people together (including different NS agencies and different disciplines); some will span different phases. Examples include:

- Access: CDEnterprise; RISC/Academic RISC; RCUK.
- Exchange: Airey Neave Trust; CSaP; CSTPV; Defence Academy; Learned Societies; Oxford Martin School; RCUK; RUSI.
- Commitment: ADT; GO Science; RCUK.
- Delivery: Ploughshare Ventures; Global Security Challenge; Niteworks; BluelightWorks; TSB; University Technology Transfer Offices; Angel/Venture Investors.

Comment.
These intermediaries have a valuable role to perform, as translators, facilitators and load-bearers; the appointment of a *Global Uncertainties* External Champion will contribute to this process. We note the paucity of intermediaries to support the Commitment phase.

11. I believe these principles need to be observed by any institution (eg government department or university) committed to successful engagement and collaborative research. Strategic bodies such as the NSC (Officials) S&T Committee and the RCUK Global Uncertainties Strategic Advisory Group are invited to review these principles, consider their merits, and – if appropriate – take action to establish them as best practice.

Dr Tristram Riley-Smith
Centre for Science and Policy
University of Cambridge

Annex 1. Phase 1 Report - Executive Summary

On 30 June 2012, we produced a report on the Inquiry Phase of the CSaP/GU Fellowship. It was entitled: *"Men of the Professor Type" Revisited: Exploring the relationship between National Security challenges and academic research.* The full report can be found here.

1. This study represents the first stage in a project that aims to explore, develop and test mechanisms to promote engagement between academia and the National Security (NS) domain. It is aligned to RCUK's Global Uncertainties Programme. It has also taken, as a point of reference, the National Security Strategy and a recent White Paper - *National Security through Technology* - which identifies a set of research challenges. (pp 5-6)

2. The main input derives from over 75 interviews with academics, officials and industry representatives. "Issues" and "solutions" identified here have been analysed and turned into a set of problems and propositions. Evaluation Criteria have been designed covering both Short-Term Delivery and Long-Term Impact[1]. (pp 6-7)

3. The underlying problems are presented under three headings: Trust & Communications; A Clash of Cultures; and Resources & Red Tape. A key conclusion is that there is a need to create conditions where relationships of trust can be established; these should change ingrained habits & assumptions along the way. *Perspective is provided with examples of productive & flourishing collaboration.* (pp 9-13)

4. Eight propositions, grouped under two headings, are presented and evaluated in Chapter 3. These are:

TACTICAL (PROCESSES)			**STRATEGIC (STRUCTURES)**		
Knowledge Exchange Schemes	......	pp 14-16	NS Portal for Research Proposals	.....	pp 21-22
Guidelines for IP/IPR	.....	pp 16-17	Accelerators & Incubators	.....	pp 22-23
Information on the Research-Base	.....	pp 18-19	Academic RISC (The "GU Alliance")	.....	pp 24-25
NS Data Release Scheme	.....	pp 19-21	NS Research Centre Strategic Study	....	pp 26-27

5. Five prioritised work-streams are then selected for **short-term action** by the CSaP Fellow (pp 28-29). These will be pursued in the second phase of the Fellowship project, from July-December 2012. In summary:

i. NS Data Release Scheme
Run a trial selecting sensitive data for managed release for research, addressing all obstacles (legal, technical, etc).

ii. Information on the Research-Base
Work with RCUK to develop & promulgate guidance on how to access information about past & current research projects.

iii. Guidelines for IP/IPR
Issue guidance on the use of IP and IPR following a review of working practices in NS Departments.

iv. Knowledge Exchange Schemes
Run a trial NS Fellowship Scheme (with visits to three universities). Explore options for Visiting Professorships.

v. NS Portal for Research Proposals
Work with stakeholders to explore options for a gateway giving academic researchers access to NS end-users.

6. A further five **strategic recommendations,** intending long-term benefits, are made for consideration by senior stakeholders. (pp 29-30). In summary:

1. Research Centres
Commission a strategic study into the merits of new NS Research Centres: identify factors behind success & failure of models, testing the vision against capability needs.

2. Accelerators & Incubators
Work with the TSB on engagement with academic research partners & Tech Transfer teams to nurture the development of IP through SMEs and university-focused Accelerators, etc.

3. An Academic RISC
Support proposals for an academic *GU Alliance* modelled on RISC, providing strategic engagement between academia, industry & HMG; proposals are made for early deliverables.

4. NSC Associates
Support knowledge exchange by establishing a multi-disciplinary academic network of *NSC Associates* who can respond to both strategic and operational requirements.

5. New Interface to Access the Research-Base
Consider developing a state-of-the-art interface to provide access to databases (in RCUK, TSB, etc) on UK research, for all stakeholders, extended to cover the historical record.

7. This paper – revised to reflect outputs from a CSaP workshop at the Royal Society on 13 June2012 – will be circulated to interested parties, including all interviewees, seeking their support in taking forward the recommendations. The Executive Summary (with a copy of the full report if appropriate) will be sent to the NS Council (Officials) Science & Technology Committee and to the Strategic Advisory Group of the GU Programme. These senior stakeholders are asked to consider the five strategic recommendations.

[1] Light Green for Short Term Deliverables | Light-Blue for Long-Term Outputs

Annex 2.
Sir David Omand's Closing Remarks at the Chicheley Hall Conference

1. We have spent 24 hours grappling with the main issues hindering improved engagement between the National Security (NS) community and academia, and the enjoying of the fruits borne of it. It has been notable that there has been so much agreement on all sides as to the benefit of such engagement. The NS community has in particular inherited from earlier generations a folk memory of the decisive part played in Britain's wartime survival through the contribution made by 'the Professor types' bringing fresh insights and knowledge to bear on the intelligence effort. There is today a real wish to engage more closely with the academic community.

2. In light of the discussions around IPR, accelerators, incubators and commercialisation, it is important, however, to emphasise that the NS agenda in improved engagement has to be about finding ways of improving national security. The NS agenda has much in common with the national agenda for economic growth, which is itself a foundation of national security, but different although there is an overlap. Ultimately, this exercise is about designing mechanisms for keeping us safe, not finding greater efficiency measures, economies in public expenditure or generating revenue.

3. We have identified hurdles to fruitful NS-academia relationships, areas for improvement, and lessons to be learned from experience of current and past contacts. It became clear, as the conference progressed, that both the NS and the academic communities must learn these lessons and alter their attitudes and behaviour to each other if the potential of this relationship is to be fulfilled.

Lessons for the NS Community

4. There needs to be a different strategic understanding between Government departments and agencies on the one hand and academia on the other: the NS community are too often liable to adopt a 'free- lunch' attitude to seeking academic advice, and the number of references made by both academics and civil servants to REF and assessment during the conference was telling.

5. There are clearly problems around NS officials' attitudes to entering debate with 'outsiders': the NS community must be more open to discussing the 'problem space' with academics, not just the 'solution space'. They cannot adopt a 'procurement' attitude where they approach researchers with specific requirements and simply demand solutions. To harness academic creativity it is essential that researchers really understand the operational context and thus the underlying problems for which their assistance is being sought. It might be necessary to find new 'safe spaces' within which the two communities can debate and discuss problems. Furthermore, it is important that officials recognise that academics have day jobs. They can spare some time to brainstorm and share thoughts, but without substantive and rewarding engagement they will quickly be turned off.

6. When NS people do approach academics it is important that they avoid just turning to, and thus over-using, the usual suspects' with whom they already have contact: they ought not to have a small group of 'favourite' academics to whom they turn time after time. While there is obvious value in using some tried and tested individuals, there is also value in engaging with a diverse range of academics and institutions. There are, of course, significant barriers to NS data release, but officials should be more proactive in looking for opportunities to make data available to researchers – it is worth it given the potential benefits that could be reaped; the work of the Administrative Data Taskforce, and the creation of Administrative Data Research Centres, is relevant here.

7. The final lesson for the NS community to recognise is that they do have 'pulling power'. If an academic receives an invitation to participate in a discussion in Thames House, Vauxhall Cross, the GCHQ 'doughnut' or even the Cabinet Office for example, it is hugely appealing and a difficult invitation to turn down if only out of curiosity.

Lessons for Academia

8. The conference also revealed a number of ways academics can do their bit in improving productive relationships with government. Firstly they should recognise that the NS community is working on behalf of the whole nation. Serious security challenges face us, and in areas such a cyber-security may well worsen in future.

It is in everyone's interest to maximize the use of the available brain power within the nation. The NS community also, by the nature of their work, throws up challenging and diverse sets of problems that are of interest academically in their own right. Examples that have been mentioned in the margins include the use of elliptical curves in secure encryption algorithms for example or machine transliteration of informal speech and argot.

9. The NS community also represents a source of potential and sometimes unique data that opens up new possibilities for research. And finally, but by no means least, the NS world does have funds available even in these constrained times to invest in high priority areas, an example being the additional funding available for research in cyber security, and aspects of counter-terrorism have also benefitted from having a stream of cross-departmental funding outside the Research Councils. The discussion at the seminar has also shown that there are ways in which academic interests in patenting innovation or otherwise exploiting intellectual capital can be negotiated with government.

10. In doing so, they must accept that there will inevitably be constraints associated with dealing with the NS community. While officials should work to make data as available as they can, issues around confidential information and clearance will never go away. Academics simply have to accept this and recognise that there is still a great amount of substantive and interesting research that can be done regardless.

11. There is also a need for academics to be more joined-up when engaging with the NS community. NS issues will very rarely fit into just one department or faculty: real benefits come from cross-disciplinary research. Academics should therefore look to form strategic partnerships where possible, which can develop into self-organising networks and lead to other opportunities, as well as forming a more established channel for communication between academics and NS people.

12. The idea of NS Associates did not really gain much traction with the delegates, but there did seem to be a lot of enthusiasm and support for NS Fellowships (as trialled by Tristram Riley-Smith), and visiting professorships and fellowships to foster partnerships and promote knowledge exchange. Sandpits, co-location and 'ideas days' were also identified as useful ways of building these partnerships.

13. So many groups mentioned the question of trust. It is such a key issue and it came up time and again. The importance of building trust here cannot be overstated. It may be worth looking at *The Principles of Scientific Advice* that were revised by the Government Chief Scientific Adviser following the forced resignation of David Nutt as chairman of the Home Office Advisory Committee on the Misuse of Drugs (ACMD). That agreed document sets out the rules of engagement between Government and those who provide independent scientific and engineering advice with the intent of building greater trust. They provide a foundation on which independent scientific advisers and government departments should base their operations and interactions, including issues of academic freedom. There may be merit in a comparable concordat between the NS community and the CSA, Royal Society (or some such institution) as a good starting point of enhancing collaboration between academia and the NS community.

14. In conclusion, a quote from Darwin comes to mind: *It is not the strongest of the species who survive, nor the most intelligent; rather it is those most responsive to change.* I have every confidence on the basis of our discussion that the capacity is there on all sides to change preconceptions and work together in adapting to our future security environment.

Annex 3. Acronyms and Glossary

ADT – the Administrative Data Taskforce formed by HMG in 2011 to review ways to make Government data available for academic research. Its report was published on 11 December 2012.

AHRC – the Arts and Humanities Research Council.

BBSRC – the Biotechnology and Biological Sciences Research Council.

BIS – the Department for Business, Innovation and Skills.

CBRN – chemical, biological, radiological and nuclear (a term used to refer to weapons and/or threats).

CDE – see Centre for Defence Enterprise.

Centre for Defence Enterprise – a "gateway" established by the MOD to provide access to all organisations that may have a disruptive technology, new process or innovation that has a potential defence application. It is aligned with TSB's Small Business Research Initiative.

CPNI – Centre for the Protection of National Infrastructure.

CSaP – the Centre for Science and Policy, Judge Business School, University of Cambridge.

CST – the Council for Science and Technology

CSTPV – Centre for the Study of Terrorism & Political Violence, University of St Andrew's

DHS – US Department of Homeland Security.

Dstl – Defence Science and Technology Laboratory; a part of MOD.

DTC – Defence Technology Centre.

EMRS DTC – MOD's Electro-Magnetic Remote Sensing Defence Technology Centre

EPSRC - Engineering and Physical Sciences Research Council.

ESRC – Economic and Social Research Council.

FST – the Foundation for Science and Technology.

GC&CS – the Government Communication & Cypher School, Bletchley Park; precursor to GCHQ.

GCSA – the Government Chief Scientific Advisor: the current incumbent is Sir John Beddington.

GSC – the Global Security Challenge (qv).

Global Security Challenge – an annual competition established in 2006 by London Business School students to empower start-ups in the homeland security technology space. It offered entrepreneurs with security ideas the opportunity to showcase their IP and compete for over $500,000 in cash-grants sponsored by the DHS.

Global Uncertainties Programme – RCUK Programme addressing the cross-cutting, interdisciplinary and international nature of security challenges. It focuses on six themes: Terrorism; Cyber-security; Threats to Infrastructures; Countering the Proliferation of CBRN Weapons & Technologies; Transnational Organised Crime; and Ideologies & Beliefs.

GO Science – the Government Office of Science, overseen by GCSA, in BIS.

GU – Global Uncertainties Programme.

HHS – US Department of Health and Human Services.

HMG – Her Majesty's Government.41

HOCAST – the Home Office Centre for Applied Science and Technology; formerly HOSDB.

HOSDB – the Home Office Science and Development Branch (now HOCAST).

IfM – the Institute for Manufacturing (qv)

i-LIDS – Image library for intelligent detection systems, maintained by HOCAST (qv).
Institute for Manufacturing - a division within the Department of Engineering at Cambridge University; it is multi-disciplinary: experts cover such diverse subjects as management, design, routes to market, technology, maintenance, strategic planning, performance measurement, production, supply networks, Industrial Policy, Industrial Innovation, etc. The aim is to achieve a joined-up approach from research to applied service delivery.

Intellectual Property (IP) – formalised/legal description of "a creation of the mind" that is owned by someone.

IP – see Intellectual Property.

IPR – Intellectual Property Rights: exclusive rights enjoyed by the owners of IP.

ITA – the International Technology Alliance (also known as the Network & Information Sciences International Technology Alliance) - a collaborative research alliance begun in 2006, between the UK MoD, the US Army Research Laboratory, and a consortium of leading academic and industry partners.

LEA – Law Enforcement Agencies: HM Revenue & Customs, Police Forces, UK Border Agency, Serious & Organised Crime Agency, etc.

MOD – Ministry of Defence.

MRC – the Medical Research Council.

NERC – the Natural Environment Research Council.

NSC – National Security Council.

ONA – the Office of Net Assessment, within the US Department of Defense.

ONS – Office of National Statistics.

OSCT – Office of Security and Counter-Terrorism, in the Home Office.

RAE – The Royal Academy of Engineering.

RCUK – Research Councils of the United Kingdom.

RISC – Security & Resilience Industry Suppliers Community.

RUSI – Royal United Services Institute

SEAS DTC – Systems Engineering for Autonomous Systems Defence Technology Centre

SIA – Security and Intelligence Agencies: GCHQ, MI5 (or Security Service), MI6 (or Secret Intelligence Service).

SLS – the Scottish Longitudinal Survey.

SMEs – Small and Medium-Sized Enterprises.

STFC – the Science and Technology Facilities Council.42

Technology Readiness Level (TRL) – A measure developed in the USA to describe the maturity of evolving technologies: 1-2 = Basic Research; 2-4 = Research to Prove Feasibility; 3-5 = Technology Development; 5-6 = Technology Demonstration; 6-8 = System/Product Development; 8-9 = System Test, Launch & Operations.

Technology Strategy Board (TSB) – the UK's national innovation agency: an executive non-departmental public body established by HMG in 2007 and sponsored by the BIS.

TRL 1-9 – see Technology Readiness Level.

TSB – see Technology Strategy Board.

End-Notes

[i] For the purposes of this project, I have focused attention on the research requirements of the Centre for the Protection of National Infrastructure (CPNI); the Home Office's Centre for Applied Science & Techology (CAST) and Office for Security & Counter Terrorism (OSCT); the Office for Cyber-Security & Information Assurance (OCSIA) in the Cabinet Office; the Defence Science & Technology Lab (Dstl) in the Ministry of Defence; and the Security & Intelligence Agencies or SIA (GCHQ, MI5 and MI6). Other departments and agencies with an interest in the outcome of this research include the Civil Contingencies Secretariat, the Foreign & Commonwealth Office, the Joint Intelligence Committee, Law Enforcement Agencies (including the Serious & Organised Crime Agency), and the National Security Council.

[ii] This focused on short 3-month proof-of-concept and/or demonstration-of-benefit studies that had the potential to lead to next generation solutions for a range of security challenges. This could be partial demonstration of a new technology, or a theoretical or experimental approach that allowed a better understanding of the proposed systems / techniques. MI5 was particularly interested in covert surveillance techniques and threat identification; GCHQ's focus was on online identity assurance and management, as well as open source analytics.

[iii] See: www.bis.gov.uk/go-science/principles-of-scientific-advice-to-government.