Information Assurance Advisory Council
IAAC

IAAC Cyber leadership Forum (Formerly PDM)
Held at Simpson's in the Strand, London, on 4th April 2019
Chaired by Lord Arbuthnot of Edrom

Report compiled by Nigel Jones, CEO IAAC

Summary of Recommendations

The theme of the Cyber Leadership Forum was National Research Strategy in Cyber Security Science and Technology. In order to increase the effectiveness of strategy the following recommendations are made:

- The strategy must identify a user or sponsor who has the authority in the wider community to define business benefits and research scope, taking account of:
    - The need to co-ordinate and monitor objectives and activity
    - Exploitation pathways
- To develop a strategy that understands the vital contribution of blue-skies, corporate and applied research in the 'triangle' of government, industry and academia. This should take into account goals, value-for-money, and process by which these might be determined.
- To develop a strategy that recognises and builds on the strengths inherent in the UK cyber security sector such as technical excellence and academic collaboration in socio-technical issues. This calls for further engagement with, for example, law; business schools; HR; Philosophers; Medical; Teacher Training, Industry and Government.
- HMG must ensure that priority risks are identified and addressed.
- There is also a need to support the wider community, nationally, regionally and locally, regarding the outcomes of research and empirically based approaches in their application in practice.
- To develop activities aimed specifically at improving integration/co-operation between industry and university sectors alongside end-users in government and elsewhere. This means more than industrial investment in university projects. It includes an urgent need to engage the talents of those universities that are teaching cyber related courses, but are not yet classed as Centres of Excellence, throughout UK regions.
- To develop a programme for the formal communication of results, taking account of security and commercial IP issues.

With thanks to IAAC's IAAC National Sponsors:

O2 · Reliance acsn Specialists in IT Security Management · sopra steria · QinetiQ · BT
NORTHERN TRUST · THALES · Raytheon UK · NORTHROP GRUMMAN

Introduction

1. The theme of the Cyber Leadership Forum was National research strategy in Cyber Security Science and Technology. The evening was convened noting that it would aim to address a number of questions pertinent to UK national strategy. These included:

   - What input is required for future science and technology strategy?
   - How are current initiatives, such as Research Centres of Excellence and Research Institutes, doing?
   - Are there processes that can be improved?
   - Are there missing themes in the current agenda
   - Is industrial research overlooked in strategy, or is it an assumed given?
   - What can government do to incentivise industrial investment and research in priority areas, alongside its investment in our universities?
   - How can and should the IAAC community help?

   This report outlines the observations and discussion points raised throughout the evening.

UK Research landscape strengths

2. **Collaborative academic community**. It was argued that the UK has a vibrant collaborative community in academic research that is not reflected elsewhere. This should not be taken for granted. The NCSC role could be described as a force-multiplier in trying to shape this collaborative working in academic-led research.

3. **Socio-technical investigation**. There is an emerging appetite for working on socio-technical aspects of security in academic institutions. This is necessary for the 'wicked problems' of cyber security. Wicked problems 'share a range of characteristics—they go beyond the capacity of any one organisation to understand and respond to, and there is often disagreement about the causes of the problems and the best way to tackle them.'[1] There are no simple solutions to wicked problems, but rather multiple strands of work, are needed to address the problem situation. Research should work on 'taming'[2] rather than solving 'wicked problems' to promote desired outcomes for the UK and its citizens and consumers. PETRAS[3] has been a good example of where the strengths described above were practiced.

[1] See Australian Government https://www.apsc.gov.au/tackling-wicked-problems-public-policy-perspective for a discussion of wicked problems in a public policy context. (Accessed 18th April 2019)

[2] Falk Daviter argues that 'in sharp contrast to the holistic ideal of problem-solving, problem taming aims to transform an ill-structured or wicked problem into a more manageable and well-structured problem for the purpose of decision-making.' See Falk Daviter (2017) Coping, taming or solving: alternative approaches to the governance of wicked problems, Policy Studies, Vol 38, 2017, Issue 6. Available at: https://rsa.tandfonline.com/doi/full/10.1080/01442872.2017.1384543?scroll=top&needAccess=true#.XN6uQKZ7m3I. Accessed 18th April 2019

[3] See https://www.petrashub.org/about/ (Accessed 18th April 2019) for the background on PETRAS.

UK research landscape weaknesses

4. **Barriers to interdisciplinary-working**. There was discussion of a number of the legacy issues regarding the way universities organise themselves, that impact upon their ability to work across subject domains. Departmental organisation can sometimes undermine collaborative working. Academic journals usually specialise by subject, so hinder the publication of cross-disciplinary and interdisciplinary research. Teaching across disciplines can also suffer because, for example, there is friction in transferring tuition fees within and between institutions. There was a need to engage universities beyond the centres of excellence.

5. **Measuring impact**. There was agreement that there is difficulty in showing the impact of academic research. Research funding has a long tail, which leaves it problematic to answer some of the following questions:

   - Who ultimately benefits?
   - How do the findings get to those who need them?
   - How do we avoid wasting resources in research even as there are technological shifts and social change?
   - How do we show impact and extract value from the research?

6. **Demonstrating impact and communication**. One argument was that not all academics appreciate the importance of demonstrating the impact of their work; they are incentivised to publish and then move on. As a result many are not good at promoting their work, or even if they could be, paid, or promoted, for doing so. More creativity is required in bringing professionals and academics together to develop research direction and close the gap between findings and their utility in practice. This requires some translation between academics and practitioners and vice-versa. There are moves afoot in some universities to address this problem in more inclusive ways than is currently common, such as briefings to policy-makers.

7. **Fragmented approaches**. In terms of industrial research, it was argued that there has not been the same collaborative and inclusive approach to addressing cyber security as had been observed in previous Government counter-terrorism programmes. Perhaps lessons identified from the past might be applied in the context of cyber security. In particular there is a highly disaggregated set of actors involved in the cyber-security problem. This poses difficulties in suppliers engaging with multiple partners and agencies. For example, there are many funding routes through Growth Partnerships, DSTL, DASA, JSaRC and DCMS. This would benefit from a whole of government approach.

8. **Lack of conceptual clarity in strategy and doctrine**. The disaggregation described above has arguably led to, or is symptomatic of, lack of clarity in the conceptual approach to the relationship between national security strategy, the business of the cyber security sector, cyber security investment and exports to other countries. This has practical implications such as the assessed widespread underfunding of investment in law

enforcement regarding cyber security and cybercrime. It was suggested that UK Policing was suffering from cuts, undermining the ability of government to deliver on its 'fusion doctrine'[4] with regard to cyber, and therefore its ability to tackle cybercrime. This has led to a situation where on one hand Government has justifiably highlighted the world-leading capability in the UK regarding cyber security, whilst on the other, has struggled to provide Law Enforcement with the resources necessary to respond effectively to rising, and ever-changing, cybercrime.

Remediating the problem issues and exploiting the strengths of the UK research landscape

9. **Creating an authoritative owner/coordinator**. Although the NCSC is noted as the 'single authoritative voice' in the Interim Cyber Security Science and Technology Strategy, it might be viewed more as fulfilling its role as 'national technical authority', rather than a focal point for research strategy. DCMS is tasked with leading the plan for research. There is a strong argument for having a single agency that acts as the focus for effective coordination, with a clear strategy to communicate this to the broadest community. The coordination role should extend to bringing industry and academia together in a single research strategy.

10. **Industry and government relations**. There are many worthy cyber security initiatives, but there needs to be greater cooperation between industry and government. Discussion on this fell into camps, where a Government view was that industry needed to do more, such as putting money into academic research institutes that are currently largely funded by Government. On the other hand, there was a view that Government needed to do more to work with industry on making their requirements clear. Industry, specifically the supplier community, needs to know the priorities. This should include making it easier for the supplier community to access the end-user community. Note that there was a call for more precision in how 'industry' was described. It is acknowledged that Government and Industry, in terms of critical infrastructure protection, has some strong relationships but this is not reflected in the overall relationship with supplier companies, from whom Government wishes to see more investment in Government initiatives, like the research institutes.

11. **Diverse social and stakeholder engagement**. There were a number of strong calls for wider engagement in addressing cyber security challenges in two main ways. Firstly, there needs to be more diversity in the community rather than the 'usual faces' being at different events and sitting on funding panels. A number of initiatives were highlighted that sought to widen participation by bringing in younger people, or where regular participants would introduce someone who previously had not been involved. Secondly, the debate was characterised as a national security elite debate. Indeed, the UK was seen as being in the 'premier league' in its approach. However, the UK still lacked a social understanding of what the problem truly is because the elite was not leading its engagement with society at large. Estonia and Sweden were hailed in their attempt to redefine their population's relationship with security, as was Singapore in its 'total

[4] See https://rusi.org/commentary/fusion-doctrine-one-year (Accessed 18th April 2019) for one assessment of Fusion Doctrine from March 2019.

defence' concept. A question remained as to how societal engagement on these issues might be conducted in the UK and, by extension, its function in shaping the research strategy. This perhaps was linked to political questions of investment in resilience, law enforcement and cybercrime, as mentioned above.

12. **Breaking out of the cyber specialism**. One way in which the cyber discussion might be given more relevance and resonance to other stakeholders, is to make its discussion less specialised. For example, it was argued that cyber security is an enabling function of the services and systems society uses. These primary functions need to form the basis of the conversation and wider engagement, alongside technological innovations involving AI, robotics and automation. There is a risk otherwise, that progress will not be made while the debate remains in the domain of the specialist. It was generally agreed that the wicked problem of cyber security cannot sit within prescriptive or specialist frameworks, just as cyberspace itself is unbounded.

13. **Framing the research system**. This in turn led to a question of how cyber security research might be framed in terms of this unbounded and inter-disciplinary context. Is doing so not a necessary condition for organising strategy? For example, suppliers might see research as part of a chain towards product development. Others might see it as a funnel, whilst others yet see it as an eco-system. If it is an eco-system, then further questions arise as to how to shape its performance as a system towards national security goals. Understanding that the market is usually event-driven, with suppliers trying to develop solutions for pressing 'here and now' problems was not in itself a strategy, but a matter of fact regarding current practice. Rather there needed to be a clearer understanding of the Government's 'here and now' problems, and those problems beyond, that could in turn influence the research agenda for industry (who would continue to invest in their own businesses), and academia. Strategy must try to shape the eco-system in which research takes place in order to address national security and resilience challenges. This would need an effective contribution from blue-skies and applied research, such that there was a suitable balance of both, and a comprehensive understanding of their function.

14. **Interventions designed for objectives**. There have been mixed results in government initiatives to intervene in the above context. Some praise was given to the way academic centres of excellence were now working and exchanging ideas in a buzz of lively debate and innovative thinking. This was stimulating university chancellors to look for further investment in those ideas. On the other hand, the Cyber Invest programme had started strongly, but was not working quite as was initially hoped in terms of investment and momentum, nor was the private sector investing enough in research institutes. How might this be explained, or at least, how might we come to understand where the problems lie? There were several contributions that addressed this directly and indirectly.

    14.1. Firstly, as a number of people suggested there needs to be a transparent 'problem book'[5] on which we can work. This is another way of saying that the requirements

[5] See https://gtr.ukri.org/projects?ref=EP%2FR022844%2F1. Accessed 17th May 2019

need to be made clear. These are not cyber security requirements per se, but wider issues that need to take cyber security as an enabler into account – AI, Machine Learning, robotics, automation etc.

14.2. Secondly, there is an absence of thought leadership in the national picture, which leads to unclear strategy and muddled thinking. We need a mechanism to support thinking at the national level. We also need the ability to work at the local level amongst communities at the same time, as what happens locally really matters when addressing resilience.

14.3. Finally, the triangle of government, academia and industry needs to be reviewed. It isn't a question of one leading the other two, but rather a genuine need to work together. It is understanding the objectives each sector has and how this might be expressed in terms of collective action.

IAAC comment

15. It was clear in the discussion that the UK national strategy cannot be described as one in which all stakeholders are clear about their contribution and desired national security outcomes. Rather the relationships in the triangle of government, academia and industry are ill-defined in terms of national cyber security research. The discussion called for a number of improvements in coordination, diversity in stakeholders, engagement with society and clarity on requirements. This presents a challenge in that a rigid top-down, requirements-based national strategy would seems elusive, not least because of the diversity of actors, and scale of the cyber security sector and end-user base. With this perceived complexity, it is not surprising that the research landscape is described as an eco-system. This eco-system would exist in some form, even without a national strategy!

16. A complex eco-system composed of entities with varying degrees of autonomy does not respond well to command and control processes, except in the most machine-like project management approach, where a customer pays for an outcome, delivered by a supplier against a specification. There is a sense then, that we are looking for a research system that performs better in the interests of national security. National security might be defined narrowly in terms of the specific needs of government agencies, or it might be defined broadly in terms of the resilience of the United Kingdom to cyber-attack and cyber-crime. It is possible that the former may be driven by specified projects, facilitated by greater tactical engagement between end-users and suppliers, whilst the latter requires more buy-in by all sectors to a wider agenda and sense of national purpose. Naturally, these are not mutually exclusive ideas, but we should understand that one approach does not in isolation serve the purposes of the other.

17. If we wish the research 'eco-system' to perform better, we must define its operation as behaviour towards goals. This naturally requires the setting of goals, and a champion or owner of the goals, who plan necessary actions and reviews performance. The actions required might be explicit and contractual, but other will be more about nudging the behaviour of the system in the desired direction through a series of incentives or

disincentives aligned to goals. This inherently will require regular review as a complex system needs monitoring in order to continue to align its performance with changing problems and perhaps changing goals. It will require engagement, and perhaps institutional changes to incorporate the views of diverse stakeholders.

IAAC Recommendations

18. The following are recommended:

- The identification of a user/sponsor who has the authority in the wider community to define the desired business benefits and scope of research objectives, taking account of:
    - The need to co-ordinate and monitor objectives and activity (including schedule, priorities and funding).
    - Exploitation pathways, involving the timely engagement of the industry partners, in order to ensure smooth transition from development into deployment, linked to a resourced improvement plan.
- To develop a strategy that understands the vital contribution of blue-skies, corporate and applied research, taking into account goals, value-for-money, and process by which these might be determined. The 'triangle' of government, industry and academia, needs to understand and engage with this process, in order to apply their talents to areas of greatest mutual benefit.
- To develop a strategy that recognises and builds on the strengths inherent in the UK cyber security sector such as technical excellence and academic collaboration in socio-technical issues. This calls for further engagement with, for example, law; business schools; HR; Philosophers; Medical; Teacher Training, Industry; Local & Central Government.
- HMG must ensure that priority risks are identified and addressed. There is also a need in parallel, to support the wider community regarding the outcomes of research and empirically based approaches to, for example; the provision of 'Roadside Assistance' for citizens and SMEs after cybercrimes; architectural approaches to reducing vulnerability; development of better software; and many more….
- To develop activities aimed specifically at improving integration/co-operation between Industry and university sectors alongside end-users in government and elsewhere. This means more than industrial investment in university projects. It includes an urgent need to engage the talents of those universities that are teaching cyber related courses, but are not yet classed as Centres of Excellence, throughout UK regions. This should create an atmosphere of inclusion and co-operation, with incentives and pilot projects such as those ongoing in the North West.
- To develop a programme for the formal communication of results, taking account of security and commercial IP issues.

Thanks and disclaimer

IAAC is grateful to its guest speakers who inspired our discussion and debate. They were Dr Madeline Carr, Director, Research Institute for the Science of Cyber Security and Dr Hugo Rosemont, Director, Security and Resilience, ADS Group. The views expressed in this brief report do not necessarily reflect those of our speakers, sponsors or any other individual participant, nor can the attribution of any point be inferred.