

# UK Academic Cyber Security Research: Best Practice for Commercialisation

Andrew Dwyer, University of Oxford  
andrew.dwyer@cybersecurity.ox.ac.uk

## 1. Overview

There is a significant and productive relationship between universities and businesses in developing cyber security academic research in the UK. This research concentrated on the 13 Academic Centres for Excellence in Cyber Security Research (ACE-CSRs) established from the first UK Cyber Security Strategy. These centres have previously been described as “a trend setter”<sup>1</sup>, however little work has explored their commercial activity. Commercialisation in this study is defined as the transaction between a university, academic consortium, or academic(s) that attract surplus financial benefit in the market; whether through consultancy, patents, collaboration or university spin-off/-out. This provides ample opportunity for commercial outputs to be included within this research.

Interviews were held at several universities across the UK, including interactions with nine ACE-CSRs<sup>2</sup> in addition to other commercialisation organisations. This involved 29 individuals over 18 interviews during May and June 2015. Due to a lack of granularity in the data collected by commercialisation offices at universities, quantitative analysis is not possible. Therefore this provides an overview of opinions and comments by individuals across different organisations. This followed the research questions of the study that are outlined below:

1. Assess the current commercialisation landscape for cyber security in industry and academia, including the broader policy environment.
2. Engage with the UK Academic Centres of Excellence in Cyber Security Research (ACE-CSRs) to evaluate how cyber security research has and can be commercialised.
3. Provide guidance to best practice for academic research through developing insights into current communication and policy limitations for future cyber security engagement in the UK market.

## 2. Previous Research

There has been important work on understanding how universities engage with business. This has primarily focused on the ability of universities to adequately commercialise according to their expertise and flexibility. Many universities have developed Technology Transfer Offices (TTOs) to facilitate these interactions; however they have been critiqued for their overvaluation of IP<sup>3</sup> and lack of expertise<sup>4</sup>. This critique has also been applied to spin-outs<sup>5</sup>. Academic research has questioned the direct role between universities and their contribution to technology-based businesses, following the example of Cambridge<sup>6</sup>. This is further followed by the need to support ‘softer’ forms of engagement in the innovation ecosystem, such as consultancy. This argues there is an intrinsic interdependence between ‘soft’ elements and the ‘hard’ development of physical products, especially in the IT sector.

---

<sup>1</sup> Pierre Anderson Consultants, 2013. *Competitive analysis of the UK cyber security sector*. London, p.60

<sup>2</sup> These ACE-CSRs were Imperial College London; Lancaster University; Queen’s University Belfast; University College London; University of Birmingham; University of Cambridge; University of Kent; University of Oxford; University of Surrey.

<sup>3</sup> Lambert, R., 2003. Lambert review of business-industry collaboration. *Norwich, UK: HMSO*.

<sup>4</sup> Sharifi, H., Liu, W., McCaul, B. and Kehoe, D., 2008. Enhancing the flow of knowledge to innovation: challenges for university-based knowledge transfer systems. In: J. Bessant and T. Venables, eds., *Creating wealth from knowledge: meeting the innovation challenge*. pp.335 – 358.

<sup>5</sup> Wright, M. and Filatotchev, I., 2014. Stimulating academic entrepreneurship and technology transfer: A case study of Kings College London commercialization strategies. In: T.J. Allen and R.P. O’Shea, eds., *Building technology transfer in research universities: An entrepreneurial approach*. Cambridge University Press Cambridge, pp.241 – 261.

<sup>6</sup> Connell, D. and Probert, J., 2010. Exploding the myths of UK innovation policy. *Centre for Business Research, University of Cambridge*.

The networks universities operate in are crucial elements in depicting good commercialisation. Yet there is concern that the UK may be trying to emulate a US-style innovation policy without considering the specific environmental determinants. This includes the applicability of venture capital to generating university commercialisation, which generated mixed responses<sup>7</sup>. This concern also extends to the use of the 'Valley of Death' popularly used in commercialisation, when ventures find it difficult to increase in their maturity<sup>8</sup>. Currently, little research exists on cyber security commercialisation, with only a few examples from the United States providing any detailed analysis, and not from a wider innovation lifecycle perspective.

### **3. Commercial Landscape in Cyber Security**

The ACE-CSR programme has provided an avenue for concentration of expertise and knowledge. A synopsis of the current landscape for cyber security is provided below:

#### **3.1 Funding**

Concerns were raised over capital investments moving away from riskier ventures. Yet Impact Acceleration Accounts (IAAs) were seen to be an appropriate mechanism to develop the commercial potential of academic work. The University of Surrey issues up to £20,000 for each successful application, of which multiple can be made. Whereas Lancaster University uses the funding in a two-stage process: the first stage as a funded feasibility study and a second funded stage likely to lead to a Knowledge Transfer Partnership (KTP). The flexibility that IAAs can provide on a singular university level ensures they can adapt to particular institutional contexts.

#### **3.2 Location**

For the ACE-CSRs, and others outside of the 'South-East Triangle' between London, Oxford and Cambridge, there was significant concern they were being overlooked on potential investment to commercialise. The perception that a focus on London was damaging was clear, with much government and private support argued to be based in this part of the UK. This is part of broader understandings of clustering and its importance in generating successful commercial activity, with multiple potential networks around the UK. Ecosystems are required to have a diversity of avenues for exploration, and in the UK, London is the only place where this is currently feasible according to participants. This understanding was also essential for engagement with incubators and accelerators.

#### **3.3 Networks**

Meaningful engagement was a strong theme, where past engagement has been restricted to sending out brochures to SMEs for example. Yet academic institutions are now far more concerned with developing deep, quality relationships. These strong community groups that form are a critical part of cyber security, with close personal networks for academics and professionals across both government agencies (such as the MoD and DSTL) and business. For SMEs, the networks that bring together clusters such as the UK Cyber Security Forum were seen positively for most participants. These strong community bonds need to be strengthened further, but also increase the openness to others, with some participants noting a potential barrier to entry due to some exceptionally strong networks working against 'outsiders'. The further development of these networks should be encouraged, with secondments, providing individuals at universities, such as the University of Kent, leading to productive long-term commercial relationships.

#### **3.4 Commercialisation Offices**

All universities interviewed for this study have a form of commercialisation office, though their application is varied. In general, they are very successful in commercialization. An example is the University of Oxford that recently attracted £300 million work of investment to its Mathematical,

---

<sup>7</sup> Hughes, A., 2008. Innovation policy as cargo cult: myth and reality in knowledge-led productivity growth. In: J. Bessant and T. Venables, eds., *Creating wealth from knowledge: Meeting the innovation challenge*.

<sup>8</sup> Select Committee on Science and Technology, 2013. *Bridging the valley of death : improving the commercialisation of research*. HC (Series) (Great Britain. Parliament. House of Commons). London: The Stationery Office.

Physical, Life Sciences and Medical Sciences Divisions to commercialise their work. Overall individual academics were happy with the work of their respective offices. Yet the lack of specialism outside of the scope of IT and computing may be neglecting the nuances and complexities of cyber security that could be enhanced. However some institutions may be unwittingly relying on key individuals as a driver for the majority of commercialisation. Therefore attempts to widen this base should be investigated.

## 4. Commercial Activity at UK Universities

### 4.1 Consultancy

Consultancy is the main avenue of commercial impact that universities offer. This is widely distributed across the ACE-CSRs, emerging from the development of 'hard' products and is often tied to IP. Achieving clear data for this is limited due to the lack of granularity in data collection in a broader categorization in IT and computing. Most academics have engaged in this form of commercialisation; either through university structures or on a private basis.

### 4.2 IP and Patents

Intellectual property is constantly being produced by universities and can be considered its *raison d'être*. However there was concern over the conflict in providing open-source solutions in cyber security in order to attain trust. One academic participant noted they would disregard most closed solutions. This is part of avoiding 'security by obscurity' due to a lack of verifiability that a solution is appropriate from closed solutions that may suffer from undisclosed vulnerabilities. This is in addition to the potentially limited financial gain and difficulty in attaining patents compared to conventional research funding, although this was not a widespread opinion. No patents at the ACE-CSRs were self-identified, although from information available on several of their websites, this is not likely to be representative. However the University of South Wales identified a patent filed on forensic imaging and acquisition<sup>9</sup>. There was concern however that in cyber security this is not a priority and this information is used as an indicator of commercialisation success, which does not accurately reflect the landscape.

### 4.3 Spin-Offs

Five universities self-identified as having spin-outs<sup>10</sup>. A key component of any successful spin-off is the personal dedication of individuals. This is due to the high level of personal commitment that has been given to a project, mainly through time dedicated in addition to their everyday university obligations. Some examples of these spin-outs are provided below:

- **University of Birmingham:** Creation of **CloudTomo**, a cloud security business which has attracted funding from Innovate UK among others, with support being provided by Alta Innovations, the university commercialisation office.
- **Queen's University Belfast:** The Centre for Secure Information Technologies, is one of the UK's Innovation and Knowledge Centres, being unique among ACE-CSRs. The centre has created 25 spin-outs, and has been extremely competitive for European and UK funding in doing so. In addition support exists for 'spin-in' companies to use incubator spaces to further develop with the support of CSIT. An example of a spin-out comes from **Titan IC Systems**, which recently received a £850,000 from Belfast-based investors<sup>11</sup>.

---

<sup>9</sup> <http://www.walesip.org/our-opportunities.htm?id=33>. Patent filed under GB1407605.3 Data Acquisition, 30/04/2014.

<sup>10</sup> These are Lancaster University; Queen's University Belfast; University of Birmingham; University of Kent; and the University of Surrey.

<sup>11</sup> <http://www.titanicsystems.com/>

- **University of Surrey:** Building on a long history of research in biometrics, Surrey formed a business with EPSRC and EU support. **OmniPerception**, was formed, acquired by Visimetrics, now part of Digital Barriers. Many PhD students from Surrey have now decided to have involvement of some form with this spin-out<sup>12</sup>.
- **University of Kent: Metarc** is a spin-out company from the University of Kent and the University of Essex developing encryption keys from the properties of digital systems. This is headquartered in Cambridge, but maintains research and development facilities at both universities.
- **Lancaster University: Quantum Base** is a spin-out that specialises in quantum security. Lancaster continues to further develop its relationship, using IAAs<sup>13</sup> as a mechanism to do this. They are part based at Lancaster's InfoLab21, a centre providing support for IT businesses.

Some universities are turning their attention to student entrepreneurialism, yet evidence of this is limited from this study, but should be further investigated. One university indicated the move in their TTO and wider commercial objectives to provide training for students and further support to develop any potential business ideas. The claim from one individual centred that students are often more likely to have time to commit, especially as graduates, and this was a core strategy they were developing.

#### 4.4 The Package

The formation of a package to offer to the market is an important component, where standalone products are unlikely to gain traction. This has led to a thematic allocation of funding, such as through Innovate UK. This thematic allocation develops confusion over what cyber security commercialisation involves, due to the integration with other products. In addition there is an imperative to combine 'hard' and 'soft' products, which participants suggested investors looked for. This is part of a conversation to sell the abilities of academics in consultancy, which are increasingly sought after with hard products. However the majority of commercialisation comes with this soft engagement: these forms should not be seen as subsidiary, they form a critical role.

### 5. Additional Challenges and Barriers

As common with the broader market, retention and pressures of progression impact on commercialisation within universities. However this is particularly pronounced in academia. This is seen in the tension in retaining early-career researchers in particular, who often hold critical knowledge on products and are necessary for continuity. A lack of bridging funding to support young researchers between projects on commercial ventures could be affecting some commercialisation. The pressing need to publish papers for post-doctoral researchers may also be leading to potential value from IP being lost. This is particularly tricky with an increase to publish in the open domain and is testing for TTOs.

The lack of measurable impact from commercial engagement for individual academics is, in part, affected by the indicators used by universities and research councils. Unlike expected outputs such as publications, as one participant was clear, attending 10 conferences may not lead to any significant output, but may generate the largest grant. Particular attention was attached to the Research Excellence Framework (REF), where academics are still strongly marked for research outputs, and is supported in other academic literature<sup>14</sup>. This embeds far more risk for universities

<sup>12</sup> <http://impact.ref.ac.uk/casestudies2/refservice.svc/GetCaseStudyPDF/40546>

<sup>13</sup> <http://www.lancaster.ac.uk/lec/business/case-studies/csr/case-studies/quantum-base/>

<sup>14</sup> D'Este, P. and Perkmann, M., 2011. Why do academics engage with industry? The entrepreneurial university and individual motivations. *The Journal of Technology Transfer*, 36(3), pp.316–339.

Winter, R.P. and O'Donohue, W., 2012. Academic identity tensions in the public university: Which values really matter? *Journal of Higher Education Policy and Management*, 34(6), pp.565–573.

and individual academics, which hold back from greater involvement in commercialisation outside of consultancy. This provided considerable frustration for commercialisation professionals to demonstrate the value of their work.

Driving growth through SMEs provided a varied response from universities. This was mostly on some naivety that these businesses may display. This requires education to some SMEs to align with academic interests and also in the opposite direction. Yet conventional engagements for business, such as KTPs are not appropriate for many small to medium enterprises, due to their significant cost. However SMEs were not a focus on this research and more work should explore this area.

## **6. Future Directions**

The Centre for Secure Information Technologies (CSIT) at Queen's University, Belfast provides the best example of the end-to-end innovation cycle. Yet this is likely only suitable for 'hard' product development – which generates clear and demonstrable impact. The links with London-based investment should also be further utilised. This is required to build a critical mass of expertise and capital in order to generate productive realisation of resources. Although this may face resistance from universities to retain their ability to control the commercial outputs of their research, there should be specialisation in cyber security. This centralization of knowledge is already occurring through organisations such as Crossword Cybersecurity<sup>15</sup> and the Academic Marketplace<sup>16</sup>. It is important to use networks already in place, such as by strengthening the ACE-CSR community and use this as a framework for supporting 'softer' commercialisation. It is clear that capital alone is unlikely to achieve genuine increase in output. Only be a package of targeted support is likely to have demonstrable impact.

## **7. Recommendations**

1. *Further engage with the Academic Centres for Excellence in Cyber Security Research (ACE-CSRs) to foster further community- building to encourage a centralised voice.*
2. *Consolidate expertise in academic research commercialisation in individual universities or as a collaboration between the ACE-CSRs.*
3. *Develop Impact Acceleration Account (IAA) use, with a potential central allocation of funds.*
4. *A centralisation of government support for the cyber security innovation ecosystem, with a recommended growth in the role of the ecosystem provided by Queen's University Belfast.*

---

<sup>15</sup> <http://crosswordcybersecurity.com/>

<sup>16</sup> <http://www.riscuk.org/academia/academic-marketplace/>