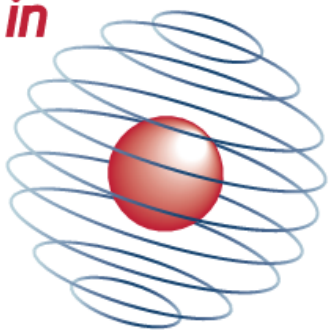
CENTRE *for* DOCTORAL TRAINING *in*
CYBER SECURITY



CDT Technical Paper

10/15

Academic cybersecurity research: best practice for commercialisation

Andrew Dwyer

Academic Cyber Security Research: Best Practice for Commercialisation

Andrew Dwyer
Centre for Doctoral Training in Cyber Security, University of Oxford

Abstract

This paper explores the interconnections between UK academic research in cyber security and commercialisation in the innovation landscape. This focuses on the Academic Centres for Excellence in Cyber Security Research (ACE-CSRs) that have been created at 13 UK universities. Through interviews with several ACE-CSRs and other stakeholders in the cyber security innovation environment, four recommendations are offered as potential areas for governments to enhance commercialisation in this area. These include further engagement with the ACE-CSR programme, consolidation of commercial knowledge, develop the use of Impact Acceleration Accounts and centralise government support on already successful centres.

Introduction

There are significant commercial relationships in cyber security by universities throughout the United Kingdom. Many are at an early stage and have not reached an appropriate level of maturity to achieve wide commercial success. This paper analyses both the extent of the current commercialisation practices and highlight best practice that UK universities are already engaged in. *Commercialisation* is defined as the transaction between a university, academic consortium, or academic(s) that attract surplus financial benefit of academic work in the market; whether through consultancy, patents, collaboration or a university spin-off/-out. This provides ample opportunity for universities to include their activities within this brief, presenting a fuller representation of the benefits of academia to the UK cyber security market.

Cyber security generates significant ambiguity between different groups that engage in the area. The UK Cyber Security Strategy does not provide a clear definition yet it can be defined as a collection of actions that protect a digital ecosystem including systems, humans, data and organisations according to user preference. This enables for a range of activities that may 'bundle' security into wider value-add packages rather than standalone products. The interdisciplinary focus of cyber security and growing pressure to commercialise produce inherent difficulties in identifying the total exploitation that academia may be conducting, limiting the paper's conclusions.

This research reveals there is significant commercial activity at UK universities, yet many are yet to engage beyond consultancy. Substantial interest is evident from university commercialisation arms to further exploit research, seeing this as a growth market. The Academic Centres for Excellence in Cyber Security Research (ACE-CSRs) are the prime foci of this paper. At the time of writing, many were less than four years old, some only recognised in the past year. Hence the centres are just reaching a maturity level where excellence in research can be translated into successful commercial activity.

This paper works through the methodology and a literature review of current research on UK university commercialisation in cyber security. This will continue through an exploration of the landscape; looking into consultancy, spin-outs and collaborations. Challenges and barriers to current commercialisation and future directions are highlighted to generate recommendations for commercial avenues in the future. These recommendations will include a call for greater use of the ACE-CSR framework and centralisation of some networks that cover the broader cyber security commercialisation lifecycle.

Background

The UK Cyber Security Strategy (UKCSS) (Cabinet Office, 2011) provided strategic

direction within government until 2015. Within this, 'Objective 4' (2011, p.21) provides the core direction, "The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives". This displays the importance to the UK government the commitment to contributing to the growth in size and versatility of the UK cyber security market through wide-ranging capabilities.

Within this period the Department for Business, Innovation and Skills (BIS), the Centre for the Protection of National Infrastructure (CPNI), Government Communications Headquarters (GCHQ), the Office of Cyber Security and Information Assurance (OCSIA) and Research Councils UK (RCUK) have funded the creation of 13 Academic Centres of Excellence in Cyber Security (ACE-CSRs). The scheme outlines three core aims on its website (EPSRC, 2015):

- Enhance the quality and scales of academic cyber security research and postgraduate training being undertaken in the UK.
- Make it easier for potential users of research to identify the best cyber security research and postgraduate training that the UK has to offer.
- Help to develop a shared vision and aims among the UK cyber security research community, inside and outside of academia.

The latter two aims promote commercial impact that this report is concerned. Four years since the scheme began, it is appropriate to assess the progression of these two aims in relation to exploitation of research in the wider market in response from interest from the Department of Business, Innovation and Skills. A Pierre Anderson Consultants' (2013) report commissioned by BIS in 2013 provided an overview to the UK Government on how it was performing according to its stated aims in the UKCSS. This revealed some wide variations in its success in fostering successful industrial-academic relationships. It is clear that the UK has a distinctive and vibrant academic community in universities that are globally recognised. It describes the ACE-CSRs as "a trend setter" (2013, p.60). Yet these centres, albeit worthwhile in university policy, have yet to gain traction in the innovation ecosystem with "some of [the] interviewees comment[ing] that universities are not aligned with business needs" (2013, p.61). These comments are common in the literature when innovations policies first gain traction from the 1990s (Sapienza, 1996; Hughes, Moore and Ulrichsen, 2011). A concluding remark states "BIS encourage[s] initiatives that foster relationships between academia and industry, such as CSIT at Queen's University Belfast, and seek to develop more" (2013, p.75). This paper emerges from this previous analysis as a critical area for the UK to develop in its cyber security capacity with a particular emphasis on the ACE-CSRs as an initiative that was created in response to the UKCSS.

Methodology and Reflections

18 interviews involving 29 individuals, including nine of the 13 ACE-CSRs[1], were held over an eight-week period from a range of stakeholders. These included academics, university commercialisation offices and those in the broader innovation ecosystem. The Department of Business, Innovation and Skills provided financial sponsorship of this study, including introductory contacts whom hold significant influence among universities and academics.

Participants formed a mixture of individuals and groups, according to the ability to gain access to the organisations. Due to time-constraints on a eight-week schedule, the format provided by participants was accepted. This included the locations where the interviews were conducted. Participants were in a significantly more powerful position (in cyber security commercialisation knowledge and position), so it is important to reflect on the dynamics through choices of

[1] The nine ACE-CSRs universities are: 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.

location, time and who was involved in the process. One of the interviews was held next to a Harrier jump jet (a British fighter jet). Was this to demonstrate the prowess of the organisation? It is definitely a spectacle for someone who is interested in the engineering of these aircraft! The mixture of introduced; a wooden chair, a faux leather sofa, varying quality of cups of tea, tours, flicking of eyes to a watch or clock, all seriously influenced this research.

To claim the researcher is solely powerless in this dynamic would be naïve. The sponsor, BIS, has significant funding implications for the universities involved, including future funding allocations. Participants expressed great interest over the purpose of the research: what was the intent? What was it going to be used for? Arriving from the University of Oxford influenced some universities: 'we' are an ACE-CSR, and still retain some forms of elitism in the public imagination; justified or not. A comment made outside of the formal interview concerned the privileging Russell Group institutions. This was a core consideration, though limited by scope to ACE-CSRs, to include institutions that fall out of this designation. The recent May 2015 election of a Conservative Party-majority government, also added to the swirling powers in this research. So, there may be certain omissions and highlights by the research participants that attempt to project powers to the interviewer (and its recipient audience, BIS).

Each interview followed a semi-structured format around core themes, to allow flexibility in each interview for in-depth and spontaneous avenues to be explored. In the interviews that were recorded, permission was explicitly granted from each individual and transcribed by the author. These were uploaded to NVivo© (version 10.2.0) where coding and cross analyses of transcripts were performed. Grounded theory was used as a way to draw conclusions from the data rather than through a priori assumptions being instilled from overly reading prior to engagement. Ciarán Dunne (2011) provides a critique to grounded theory that is used here. It is clear that the interviews required the development of good rapport and knowledge on the subject matter to gain the trust of participants. Therefore it is difficult to follow the initial methodological work of Glaser and Strauss (1967). It is impossible to somehow detach oneself as an 'outsider' to research following feminist and post-structuralist critiques (Clarke, 2003; Mills, Bonner and Francis, 2008; Wuest, 1995). Grounded theory is useful in reducing a priori assumptions to data, yet recognising that as a researcher, we are already implicated in the research process.

Being implicated in the research (re)constructs the world: regarded as 'impact', collaborating with BIS and engaging in the development of knowledge in the cyber security innovation landscape. Maintaining a critical awareness of how impact may be influencing society is crucial. Harmon, Caulfield and Joly (2012, p.8) state, "on the surface, these policy trends seem to create an untenable situation for the academic research community, and various scholars have argued that the pressure to commercialize conflicts directly with the idea of free exchange of scientific knowledge." They continue that a balance is necessary, providing a narrow definition of medical commercialisation focused on patents and licences, which can be easily applied to cyber security. This paper takes a broader commercialisation proposition detailed in the introduction, embracing diversity of opinion within academia in its approach, and exploring the tensions that can exist in commercialisation.

During the initial stages of this research, no clear commercial practices or processes were assumed. This altered the direction of the interviews, including planned commercial process mapping to compare alternative pathways between universities. This developed on 'strategic roadmapping' used by Kapletia, Felici and Wainwright (2014) was not used due to its inapplicability in the current academic context. The following paper outlines insights from these interviews, drawing on themes that emerged during this process following the questions below.

- Assess the current commercialisation landscape for cyber security in both

industry and academia, including the broader policy environment.
- 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.
- 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.

University Commercialisation Research

"UK Policy is characterised by a systemic process involving a number of initiatives designed to increase the capacity of universities to respond to the needs of business, public services, and the wider community, and to transfer knowledge" (Wright and Filatotchev, 2014, p.258)

The 'third' stream emerged during the 1990s as an alternative to block grants to universities, and competitive research grants (first and second streams respectively). Hughes, Moore and Ulrichsen (2011, p.79) state "third stream activity refers to those activities that seek to engage more directly with users to exchange knowledge, including contract or collaborative research, spin-outs and licensing activity, personnel exchange, training courses and joint curriculum development, as well as social regeneration, public outreach, the provision of public arts and musical events and school-based activities." This transformation was explicitly detailed in 1999 with the Higher Education Reach-Out to Business and the Community (HEROBC). The authors assert that through the third stream, "the knowledge captured within HEIs [Higher Education Institutes] is only of economic use if it can be exploited by organizations and individuals external to the organization" (2011, p.83). This may assert the need for greater commercial activity but may neglect the nuances that universities can play as individual actors, and their relationships within wider ecosystems. The argument is supported by Connell and Probert (2010, p.95) where universities are "important contributors to the wealth of the region [Cambridge], but the relationship with technology-based firms is often less direct than is assumed by government policymakers." This is critical to understanding the relationships between academia and industry in commercialisation. In addition they provide critique to assumptions where: 1) it is research that is the key source of technology and innovation; 2) venture capital as the primary source of funding, and; 3) co-funding multi-partner collaborative research is the best way government can support technology development projects. These three points come through in the research and are discussed later, particularly around point two.

In this critical piece on understanding the UK innovation ecosystem, Connell and Probert (2010) develop their work around the 'Cambridge Phenomenon'. There are some critical observations on technology innovation, which are also pertinent to cyber security. Nearly all leading players in software and ICT started with a 'soft' model. The 'soft' model involves consulting or R&D contracts for customers rather than the development of technologies with 'hard' properties that are more readily patentable. In addition they respect some of the particular risks that ICT and software start-ups may have. Though it may be easier than some other disciplines, such as physics or engineering, due to shorter development timescales. This view is supported in their study, where entrepreneurs believe consultancies are responsible for the development of the cluster rather than the University of Cambridge. Interestingly they comment, "venture capital funding may be a distraction to start-up firms in this sector" (2010, p.48). Hence, they highlight a mismatch in emphasis by innovators and government policy.

Commercialisation Offices

Concurrent to third stream of funding, there has been a growth in universities with Technology Transfer Offices (TTOs) or associated commercialisation offices. These were created in order to improve the exploitation of academic research. The advantage is their ability to be "able to benefit

from [their] capacity to pool the inventions across research units and build a reputation within universities" (Sharifi, Liu, McCaul and Kehoe, 2008, p.343). In the first comprehensive analysis of their role, the Lambert Review (2003) was critical of their efficacy in generating value for money. In particular it stated deficiencies in Intellectual Property (IP) commercialisation where the lack of quality in provision lead to divergent outcomes (Sharifi et al., 2008; Perkmann et al., 2013). A lack of engagement from UK business came from a lack of value attached to the research produced by universities (Breznitz, 2014). Connell and Probert (2010, p.91) felt universities locked-down their IP rights and therefore undermined cooperation; claiming this was due to TTOs "staffed by non-scientific and/or non-commercial people who do not understand the complexities of the science and/or the commercial situation." This is countered by this research, where some universities demonstrate a high degree of specialism, and it seems at least some universities have responded to the criticism. Yet in Wright and Filatotchev's (2014, p.243) study on King's College London Enterprise (KCLE), one must respect some the difficulties in commercialisation for these offices where budgets are difficult to manage due to the "lumpy and unpredictable" nature of the environment.

Spin-off

The creation of a *spin-off* (or *spin-out*) is the clearest indication of university commercialisation, yet providing definitive stand-alone cyber security ventures is problematic. Their development "is a complex process, involving diffusion of basic research and its ultimate commercialization" (Sharifi et al., 2008, p.338). Much of this requires individual dedication (Perkmann et al., 2013) that may lead to the success or failure and is currently underrepresented in literature in this area. There have been frequent accusations of overvaluation (Wright and Filatotchev, 2014), not dissimilar to arguments around IP. Wright and Filatochev claim the public sector origin of university funding can create problems when later attempting to raise subsequent funding. This mixture of IP and spin-offs causes difficulties in creating commercial success.

Environment

For a positive commercial outcome, the operating innovation environment is a key determinant of the likelihood of success. The current UK environment worries Hughes (2008, p.80). He notes there is "a danger today that the evolution of innovation policy structures based on copying perceived cultural characteristics and structures of the US innovation system will also fail to deliver the goods." This attracted discussion during this research with mixed opinions over its applicability due to differences in venture capital. Further critique is mounted by the Select Committee on Science and Technology in the UK House of Commons (2013, p.9) on the linearity of commercialisation. They particularly single out Knowledge Transfer Partnerships (KTPs), where the interchange of ideas and feedback loops are not well understood. One key UK Act of Parliament transformed the early operating environment, the UK Patent Act 1997 (Wright and Filatotchev, 2014, p.258). This aided clarification for universities in relationships with academics, where they commonly own the work produced. Yet is not enforced by all. It is worth noting that the innovation landscape is not concerned solely with commercialisation, being far less common than other, softer forms of engagement (Hughes, Moore and Ulrichsen, 2011; Perkmann et al., 2013) which are core to the academia's impact on society.

Academic Cyber Security Commercialisation Research

There is precious little research on cyber security and the innovation landscape. Those that have concern the United States providing no direct comparison to the UK. This is particularly so with academic cyber security research. Maughan *et al*. (2013, p.16) on TTOs claim "some institutions have offices and programs dedicated to support licensing and ventures, many show remarkably little interest in supporting technology transition, and any success is typically the result of extremely dedicated researchers' efforts." Their paper concerns 'hard' products in the

US with discussion on 'soft' elements is restricted. Although there is discussion around specific intermediate R&D institutes and centres such as the US MinTech, there are no analyses of institutional methods to improve commercialisation. Some authors such as Bauer and van Eeten (2009, p.707), claim that "cyber security policy needs to start from a clear and empirically grounded understanding of the nature of the problems before possible solutions can be devised." Although in principle this sounds appropriate logic, the rapidly changing cyber security environment needs a far more flexible approach to developing policy.

The 'Valley of Death' is common in cyber security commercialisation research (Kapletia, Felici and Wainwright, 2014; Select Committee on Science and Technology, 2013). The claim is as follows; cyber security start-ups achieve certain maturity and then find it difficult to fund or exploit their products to scale, hence entering the 'valley'. These authors argue it has certain benefits with commercially attractive ventures likely to attract funding. Governments must be aware of over-funding to strike a balance, maintaining appropriate funding that does not restrict potentially successful ventures, but does not waste capital on those unlikely to prosper. NASA Technology Readiness Levels (TRLs) (Mai, 2015) are regularly appropriated for technology commercialisation: adapted for use in European Horizon 2020 (European Commission, 2015). Kapletia, Felici and Wainwright (2014, p.143) state in their preparatory analysis of the UK innovation ecosystem that "it is clear that measures must be taken to ensure that investments in promising cyber security and privacy technologies survive the valley of death and are given the opportunity to deliver high value impact." Therefore an appropriate level of financing is required, but must be applied cautiously. This report aims to articulate some avenues of exploration in this area, providing some initial work from the perspective of UK universities and academics on cyber security commercialisation.

Current UK University Commercialisation Landscape in Cyber Security

There have been significant collaborative and educational engagements made by UK universities for the past 20-30 years. A significant development was the first MSc in Information Security launched in 1992 by Royal Holloway, University of London (Ciechanowicz, Martin, Piper and Robshaw, 2003). The ACE-CSRs are a later critical contribution through their work with industry. This was recognised by all participants indicating clear benefits as a community and increased industrial collaboration. The initial centres were formed in 2012 after the first assessment round in 2011. There were subsequent calls in 2012 and 2014 for the current funding stream ending 2017. Many centres have therefore had limited time to generate relationships before productive work can begin. This led one participant to claim "*four years is not enough.*" This is likely to be accurate statement for many institutions, especially those aiming to produce high-quality collaborative research.

> *"Nothing will just arise, I don't think anything will arise naturally because we're an ACE except that it's extra credibility that industry might look at and say we'll go to [here] because you know, they obviously have some critical mass there but that is going to be quite… is slow."*

The above sentiment was widespread, with financial support totaling up to £20,000 in the latest 2014 round. This raised concerns over the ability of these centres to independently launch sustainable commercial relationships. However there are centres outside of the ACE programme who were keen to demonstrate their abilities to commercialise. These focused research on thematic issues, with one claiming "*people don't speak to security centres in particular but go to specialist centres in niche areas*". This thematic organisation is already prevalent in ACE-CSRs, and therefore as other universities have independently developed in this way, should be continued.

Cyber security has gained high-profile media awareness in the past 18 months with attacks on Sony Pictures and Target (a US department

chain). This, along with several government initiatives such as Cyber Essentials, have increased the demand for cyber security products and services and will continue to do so. The UK market is expected to increase to £3.4bn by 2017 (Pierre Anderson Consultants, 2013). Yet in regard to commercialisation, the UK is perceived to be lagging behind the US in terms of the ability to go to market. There is praise that Andy Williams is Cyber Security Envoy at the British Embassy in the US to gain access to this large market. This increase in awareness was explained explicitly: "*we're getting charities, insurance companies, recruitment agents. All these we would never have seen before are getting worried, so the market is only going to get more [sic].*"

During interviewing, concerns were raised over the difficulty in 'selling' and the classification of cyber security. The thematic nature of the emerging discipline, leads to integration with other areas and products, restricting the ability for a distinctive cyber security market to emerge. Innovate UK provides an example of this movement:

> "*The aim is not to build here another firewall, another algorithm. It's here to take some of those best practices and ideas that sit in industry and research and take it to a particular industry. So for example, I get people focused on an industry business model, it could be automated cars, it could be manufacturing, or it could be, erm, supply chain for sportswear for example whereby you know, data flows between those are open to attack.*"

This is common to computing, yet the multidisciplinarity of the area causes confusion among commercialisation arms. Is a product or service to be classified as 'cyber security' or not? Therefore even if data is recorded, it may exclude substantial amounts of quality cyber security research output by academia. This is complicated by perceptions of 'unique' clients defining the market. Defence and intelligence agencies are seen as the prime market for some participants, whilst for others this is minimal. These discrepancies between cyber security knowledge and commercial practices in the academic environment, warrants this paper's wide definitions and focus on experience rather than providing data sets.

Funding

Many participants believed "*most cyber security companies have an insignificant revenue stream – [and] don't have capabilities to grow fast enough*". Some were concerned over the ability of private finance to provide early-stage ventures adequate funding. It is suggested venture capitalists are moving away from 'risky' investments to higher maturity levels. There was further pointed critique at government funding of research, such as by the Engineering and Physical Sciences Research Council (EPSRC). Yet this is currently allocated via the dual support system, which is part of the block grant to universities from central government. Therefore this was not considered for this report.

Impact Acceleration Accounts (IAAs) were credited by ACE-CSRs and their respective commercialisation arms as being extremely successful in enabling them to develop the commercial potential of 'hard' products. EPSRC provides grants of £600,000 to £6 million to individual UK universities to assist in promoting academic impact, incorporating commercialisation. These are processed locally by universities and vary in their application. Two examples come from the University of Surrey and Lancaster University. Surrey issues up to £20,000 for each successful application, where subsequent additional applications can be made. Lancaster uses the funding in a two-stage process; the first stage as a funded feasibility study, a second stage as funded research likely to enter a KTP. Many of these engage an external industrial partner in order to gain funding as per the requirements of that institution. However the involvement of Small and Medium Enterprises (SMEs) were seen to be flexible but are often "*firefighting*", making engagement difficult for universities. IAAs are extremely beneficial when "*there is no money... it becomes harder to justify from an investor so that often becomes a very strong case for government investment*" and therefore government assistance is sometimes required to develop

the maturity before it becomes attractive to the market.

Location

Although not anticipated at the start of the study, the issue of location became a theme for many interviews; in both developing relationships and where the market is located. This was particularly the case for universities outside of the 'South-East triangle'. One participant stated that "*outside of London, Oxford and Cambridge it is much harder*" to commercialise cyber security. Another is frustrated at the focus on the London area:

> "*It doesn't have to be in London. Everything happens in London but there's [others] outside of London, and there is growing technology outside of London and it's never accepted by governments and big organisations in London!*"

An increasing awareness of the importance on clustering in promoting community and commercialisation opportunity was promoted. The focus on having innovation hubs, incubators and other schemes for promoting growth all detailed the criticality of location and the need to be among a mix of different individuals. This was acknowledged in an interview discussing the 'Cambridge Phenomenon' where the essential element to its success was crystallised by "*attitude, critical mass, and intelligence.*" More interviews developed the idea of an 'ecosystem' approach without which it would be difficult to commercialise any products; in cyber security or not. For one university in particular, plugging into an ecosystem around Bristol and Gloucester was a critical growth area. This demonstrates that although cyber security is 'online', like other digital technologies, geography is still an important asset for commercial engagements, witnessed in the growth of campuses for large internet businesses (see Graham (1998) for a broader perspective).

Commercialisation Offices

During this research, it became evident that many universities are doing very well at cyber security commercialisation whilst others are less mature in their development. In general UK universities are successful in many disciplines, with Lancaster University winning the Small Business Charter Gold Award in 2014 for its work with SMEs, and the University of Oxford winning £300 million worth of investment to commercialise activity in its Mathematical, Physical, Life Science Division and Medical Sciences Divisions. This interest in commercialisation was noted by participants to have been particularly inspired by the increase in importance of 'impact' in the Research Excellence Framework (REF). This increased commercial activity from academics that wish to demonstrate their research 'impact'. Attitudes towards these offices from academics were wholly positive, in contrast to much literature on these offices. One said; "*as an academic... I find we have a research, business support team who are fantastic.*"

Yet commercialisation offices did not receive the same warm reception from those external to universities with concerns over their ability to produce additional value. This criticism is targeted at the lack of individual expertise in cyber security in order to comprehend implications for industry. This led, according to some interviews (both within and outside universities) to an overvaluation of IP, and one that is unlikely to ever be fully resolved. This problem is exacerbated by the dependence on key individuals within research groups in cyber security to hinge commercial activity. This is clear in several interviews, with two explicitly naming academics with whom they work, potentially causing problems in the lateral application of commercial activity. Due to high applications of energy required to develop commercial relationships and work with academics, this is not unsurprising. Key contacts are sources of information and development in many organisations outside of academia. An example was provided by one individual:

> "*You know you might expect a TTO [Technology Transfer Office] tech transfer person to be able to go in there and uncover things and this is not this type of culture here, you know, it's a kind of group that is already plugging straight into industry, they are selling their services to industry*"

Dependence on key individuals is exasperated by the organisational structure of many commercialisation offices. A large amount of independence is still given to academics to develop their career and research direction. Many commercialisation arms enable academics to develop relationships and use these without the involvement of them, where they are an optional service academics may wish to use, with the University of Cambridge the classic example of this arrangement.

There are positive drivers for cyber security commercialisation in the UK market for universities, particularly in the creation of the ACE-CSRs. Strong market forces are driving further consumption of cyber security products and expertise from academia provides ample opportunity. Though warning signs in the current practices exist. This includes a perceived lack of specialism and knowledge in commercialisation offices, an increasing concentration of activity that encourages commercialisation in London and the South-East, and a movement to more mature propositions.

Networks

> *"The only way you're going to get business-critical interest is you have to have a very strong collaborative link, it's probably long established. Good will and a reciprocity and understanding the sensitivities involved and I think a lot of it is about getting, undertaking that journey erm… such that you have confidence on both."*

This is evident in engagement with SMEs. Universities should not offer a *"brochure, why don't you try and be a bit smarter with the way you protect yourself?"* There is greater acknowledgement by universities for partnership and meaningful engagement. A 'team' of specialists who can work together to attract venture capital investments, or to position products is essential. An example is the University of South Wales (not an ACE-CSR), in the administration of the Tiger scheme, a cyber security professional certification in penetration testing. This has enabled detailed knowledge of cyber security to lead to a fruitful collaborative approach with its Information Security Research Group.

A desire to strengthen community groups within cyber security is clear, being broadly supported by participants. In particular, some see the ACE-CSR initiative as a platform to provide a 'single voice' for cyber security academics and should be further developed. Wider groups of government bodies such as the Ministry of Defence (MoD) and industry, such as QinetiQ, are also attempting to form their own networks. The 'Academic Marketplace' has been recently created where academics can post their research along with commercial intention in a cyber security stream that is freely accessible. This has been created by the UK's Security and Resilience Industrial Supplier's Community (RISC). At the time of writing, there were two universities who had academics with projects highlighted: the University of Birmingham and Queen's University Belfast.

Government and large primes were seen favourably by many due to their understanding of university processes, contracting and the agreed flexibility that is common in their discussions. DTSL and the MoD were noted for their flexibility in IP for students to be involved on sometimes confidential work. Common between government and large business are well-known processes, even if contracts get stuck in the "*bowls of the legal department*" according to one commercialisation professional. This levelling of expectation is critical to their work and is not as common in SME relationships. Large industry partners also have the ability to fund postdocs, engage in KTPs, and are more likely to offer secondments. Secondments are seen as a key component for engagement for those who had engaged in this way. Although a form of indirect commercialisation, the relationships developed here seem to have a positive impact on the cyber security commercial landscape for the universities and individuals involved. A highlighted example by one university was the use of a Royal Society Industrial Fellowship which has led to much follow on collaboration and consultancy work.

Bodies such as Innovate UK (formerly the Technology Strategy Board) is well received by interviewees from a variety of

backgrounds. Although there is a capped rate 30% that can be tendered for by a research organisation, it is critical that "*you can't have new innovation without having a basic research coming from it, you know, it's kind of plucking an idea of the sky, you know, without any fundamental research.*" Critically, funding is provided through grants with little or no restriction, ensuring IP is retained in the partnership, an attractive avenue for further cyber security academic exploitation. SMEs are increasingly involved with 'clusters', the majority through the UK Cyber Security Forum; a body championing issues for SMEs. Individual clusters have different foci, whether it be awareness, education or primarily pursuing a growth agenda such as the North West Cyber Security cluster. This clustering, regardless of background or future trajectory, provides universities and SMEs a conduit in which to engage with one another and is a positive development.

Incubators and Accelerators

There are multiple incubators and accelerators in the UK. A common theme is the ability to generate a porosity of 'borders' in developing commercial work. One participant claimed that for its pre-accelerator and incubator to work it "*has to be central, accessible and where people work*". This openness is seen at Queen's University Belfast, at the Centre for Secure Information Technologies, demonstrating an impressive amount of incubation space for start-ups. They claim this is an essential part of commercialisation to engender an entrepreneurial spirit. A critical core component of any incubator's remit is building community as "*it helps to stimulate commercial activity... [and] itself is not as a whole process in which you do community-building.*"

Only one incubator, Queen's University was visited in this research, which has dedicated academic space for cyber security. Others such as CyLon and SetSquared do offer similar activities but are not primarily arenas for academic research. CyLon is a new accelerator for cyber security, created by investors in London, aiming to plug the 'gap' in the 'valley' to spur small start-ups to speed up their growth. Yet there was criticism of its value for all areas of cyber security:

> "*You know that's the one condition you get £5000 [per founder] in all and your CEO basically has to be based there. It's like it's really expensive to live in London in Hammersmith and you're a small company starting up first of all you have to be away from your team and you have to be in London.*"

Its stated intention is "to assist founders in building commercial businesses that deliver outstanding information security technology" (CyLon, 2015). The SetSquared partnership is a collaboration between the universities of Bath, Bristol, Surrey, Southampton and Exeter. This is co-funded by HEFCE and Innovate UK in a £3.2 million 'ICURe' project: however this is primarily for local businesses rather than for university spin-outs and not exclusively for cyber security.

Current Commercial Activity at UK Universities

Consultancy is the main avenue of commercial impact that universities have to offer. There is healthy activity at all UK ACE-CSRs that were sampled. This is widely recognised as the widest-spread activity that academics have in direct commercialisation, but achieving clear data for cyber security is difficult due to variations in data collection. The majority of consultancy occurs as a result of personal initiative and remains on a private basis. Therefore data is partial and unlikely to be at a level of granularity where cyber security activity can be identified. Often consultancy emerges from the development of 'hard' products, offering services on implementation and operation. Hence, an interdependency exists in the cyber security ecosystem, with many academics preferring consulting over spin-offs, due to the reduced personal commitment required.

IP is consistently produced by universities, with only some of this leading to a commercial output; with much shared publically through reports, journals and other forms of publication. The public nature of IP raised concern from some academics on restricting this to the commercial domain. One concern is the stifling of innovation that may occur,

especially in patent development. This reticence is displayed by one participant:

"If somebody did patent a really good encryption algorithm, well how you say you do it in cryptography the result of it is that it stifles its use as it is encumbered by patents and people look for those without patents so, yeah, I don't know what to make of all of that."

For much of the area, cyber security needs to be open in order to verify its credentials as being 'secure'. This is part of the principle of 'security by obscurity' (see more on this topic from Hoepman and Jacobs (2007)) that is avoided due to the perception that it does not lead to an appropriate form of protection.

"Yeah open access, er open source is very, very important and as security people we probably quite rightly, so just disregard any or most of the closed solutions."

Other concerns were raised by academics on patent applications and intellectual property development, where little gain is likely compared to the input required. Yet commercial arms see value of these applications in generating commercial and reputational value for the university; however they may be overvaluing this.

"Universities tend to value their IP too highly you know, they got an idea, yay! The hard bit is getting it commercialised so you can't think your idea is worth loads and loads and loads as it actually hasn't got across the chasm yet."

Tensions were voiced by an academic need to publish papers for credibility *vis-à-vis* commercialisation, especially for early-career researchers. This complicates work for commercialisation offices.

"Two things there. One, are you destroying a patent by publishing it? Which is quite easy to do. And second, which aspects of the patents we do like to treat as confidential."

Yet, regardless of this, patents are being produced at ACE-CSRs. However this is not exclusive, with the University of South Wales developing on a PhD thesis on disk copying where a patent has been filed. Yet there is realisation that:

"*Over the years we more successfully commercialise software than the patents in commercialisation but the government generally is more interested in funding patents."*

The Package

The creation of a package is a critical component for university commercialisation. There is an increasing market expectation for applications and products to have 'built-in' cyber security. This is recognised by Innovate UK, who base funding allocations according to thematic problems. Interweaving into other higher-level attributes demonstrates an expanding sector but is increasing the difficulty for policy-makers to identify and support commercialisation. Participants explained the pressing requirement to sell integrated cyber security products, with others noting that standalone products may have been successful in the past, but this is unlikely to be so in the future. This adds pressure to combine 'hard' and 'soft' university products.

"The thing which investors look for, and they're looking for a hard [product], and I think that is what makes it difficult it is because a lot of cyber security people do more consultancy based the majority of are actually implementations and project management."

This is also seen in conversations how to sell 'academics' in an environment where 'soft' skills in consultancy are tied to demonstrable 'hard' product development:

"How do you package a consultant for an external collaborator is often that discussion"

Understanding how to improve the 'package' offered is key to increasing any form of engagement. This led to participants reiterating the need for education on commercialisation specific to cyber security, rather than general training already on offer by university commercialisation offices.

Queen's University, Belfast

The university hosts the Centre for Secure Information Technologies (CSIT): the UK's Innovation and Knowledge Centre (IKC). This specialises in innovation, including groups of engineers that quickly assemble and test products from academic research or from other external partners. Products are developed beyond the abilities of many other universities. Its industry collaboration forms tiers of involvement where a 'prime' can gain access to it strategic advisory board for £30,000.

"We did it so we do not need to that money because it's a drop in the bucket. [What] we need is someone to make a decision that they had to get value back and also there's more of a commitment on that person."

CSIT also engages with SMEs at a lower cost to gain access to the centre's activities and leverage its reputation. Core to this is the open access to IP generated. There is:

"Open access to all of our IP, we have source code repositories that they can just download stuff and there are no more NDAs [Non-Disclosure Agreements]."

There is an attempt to bridge the 'Valley of Death' through provision for academics to approach CSIT and access broad-based support across both technical and commercial domains. It also makes use of IAAs and private financing demonstrating good use of the existing ecosystem to provide an iterative innovation system with appropriate feedback mechanisms.

University of Surrey

Prior to being recognised as an ACE-CSR in 2015 a substantial body of research existed. This includes the Secure Voting System developed for the Victoria Electoral Commission in Australia where a long lead-in for a commercial relationship is required:

"There was a long lead time for those kind of issues and you know they did want reliability and trust and in terms of all the kind of acceptance testing and sending it out for review."

In contrast to more general cyber security commercialisation this is:

"More a team thing and connections as to whether it's going to be useful and less of a technology based thing. I think the secure voting thing is a bit of an exception actually as that will very much depend on the reputation of the people who has developed it, we're getting back to the people aren't we? Back to the people."

Highlighting this particular case shows the importance people and contacts, especially where this engagement is international. In addition, GeoLang a Welsh-based business won TechUK's 'Most Innovation Cyber Security Company' award. This was facilitated through research with Surrey that led to two patent filings. This demonstrates the work that universities can do with funding from Innovate UK in collaboration with business. Even though this is not a 'direct' commercialisation, this form of university engagement is essential.

Spinning-off

"If you look at the spin-offs and start-ups which universities have, [it is] a really good model... work with a commercial partner to commercial fruition, because if it stays in academia and never hits industry then I don't see the point."

Five universities self-identified as having spin-offs [2] . Commercialisation arms and offices provide critical support networks for academics. This primarily is administrative support, an advice network and links to industry contacts. Those academics who have spun-off have positive attitudes to the support offered. Yet there are significant obstacles that on reflection are seen to be necessary. These are not the greatest hurdles for academics but developing an effective business plan was far more challenging for example.

[2] These are Lancaster University; Queen's University Belfast; University of Birmingham; University of Kent; University of Surrey.

A key element for spin-offs is the team of individuals who can succeed in the market. This normally requires a senior academic who spearheads the team for academic credibility; yet the time demand is often too high for serious engagement. This concern was raised by a senior academic who may potentially spin-off:

"At the moment it has been taking up a lot of my time, erm and it's clear that I'm not able to put the increased amount of time that's needed for a kind of whatever start-up company and I want to be involved. I want to stay involved but in terms of doing a lot of the running around and checking things out, that still needs to be more junior people or other participants."

Focus has been enabling academics to commercialise, but there is a growing interest in students and graduates. This is not surprising due to the large amount of entrepreneurial activity in the student population, where in 2014, over 4,600 spin-offs were created by graduates compared to under 400 elsewhere (Higher Education Statistics Agency, 2014). The perception that students are more motivated is generating this, yet in cyber security there is little evidence this is happening.

Concerns over the 'Valley of Death' were exposed in this area. The lack of early-stage funding before a prototype or proof of concept could be developed is worrying as the majority of funding only appears during higher levels of maturity. This supports previous done by Wright et al. (2006) on understanding the relationship between venture capital and spin-offs in the UK. Some participants believed venture capitalists are entering later, when risk is lower. However if funding is secured, it is a significant boost and a form of assurance for external partners.

Challenges and Barriers to Commercialisation

There is worry over a lack of cyber security specialists in commercialisation arms; where nuances are being missed amidst wider knowledge in IT and computing. This was tied to broader support for academics with informal support underrated in funding mechanisms. Another barrier to long-term innovation lifecycle management is in the ability of universities to retain academics. Though this is a broader organisational difficulty, this is accentuated by dominant academics in commercialisation, where a departure of a key individual can have a severe adverse impact. In addition, research contracts can be fragmented, leading to a loss in junior researchers with critical knowledge on a product, further complicating continuity.

"If you're just employing people for research contracts, research contract, that you know is going to be gaps between and you're going to lose people so you, you need that buy-in from faculty to actually to say we commit to this and we will bridge funding."

Hence, there is a real risk without bridge funding, that some commercial opportunities may be squandered.

Relationships with industry can be problematic, due to unpredictable return and instability of income. Many large enterprises do not require universities, as many have their own large research centres. Therefore exploiting niche capability at UK universities is needed, but does demonstrate vulnerability. The disparity in university engagement metrics between academic research and commercialisation is also troublesome:

"You've probably got to go to 10 conferences, it's a lot of effort for no guaranteed return. It's not like writing a research grant, which has no guarantee, but I think there's an acceptance within the institution that, that is an output and a metric that is understood as an institution. Whereas going to 10 conferences which actually in the end net the biggest grant, collaboratively that may ever come out of it, they don't see it that way, institutional metrics, national, are problematic."

Forging fruitful commercial outputs is different to outcomes expected of academics. Whilst academics may be entering the community, commercialisation offices may find this difficult due to a potentially closed community that can often stifle commercial

activity. One university noted how it is difficult to refine products for this reason.

"It's a really closing community and they go over to the sort of conferences in Europe and everyone knows everyone, you know?"

Small-Medium Enterprises (SMEs)

SME engagement offers a diverse response among universities, especially on the naivety some display.

"If they're naïve that they've never dealt with the university before, there is a bit of an education as to what, how university operates and what our protocols are and match that and that's what comes with the territory."

This research did not engage directly with SMEs, but concerns over alignment with academia and commercial benefit were indicated. SMEs are unlikely to offer universities what some large enterprises do; such as capital and pathways for student employment. Yet engagement is improving compared to the past. KTPs are a key initiative to support industrial collaborations through Innovate UK. These can cost £18,000 to £21,000 and are seen as far too high for the small size of many cyber security businesses in the UK. Therefore engagement with SMEs more generally may need review, but are out of scope for this report.

Academics are prime drivers of commercialisation in universities, due to the large degree of freedom they are given.

"I would say largely it's driven by an academic or group of academics or students, erm, that wish to see their thoughts go into the public domain whatever that may be, erm, and it's usually because they want to see the utility of engaging with third parties and user community."

Though this is a highly positive for academia, it does mean that unlike elsewhere in the innovation ecosystem, it is far more fragmented. This leaves personal commitment as central to development of commercial relations. Products developed outside of formal university-allocated time is common due to this. Those who had been engaged in a form of spinning-off noted that time was at an extreme premium and in tension with university requirements, more so than any other form of commercialisation.

There is scepticism over translation of funding into successful commercial activity. One barrier is a lack of institutional understanding:

"It annoys me all the time over the years, but they don't understand the fact that actually buying for work with industry is just as valuable as buying time out for research but the commercial stuff is seen as more of a risk. I'm not sure it is more of a risk because if research funding ends, commercial funding ends and it is still finger in the air to whether you are going to get anymore."

The Research Excellence Framework (REF) is an additional important driver in the commercialisation landscape for universities and academics.

"At the end of the day academics are still marked against much more strongly for research outputs which includes patents and grants."

These drivers are well documented in other research (D'Este and Perkmann, 2011; Winter and O'Donohue, 2012) with a lack of perceived guarantee in commercialisation is a major concern. This has organically led to key individuals at universities, with academics not previously attempting commercial exploitation finding the process burdensome. Yet this is not a deficiency, as the barrier sifts those likely to be successful to come forward and are likely to bridge the 'Valley of Death.'

Future Directions

CSIT at Queen's University is the best example of end-to-end innovation lifecycle coverage in the UK as part of an iterative commercialisation process. The success in Belfast is being extended:

"Belfast is kind of an engineering engine and CyLon is like the front-facing... bringing those potential investors."

This growth is to be praised. Yet other universities are likely to develop their own

similar initiatives that could likely flood the ecosystem, diluting any positive impacts of having fewer, well utilised streams of engagement for academics and universities. London is fast-becoming the hub, with an investor network, symbolised by the opening of a European Office by Paladin Capital Group (a Washington-based private equity group).

Participants were anxious over scalability of resources in establishing maturity from early-stage development; particularly referencing venture capitalists. Yet this chasm has lessened with government funding including IAAs and Innovate UK projects. There is appetite to expand the IAA scheme, and perhaps develop a similar programme for cyber security in particular. However there is disagreement over whether this should be administered locally or centrally. IAAs are key to developing early-stage ideas and should remain flexible to foster success (and failure if it is clear commercialisation is unlikely).

The lack of critical mass at universities has generated support for some pooling of resources. This includes a centre as a base for consulting, a test-bed for development, or perhaps a central area for information and contact for academic research; yet this may face resistance from universities. Centralisation of knowledge on cyber security commercialisation is already happening; such as through the Academic Marketplace and the work being conducted by Crossword Cybersecurity in detailing academic projects in in the UK and further afield. A suggestion by a participant to increase student enterprise should be further explored, enabling all cyber security PhD students an opportunity to have an industrial placement would be beneficial, similar in outlook to the Centres for Doctoral Training in Cyber Security.

Engagement and fostering of expertise should focus on using current structures in place; the ACE-CSRs and the IKC at Queen's University Belfast. Engaging universities that may not be part of the programmes would be beneficial to create an integrated network. The recognition of ACE-CSRs should be utilised through further developing community. This can be a focal point for communication and collaboration, not only benefiting commercialisation but other forms of engagement. The annual ACE- CSR conference would be a good location for further collaboration. As one participant noted:

"a relationship with industry, industrial partners, industrial groups and they sit around a table and tell you this is the real problem and getting to that stage and that really does engage the academics and because whether it's on a speculative normal funding output you've got that in the back of your mind, you know, you've got some context."

It is clear from each interview that providing capital alone is unlikely to succeed due to comparatively lower levels of funding in comparison to large research grants. Therefore a package of funding, with specific cyber security commercialisation and advice are likely to interest academics and universities.

Conclusions

This paper has analysed a wide variety of academic cyber security research commercialisation in the UK. Though this is at different levels of maturity among ACE-CSRs; the most significant commercial activity is consultancy, along with significant collaborative outside this study's remit. Best practice currently resides at Queen's University Belfast in supporting end-to-end innovation support. This paper does not provide a complete analysis of activity in the UK, but offers insights from particular individuals. Due to data limitations, data was not collected as accurate conclusions are unlikely to be attained.

The ACE-CSR programme is in its infancy due to the limited time to develop productive commercial relationships. If further acceleration of commercialisation is desired then this may require limited additional funding to utilise current structures as outlined in the recommendations. Commercialisation will happen regardless, and continue to accelerate due to wider

market conditions; but is unlikely to fulfil its potential without assistance.

Development of a pathway for academics would be the most beneficial output of this research, due to the limited entry points for industry to engage with academics and the limited ability of universities to provide cyber security specialists. This should follow on from initiatives such as the Academic Marketplace in order to facilitate relationships at relative low-cost. This also includes using CSIT at Queen's University Belfast as a clear avenue for academics to engage with, especially on 'hard' products, instead of attempting to recreate an already successful centre elsewhere. This addresses some concerns of a concentration in London by being based in Northern Ireland, whilst also providing a focal point for investors in London to complete the innovation lifecycle.

Successful commercialisation requires strong personal and community bonds, and though encouraging academics is warranted, only those who seek to come through some institutional barriers are likely to succeed. Some resistance can be productive. Those likely to cross the 'Valley of Death', existing in the UK as much as the US, is due to the determination of the individual academics (or students) involved. Therefore a strengthening of community in the ACE-CSRs is to be encouraged to gain a single voice and greater strategic direction for the university cyber security sector.

Recommendations

- *Further engage with the Academic Centres for Excellence in Cyber Security Research (ACE-CSRs) to foster further community-building to encourage a centralised voice.*

- *Consolidate expertise in academic research commercialisation in individual universities or as a collaboration between the ACE-CSRs.*

- *Develop Impact Acceleration Account (IAA) use, with a potential central allocation of funds.*

- *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.*

Acknowledgements

This research was sponsored by the Department for Business, Innovation and Skills and received ethics approval from the University of Oxford Social Science and Humanities Research Ethics Committee (reference: SSD/CUREC1A/15-052).

Bibliography

Bauer, J.M. and van Eeten, M.J.G., 2009. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, [online] 33(10–11), pp.706–719. Available at: <http://www.sciencedirect.com/science/article/pii/S0308596109000986>.

Breznitz, S., 2014. The Fountain of Knowledge: The Role of Universities in Economic Development. Stanford University Press, pp.41 – 59.

Cabinet Office, 2011. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. [online] Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> [Accessed 3 May 2015].

Ciechanowicz, C., Martin, K.M., Piper, F.C. and Robshaw, M.J.B., 2003. Ten years of information security masters programmes. In: *Security education and critical infrastructures*. Springer, pp.215–230.

Clarke, A.E., 2003. Situational analyses: Grounded theory mapping after the postmodern turn. *Symbolic interaction*, 26(4), pp.553–576.

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

CyLon, 2015. *CyLon Accelerator*. [online] Available at: <https://cylonlab.com/> [Accessed 26 Jun. 2015].

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.

Dunne, C., 2011. The place of the literature review in grounded theory research. *International Journal of Social Research Methodology*, 14(2), pp.111–124.

EPSRC, 2015. *Academic Centres of Excellence in Cyber Security Research - EPSRC website*. [online] Available at: <https://www.epsrc.ac.uk/research/centres/acecybersecurity/> [Accessed 4 May 2015].

European Commission, 2015. *Horizon 2020*. [online] Available at: <https://ec.europa.eu/programmes/horizon2020/> [Accessed 8 Jun. 2015].

Glaser, B. and Strauss, A., 1967. The discovery of grounded theory. 1967. *Aldin, New York*.

Graham, S., 1998. The end of geography or the explosion of place? Conceptualizing space, place and information technology. *Progress in Human Geography* , [online] 22 (2), pp.165–185. Available at: <http://phg.sagepub.com/content/22/2/165.abstract>.

Harmon, S.H.E., Caulfield, T. and Joly, Y., 2012. Commercialization versus open science: Making sense of the message(s) in the bottle. *Medical Law International* , [online] 12 (1), pp.3–10. Available at: <http://mli.sagepub.com/content/12/1/3.abstract>.

Higher Education Statistics Agency, 2014. *HESA - Higher Education Statistics Agency - HESA - Higher Education Statistics Agency*. [online] Available at: <https://www.hesa.ac.uk/pr202> [Accessed 26 Jun. 2015].

Hoepman, J.-H. and Jacobs, B., 2007. Increased security through open source. *Communications of the ACM*, 50(1), pp.79–83.

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*.

Hughes, A., Moore, B. and Ulrichsen, T., 2011. Evaluating Innovation Policies: A Case Study of the Impact of Third Stream Funding in the English Higher Education Sector. *Science and Innovation Policy for the New Knowledge Economy*, pp.79 – 105.

Kapletia, D., Felici, M. and Wainwright, N., 2014. An integrated framework for innovation management in cyber security and privacy. In: *Cyber Security and Privacy*. Springer, pp.135–147.

Mai, T., 2015. Technology Readiness Level. [online] Available at: <https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html> [Accessed 8 Jun. 2015].

Maughan, D., Balenson, D., Lindqvist, U. and Tudor, Z., 2013. Crossing the 'Valley of Death': Transitioning Cybersecurity Research into Practice. *Security & Privacy, IEEE*, 11(2), pp.14–23.

Mills, J., Bonner, A. and Francis, K., 2008. The development of constructivist grounded theory. *International journal of qualitative methods*, 5(1), pp.25–35.

Perkmann, M., Tartari, V., McKelvey, M., Autio, E., Broström, A., D'Este, P., Fini, R., Geuna, A., Grimaldi, R., Hughes, A., Krabel, S., Kitson, M., Llerena, P., Lissoni, F., Salter, A. and Sobrero, M., 2013. Academic engagement and commercialisation: A review of the literature on university–industry relations. *Research Policy*, [online] 42(2), pp.423–442. Available at: <http://www.sciencedirect.com/science/article/pii/S0048733312002235>.

Pierre Anderson Consultants, 2013. *Competitve analysis of the UK cyber security sector*. London.

Sapienza, A., 1996. Knowledge Frontiers: Public Sector Research and Industrial Innovation in Biotechnology, Engineering Ceramics, and Parallel Computing. *R&D Management*, 26(1), p.93.

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.

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.

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.

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.

Wright, M., Lockett, A., Clarysse, B. and Binks, M., 2006. University spin-out companies and venture capital. *Research policy*, 35(4), pp.481–501.

Wuest, J., 1995. Feminist Grounded Theory: An Exploration of the Congruency and Tensions between Two Traditions in Knowledge Discovery. *Qualitative Health Research* , [online] 5 (1), pp.125–137. Available at: <http://qhr.sagepub.com/content/5/1/125.abstract>.