THE FUTURE OF RESEARCH AND DEVELOPMENT IN THE UK'S SECURITY AND INTELLIGENCE SECTOR

Charlie Edwards and Calum Jeffray

RUSI
www.rusi.org

Royal United Services Institute

OCCASIONAL PAPER

About the Paper

Research and development continues to be a national priority for the UK government as part of its long-term strategy to increase innovation and skills within technology and knowledge-based industries. Yet at a time when technological advantage is critical within the security and intelligence spheres, sufficient and targeted investment in appropriate R&D programmes is far from guaranteed. Ahead of the 2015 Strategic Defence and Security Review, the aim of this paper is to explore whether there are ways to improve engagement between government and investors operating in this sector, in order to ensure that R&D investment is strengthened, priority capabilities are understood by investors, and critical capabilities are sustained.

The authors are very grateful to Global Strategies Group and, in particular, Damian Perl and Tim Matthews for their invaluable support. Thank you also to RUSI colleagues Adrian Johnson and Harry Wood.

About the programme

National Security and Resilience (NSR) Studies at RUSI is the only programme of its kind in the British think tank community. The programme focuses on five research areas: terrorism, organised crime, resilience and emergency management, cyber-security and intelligence. Established in 2004, NSR conducts a broad range of research, advisory and consultancy services for policy-makers and practitioners in the UK, Europe, North America, the Middle East and Africa. The team includes academics, former policy-makers, practitioners (with operational experience), and researchers who deploy an evidence-based approach to research to improve policy- and decision-making.

About RUSI

The Royal United Services Institute is the UK's leading independent think tank on international defence and security. Its mission is to be an analytical research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Annual membership subscriptions and donations are a key source of funding for the Institute; together with revenue from publications and conferences, RUSI has sustained its political independence for over 180 years.

RUSI is a registered charity (No. 210639).

www.rusi.org

Occasional Paper, March 2015

The Future of Research and Development in the UK's Security and Intelligence Sector

Charlie Edwards and Calum Jeffray

www.rusi.org

The views expressed in this paper are the authors' own, and do not necessarily reflect those of RUSI or any other institutions with which the authors are associated.

Comments pertaining to this report are invited and should be forwarded to:

Charlie Edwards, Director of National Security and Resilience Studies, Royal United Services Institute, Whitehall, London, SW1A 2ET, United Kingdom, or via e-mail to charliee@rusi.org

www.rusi.org/publications

The Future of R&D in the UK's Security and Intelligence Sector

While security and intelligence agencies require a technological edge over their adversaries, developing truly innovative and disruptive technologies is rarely easy or straightforward. Research and development (R&D) is costly and can take years or even decades to generate final outputs which align with the particular requirements of a set of end-users. While R&D is historically the most-cited metric of innovation in an economy,[1] investment on R&D in the UK has been in steady decline over the last thirty years. In 2012 – the most recent year for which figures are available – R&D amounted to 1.72 per cent of UK GDP; this is down from the around 2 per cent mark sustained in the late 1980s, lower than the 2.06 per cent average for the EU, and far short of government's target to have increased UK R&D investment to 2.5 per cent of GDP by 2014.[2]

The UK government maintains an annual ring-fenced science and research budget of £4.6 billion, yet this does not necessarily apply to the security and defence sectors, where there has been a dramatic reduction in budgets since the 2010 Strategic Defence and Security Review (SDSR). Spending in this sector fell faster than in any other area of government between 2011 and 2013, and expenditure on R&D has slumped compared with the private sector.[3] This has led to a widespread belief that current levels of funding for R&D activities in this sector are insufficient.

This is problematic in the area of national security where operational priorities often necessitate innovation that is fast and responsive to the needs of the security and intelligence agencies without disproportionate financial burden. The agencies face an ever-more diverse range of technically competent adversaries, yet have less control than ever over the development of new technologies, which today is predominantly driven by consumer demand rather than government priorities.

The UK has a flourishing private technology sector, often based in clusters such as London's 'Silicon Roundabout'. Yet many start-up companies and small and medium-sized enterprises (SMEs) continue to find it difficult to secure appropriate funding and support from investors in order to develop their concepts into capabilities (crossing the so-called 'valley of death'). In

1. National Audit Office, *Research and Development funding for science and technology in the UK*, Memorandum for the House of Commons Science and Technology Committee, June 2013, p. 7.
2. ONS, 'UK Gross Domestic Expenditure on Research and Development, 2012', *Statistical Bulletin*, Office for National Statistics, <http://www.ons.gov.uk/ons/dcp171778_355583.pdf> accessed 3 November 2014, p. 3.
3. "Defence Spending Hit the Hardest", *Financial Times,* 8 September 2014.

June 2014, *The Economist* reported that employment in London's technology and information businesses had grown by 11 per cent since 2009, and while funding from venture-capital firms tripled to $1.2 billion in the last financial year, competition for capital has become ever-fiercer.[4]

The government and the agencies have recently taken notable steps to increase their level of transparency and open up the market to a broader range of young and technically adept SMEs; the Government Communications Headquarters (GCHQ), for instance, has developed an SME-engagement strategy and has begun to run open calls for innovative proposals, under the broad headings of 'finding the threat' and 'working securely in insecure environments'. There remain, however, significant obstacles to linking government requirements for national security with innovation and emerging capabilities within the private sector. R&D in security and intelligence capabilities suffers from a number of market failures, including the inherent tension between a fast-moving technology market and a slow-moving government bureaucracy, and the secret and sensitive nature of the work of the security and intelligence agencies. As a result, industry is unable to communicate with its end-users, ascertain their capabilities and requirements or focus its R&D efforts appropriately.

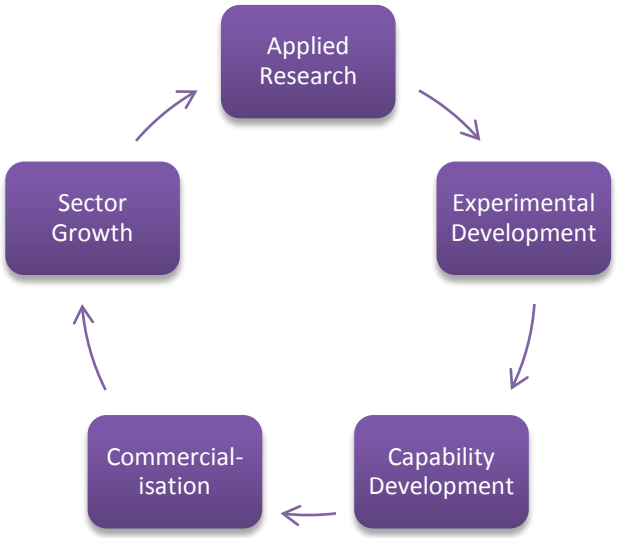
The Importance of an Innovation 'Ecosystem'

Similar to many other countries, the UK's framework for innovation is elaborate, involving financial and non-financial collaboration between a multitude of different stakeholders, including businesses; higher education and other research institutions; national laboratories; business support organisations; government departments and policy-makers; business lenders and funding agencies; private investment firms; and innovation infrastructure bodies.

These various stakeholders and organisations function within an innovation 'ecosystem', whose success relies on each of its components operating effectively, as shown in Figure 1. For example, product design and development depend on relevant applied research taking place further upstream, and investment for research in specific areas is only likely to take place if there is potential for economic growth and opportunities downstream. In order for there to be high levels of innovation within this system, therefore, there must be suitable levels of funding at each stage of the process and the system must function as a unit. If one component ceases to perform, all other parts of the ecosystem are affected and the conditions for innovation become suboptimal, generating barriers to growth.

4. "Jammin' in the capital", *Economist*, 21 June 2014.

Figure 1: Feedback Loop within the Innovation Ecosystem



The government has made it clear that 'achieving operational advantage over potential adversaries depends on investment in technology',[5] and there has never been a greater need for technological innovation within this ecosystem to enable the security and intelligence agencies to counter a range of increasingly diverse and global threats. Significant challenges exist however – both specific to the national security domain and more generally – that currently hinder the sector's ability to sustain a healthy and dynamic ecosystem that can develop disruptive technologies to aid national-security efforts. For example, there is a long way to go before the UK security sector is seen as an attractive market for private investors, given the persistent culture of secrecy, government inefficiencies and a high level of uncertainty over future procurement and adoption trends.

Ahead of the coming 2015 SDSR and renewal of the National Security Strategy (NSS), this report explores the UK's R&D roadmap to 2020 and beyond in order to identify market failures that can be corrected and inefficiencies that can be addressed – such as the scale of investment by private firms and the level of R&D collaboration between the agencies, industry and private investment firms. It is not intended to criticise current government efforts in this area, nor does it focus solely on innovation policies that help businesses cross the valley of death (while these may be successful in bringing some innovations into the commercial sphere, there is no guarantee that the innovation ecosystem will thrive as a result). The report's ultimate aim is to explore

5. Ministry of Defence, *National Security through Technology: Technology, Equipment and Support for UK Defence and Security*, Cm8278 (London: Stationery Office, 2012), p. 33.

whether there are ways to improve engagement between government, private investors and industry operating in this sector, in order to ensure that R&D investment is strengthened, priority capabilities are understood by investors and critical capabilities are sustained.

Key Questions

- Does the government and its agencies know what their requirements are, what capabilities they plan to develop internally, and what they expect to procure from the private sector?

- Is there a need to stimulate R&D investment in this sector from private investors such as venture capital and private-equity firms? If so, how?

- As technology is developed over ever-shorter time horizons, is there too much of a focus on fulfilling short-term capability gaps, to the detriment of developing long-term disruptive technology?

I. Technology and Innovation in the UK Risk Environment

The UK has a long history of using science and technology to aid national security efforts. From the code-breakers at Bletchley Park during the Second World War to counter-terrorism surveillance operations today, the security and intelligence services have relied on new and emerging technology to counter existing threats, gaining a reputation for excellence in R&D and innovation in the process. Traditionally, much of the 'big science' and most cutting-edge R&D work in security and intelligence was undertaken by these and other public-sector institutions, funded by government departments. This centralised approach saw government possess leading knowledge and capabilities, which it could then distribute to close industry partners if it so wished.

Since the end of the Cold War, and in particular following the rapid evolution of information and communication technology (ICT) in the 1990s, there have been two fundamental changes in the relationship between national security and R&D. As the R&D capabilities of industry have grown, private-sector expertise now outstrips that of government in many areas, particularly in fields such as ICT. The commercial ICT sector has become one of the biggest industries in the UK – as in many developed countries. The scale of R&D in the private sector now far exceeds that of the public sector, with this gap likely only to increase with time. As a consequence, government may no longer find itself at the cutting-edge of much emerging ICT; hi-tech products are more readily available to the public and government has less control over the pace of technology development than ever before.

Second, the UK faces an increasingly capable and diverse range of threats. The National Risk Register notes that these threats include, among others, terrorist attacks; chemical, biological, radiological and nuclear attacks; the spread of pandemic viruses; organised crime; and cyber-attacks on critical national infrastructure (CNI). The NSS identifies technology as a key driver of many of these threats, and emphasises that, in the future, both state and non-state actors will have access to a greater range of technology which can be used both to protect and attack national security.[1] It also describes how 'in an age of uncertainty, we need to be able to act quickly and effectively to address new and evolving threats to our security'.[2]

1. HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Cm7953 (London: Stationery Office, October 2010), p. 16.
2. *Ibid.*, p. 5.

Technology as a Threat

Both the NSS and the Ministry of Defence's (MoD) White Paper *National Security through Technology* acknowledge that the capabilities of the UK's adversaries will increase as technology becomes more sophisticated and readily available. The MoD notes that the threat will emanate from:[3]

> ...not only sophisticated military weapons, but also greater innovative and ingenious application of readily available civil technologies. Where adversaries can more easily buy high-technology products on the open market, this potentially reduces our operational advantages.

In the NSS, meanwhile, the government predicts that 'the pace of scientific and technological innovation is likely to continue to increase' and 'technological knowledge will spread more widely and more rapidly than before'. As a result, 'the advantage that the West has traditionally enjoyed in technology is likely to be eroded'.[4]

A first major trajectory of this threat comes from hostile actors such as terrorists and organised criminals exploiting commercially available technology to further their aims. For instance, the rise in the use of the Internet and social media has made it easier to spread violent extremist ideology and propaganda, thus aiding recruitment and fundraising efforts. It has also helped operational planning, providing groups with the means to more securely research and identify targets, equipment and methods in order to achieve more lethal effects. Similarly, organised criminal groups have learned how to exploit the Internet to commit cyber-enabled crimes such as fraud, theft, extortion and child sexual exploitation.

Another major threat trajectory is the way in which such actors exploit the increasing dependence of the UK's CNI, government services and businesses on ICT, and particularly the Internet. The NSS ranks cyber attacks on these systems by other states, organised criminals and terrorists as a Tier 1 national security risk. The UK Cyber Security Strategy reminds us that 'key data and systems on which we now rely can be compromised or damaged, in ways that are hard to detect or defend against', and that 'events in cyberspace can happen at immense speed, outstripping traditional responses'.[5]

One of the biggest intelligence leaks in recent times is a further reminder of how the agencies' capabilities and technology may be used against them. The revelations by the National Security Agency (NSA) contractor Edward Snowden disclosed many of the tools and techniques used by agencies such

3. Ministry of Defence, *National Security through Technology*, p. 8.
4. HM Government, *A Strong Britain in an Age of Uncertainty*, p. 16.
5. Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: Stationery Office, November 2011), pp. 5, 7.

as GCHQ to combat the threats the UK faces online and elsewhere. The revelations have made the job of the intelligence agency much harder, in the view of former chief Sir Iain Lobban, as criminals and terrorists have adapted and diversified their own methods having learned those of the agency; what used to take GCHQ's Internet Ops Centre two weeks to accomplish now takes six weeks.[6]

In summary, much of the potential threat derives from three factors: the 'democratisation' of science and technology, which puts more information and capability in the hands of small groups and individuals; the proliferation of new technology, which provides hostile actors with an increasing choice of weapons; and the pace of change in many technological domains, which may exceed the speed with which law enforcement and the security agencies can respond.[7]

Technology as a Solution

While technology is a major component of many national-security threats, it also plays a key role in combating these threats. The contribution it makes is recognised by a wide range of government documents, including the NSS, SDSR, National Risk Register, Serious and Organised Crime Strategy, National Cyber Security Strategy and the counter-terrorism strategy (CONTEST). According to the Home Office, 'Success in delivering relevant science, innovation and technology is vital to the delivery of CONTEST. Science and technology impacts every area of the strategy'.[8]

The Office for Security and Counter Terrorism (OSCT) within the Home Office co-ordinates cross-government work in science and technology to aid national-security efforts. These include areas such as countering terrorism through improving the ability of law enforcement to 'pursue terrorists, prevent radicalisation, protect essential services and infrastructure and prepare for a terrorist attack'.[9] Perhaps the biggest contribution that science and technology can make to national-security efforts, however, is intelligence. Intelligence collection and analysis are technology-intensive activities, requiring increasingly sophisticated methods to filter, sort and analyse ever-growing volumes of communications data.

This presents a clear challenge for the security and intelligence agencies. Given the rapid evolution in technology, there is more pressure for them to conduct R&D and develop more sophisticated capabilities than those of their

6. Charles Moore, "GCHQ: 'This is not Blitz Britain. We sure as hell can't lick terrorism on our own'", *Daily Telegraph*, 11 Oct 2014.
7. Ministry of Defence, *National Security through Technology,* p. 4.
8. Home Office, *The United Kingdom's Science and Technology Strategy for Countering International Terrorism* (London: The Stationery Office, August 2009), p. 3.
9. *Ibid.*, p. i.

adversaries, over much-shorter time horizons. One academic highlights this challenge in the context of counter-terrorism:[10]

> The asymmetry here is clear enough: not only must a national counterterrorist strategy be able to respond and innovate across a broader spectrum than terrorists require to be successful, it must also do so as rapidly as, if not more rapidly than, terrorists.

According to the MoD, to stay ahead of hostile actors there is a need for both superior technology (so-called 'operational advantage') and the ability to operate, maintain and refresh certain capabilities effectively, without being dependent on others (so-called 'freedom of action').[11] Achieving these is likely to necessitate investment in a multitude of capabilities, given uncertainties over whether a particular capability will ultimately prove valuable and how long the technology will remain relevant in an ever-changing technical environment. This will be very hard to achieve without the innovation, resources and expertise of the private sector.

To fully leverage this innovation requires closing the gap between the R&D efforts of the public and private sectors; closer alignment is needed to prevent agencies experiencing an 'IT gap' caused by the speed of change and innovation in the commercial high-technology sector. Since the development of technologies is iterative and achieved by the gradual evolution of capabilities, research continuity and funding stability are essential.[12] The provision of suitable systems of finance that support innovation and growth within the security and intelligence sector is far from obvious, however, particularly within the context of the UK's complex and disjointed R&D funding landscape.

10. Paul Cornish, 'Technology, Strategy and Counterterrorism', *International Affairs* (Vol. 86, No. 4, 2010), p. 885.
11. Ministry of Defence, *National Security through Technology,* p. 14.
12. Evidence submitted by ADS to the House of Commons Science and Technology Committee enquiry, 'Bridging the Valley of Death: Improving the Commercialisation of Research', Eighth Report of Session 2012/13, March 2013.

II. The Context of R&D in the UK

Investment in security- and intelligence-related R&D must be placed in the context of the UK's R&D framework as a whole, since many of the current challenges are not necessarily specific to this sector. Declining investment, a comparatively low capacity to develop and commercialise products, and a multiplication of the types of organisations both funding and undertaking R&D activities are all general challenges to UK R&D.

The R&D landscape in the UK, as in many other countries, is complex, involving funding and implementation by a broad range of government, business, higher-education and not-for-profit stakeholders. Table 1 illustrates the separation between the types of organisations funding R&D, and the types of organisations carrying out R&D.

Table 1: Sectors which Fund or Carry Out Research and Development

Sectors Funding R&D	Sectors Undertaking R&D
UK Business Entities whose primary activity is the market production of goods or services (other than higher education) for sale to the general public at an economically significant price.[a]	**UK Business** (See left)
Overseas Institutions and individuals located outside the political borders of a country and all international organisations (except UK business) including facilities and operations within the country's borders. It includes funding from public and private entities overseas as well as the European Commission.	**Overseas** Institutions and individuals located outside the political borders of a country and all international organisations (except UK business) including facilities and operations within the country's borders.
Private Non-Profit Non-market, private non-profit institutions serving the general public, such as charities. They provide individual or collective services without charge or at prices that are not economically significant.	**Private Non-Profit** (See left)
Government All departments, offices and other bodies which provide services to the community (other than higher education) which cannot otherwise be conveniently and economically provided. In the UK, it is made up of government departments and agencies, higher-education funding bodies and research councils.	**Public Research Institutions** All departments, offices and other bodies which provide services to the community (other than higher education) which cannot otherwise be conveniently and economically provided. In the UK, it is primarily made up of government departments and agencies .

Sectors Funding R&D	Sectors Undertaking R&D
	Higher Education Institutions All universities, colleges of technology and other institutions of post-secondary education, as well as entities administered by, or associated with, higher education institutions.

[a] Prices are economically significant when they have an impact on the amount suppliers are willing to provide or customers are willing to purchase.

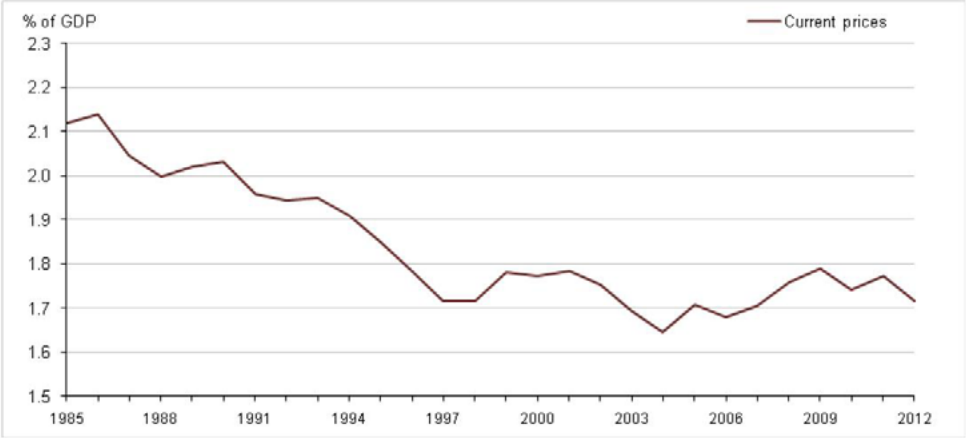
Source: National Audit Office, *Research and Development Funding for Science and Technology in the UK*, p. 11.

Responsibility for overall research and innovation policy in the UK lies with the Department for Business, Innovation and Skills (BIS), which publishes an annual Innovation Strategy. The 2014 strategy notes that 'Leading national innovation systems perform well across a broad range of system metrics, including excellence of research systems, intellectual assets and linkages and entrepreneurship', though it recognised that 'UK expenditure on R&D as a share of GDP remains behind many of the world's other major economic powers'.[1] According to figures from the Organisation for Economic Co-operation and Development (OECD), in 2011 the US continued to be the world's largest performer of both public and private R&D (accounting for approximately 32 per cent of the total global spend), followed by China (16 per cent) and Japan (12 per cent). The UK ranked seventh, with 3 per cent, amounting to £27.4 billion.[2]

The Office for National Statistics (ONS) publishes an annual statistical bulletin tracking gross UK domestic expenditure on R&D.[3] In 2012, the most recent year for which data are available, total R&D expenditure represented 1.72 per cent of UK GDP, a decrease from 1.77 per cent in 2011.[4] This figure falls short of the EU average provisional estimate of 2.06 per cent of GDP; BIS targets within previous strategies to raise UK R&D investment to 2.5 per cent of GDP by 2014; and the recommendation of the BIS Select Committee in December 2014 for the government to commit to a 3 per cent target of GDP in R&D investment by 2020.[5] Figure 2 demonstrates how expenditure as a percentage of GDP has, in fact, been in overall decline since 1985.

1. BIS, 'Innovation Report 2014: Innovation, Research and Growth', March 2014, p. 3.
2. *Ibid.*, p. 19.
3. Details of the methodology used to calculate these figures are available at <http://www.ons.gov.uk/ons/guide-method/method-quality/quality/quality-information/business-and-energy/gross-domestic-expenditure.pdf>.
4. Office for National Statistics, *Statistical Bulletin,* p. 3.
5. House of Commons Business, Innovation and Skills Committee, *Business-University Collaboration*, Seventh Report of Session 2014-15, HC 249 (London: Stationery Office, December 2014)

Figure 2: UK Gross Expenditure on R&D as a Percentage of GDP, 1985–2012



Source: Office for National Statistics, 'UK Gross Domestic Expenditure on Research and Development, 2012', Statistical Bulletin, <http://www.ons.gov.uk/ons/dcp171778_355583.pdf> accessed 3 November 2014, p. 4.

Partly as a response to this declining trend, in 2013 the House of Commons Science and Technology Committee (STC) requested that the National Audit Office (NAO) examine R&D spending in the UK since 1995, particularly in comparison with other countries. The subsequent NAO report found that the trend within the UK was away from governmental funding of R&D programmes towards instead providing industry and the private sector with incentives to undertake R&D themselves. In summary, it concluded that 'the government has progressively reduced the amount it spends on undertaking R&D itself, but at the same time, has increased the funding it provides to UK business'.[6] Tax incentives are an example of this support, whereby companies that are subject to UK corporation tax can reduce their tax bills by a proportion of their revenue spending on R&D.[7]

This shift from 'direct' to 'indirect' government investment is illustrated by figures which show a 19 per cent reduction (£559 million in real terms) in the R&D undertaken by public research institutions between 1995 and 2011. While funding for R&D in the government sector declined, government departments' funding to UK business over the same period increased by £255 million (19 per cent). It is noteworthy, however, that the 34 per cent growth in R&D performed by UK business over this period was primarily financed by UK business itself and from overseas, with real-term increases of £2.8 billion (30 per cent) and £1.3 billion (51 per cent) respectively.[8]

6. National Audit Office, *Research and Development Funding for Science and Technology in the UK,* p. 7.
7. *Ibid.*, p. 27.
8. *Ibid.*, p. 21.

The dominance of private-sector R&D is also highlighted by BIS, which notes that 'The business sector is the largest performer of R&D in the UK, accounting for approximately two-thirds of [gross expenditure research and development]'.[9] The NAO agrees with these figures, stating that '64 per cent of the R&D undertaken in the UK in 2011 was by UK business, largely financed by UK business itself, which contributed to 69 per cent of the sector's overall funding'.[10] It also notes, however, that 'UK spending on R&D is concentrated in a small number of very large firms'.[11]

Research versus Development

BIS consistently highlights the UK's strong international reputation in applied research, claiming 'Our research base is well rounded and impactful across most major research fields and is demonstrably world-leading with high and rising research quality, despite increasing competition from emerging powers'.[12] Elsewhere, it boasts that:[13]

> With four of the world's top ten universities, and more Nobel prizes per capita than any other large nation, the UK punches well above its weight in terms of its research excellence. Only a handful of countries can compete with us in terms of the strength, breadth and depth of our scientific activities...

The STC also describes the country's academic research as 'the jewel in the crown of UK innovation activity'.[14]

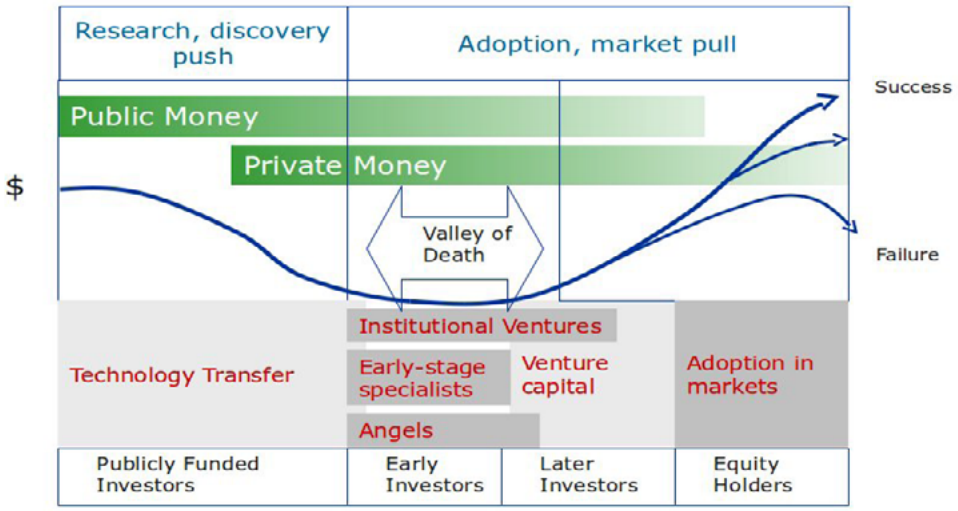
The challenge for government is how this world-class academic research can be translated into capability development and commercial outputs, particularly if they align with national-security interests. A range of both government and industry commentators the authors spoke to recognised the past failure to exploit this research base, and there was consensus that the UK's strength lies more in the research than the development aspect of R&D.

While there is latent potential in this regard, one of the biggest hurdles the UK faces is how to fund companies in their growth stage of development, and commercialise the innovations they produce. This problem is commonly

9. BIS, *Innovation Report 2014*, p. 23.
10. National Audit Office, *Research and Development Funding for Science and Technology in the UK*, p. 8.
11. *Ibid.*, p. 8.
12. BIS, *Innovation Report 2014*, p. i.
13. BIS, *Creating the Future: A 2020 Vision for Science and Research*, consultation on proposals for long-term capital investment in science and research, Department for Business, Innovation and Skills, April 2014, p. 12.
14. House of Commons Science and Technology Committee, *Bridging the Valley of Death: Improving the Commercialisation of Research*, Eighth Report of Session 2012/13, HC348 (London: Stationery Office, March 2013), p. 4.

referred to as the valley of death, describing the point where a business experiences an expertise and/or funding gap, which prevents the progress of an idea or proof of concept to the point where it provides the basis of a commercially successful product or business (Figure 3).[15]

Figure 3: Illustration of the Concept of the Valley of Death



The concept of the valley of death is an issue which is considered to particularly affect the technology sector. As previously noted, the ICT sector is one of the UK's fastest-growing industries. 'Software, IT and telecoms services together generated 4.2% of UK gross value added in 2011 and provided 885,000 jobs', claims Innovate UK (formerly the Technology Strategy Board) in its 2014/15 Delivery Plan. 'We have 107,000 software businesses, and are the world's number two exporter of telecoms services (£5.4bn) and number three in computer services (£7.1bn) and information services (£2bn)'.[16]

In August 2014 Simon Segars, chief executive of Arm Holdings, applauded the rise of digital entrepreneurialism and the number of new technology companies being created in the UK, but lamented the current lack of capital available for their growth stage.[17] Small businesses and start-ups experience the valley of death and the barriers to commercialisation more keenly, since they are thought typically to be driving high-technology innovation but without the capital needed to transform ideas into commercial products. Not only are small companies unable to secure funding for product development, but in Segars's opinion this funding shortfall also makes them more likely to sell early rather than stay independent.

15. *Ibid.* pp. 3, 87.
16. Technology Strategy Board, *Delivery Plan: Financial Year 2014-15*, <https://www.gov.uk/government/publications/innovate-uk-delivery-plan-2014-to-2015> accessed 3 November 2014, p. 56.
17. "Arm chief laments lack of capital for start-ups", *Financial Times,* 19 August 2014.

This situation has not been helped by the post-2007 economic downturn. Evidence submitted to the 2013 STC report 'Bridging the Valley of Death: Improving the Commercialisation of Research' suggested that a business such as Arm would not obtain the venture capital investment it received in the 1990s in today's financial environment, without which it might have failed to become one of the world's leading computer chip manufacturers.[18]

The UK government is aware of the problems encountered by small businesses in light of the recession, recognising that 'a small but important minority of innovative, growth-oriented businesses continue to face difficulties in attracting funding'.[19] It is important to distinguish between small start-up companies and more established medium-sized enterprises in terms of the extent of their skills, the maturity of their capabilities and the subsequent support needed to support their growth. The government's innovation policy therefore offers several tools and support mechanisms to such businesses, which are increasingly consolidated within Innovate UK. The mission of this agency is to:[20]

> ...promote the role of government as 'lead customer' for business – articulating problems and challenges, engaging with business to find solutions, and providing a route to market. The main tool for this is SBRI (the Small Business Research Initiative), which since 2009 has provided more than 1,500 contracts, helping small companies to develop new products and services.

The general consensus within industry is that Innovate UK's different support mechanisms are valuable and play a vital role in the early development stages of innovation, although it is too early to evaluate its success since many of its initiatives were only recently established. An initial assessment was provided in 2013 by the STC, which raised concerns about 'the access of small firms to large scale test and experimental production facilities', and while it praised initiatives such as the SBRI, it also noted that these 'lack sufficient funds to meet the demand from companies'.[21] Demand for public-sector grant funding is high, and it is an enticing prospect for small technology companies given that it does not require any loss of equity.

18. House of Commons Science and Technology Committee, *Bridging the Valley of Death*, p. 11.
19. HM Treasury, *Bridging the finance gap: A Consultation on Improving Access to Growth Capital for Small Businesses* (London: Stationery Office, December 2003), p. 5.
20. Technology Strategy Board, *Delivery Plan,* p. 8.
21. House of Commons Science & Technology Committee, *Bridging the Valley of Death,* p. 3–4.

The Role of Private Investors

There are disadvantages to public-sector funding, however. Aside from being highly competitive, small businesses in particular find the application process highly bureaucratic, and the resultant sums of money tend to be relatively small compared with investments made in the commercial sector. A more traditional route for start-up companies to cross the valley of death is to seek capital from private investors such as venture capitalists, private-equity firms and business angels. While capital of this nature is usually acquired by exchanging equity, investments can be much more significant.

The different types of private investors have varying strengths and, as demonstrated in Table 2, are typically involved in different stages in the growth of companies and the process of capability development. At the most basic level, business angels are often the source of the earliest forms of investment, venture-capital firms focus on developing products and helping them to reach market, while private-equity firms assist with company enlargement and expansion.

Table 2: The Main Types of Private Investors

	Description	**Funding Stage**
Business Angels	An individual or network of individuals who invest their own money directly in entrepreneurs and young companies to help them reach the proof-of-concept or early development stage.	Seed funding and start-up
Venture Capital	Organisations that provide financial backing to promising concepts or technologies, investing in companies in their seed (concept), start-up and early stages of development.	Start-up and growth
Private Equity	Organisations that invest in more-mature companies with the aim of driving business growth, often through increasing margins and/or identifying sources of revenue growth	Growth and expansion

The importance of private investors is widely recognised by governments, which see venture capital in particular as a key component of the innovation process, and have consequently sought to promote the industry. Venture capital has been found to help businesses to 'invest more than they would otherwise, to grow more quickly, and sustain performance in the long term' and is an important source not only of funding, but also of expertise and networks for young companies.[22] There is also evidence to suggest that 'venture-backed firms are responsible for a disproportionate number of patents and new technologies, and they bring more radical innovations

22. Josh Lerner, Yannis Pierrakis, Liam Collins and Albert Bravo Biosca, 'Atlantic Drift: Venture Capital Performance in the UK and the US', NESTA Foundation Research Report , June 2011, p. 3.

to market faster than lower-growth businesses that rely on other types of finance'.[23] While venture capital is primarily considered a profit-driven sector, experts also suggest that its 'unique link between finance and innovation also positions it to function as a sort of incubator for R&D'.[24]

The first-venture capital fund was created in the US in 1946, and the growth of the industry accelerated in the 1970s. Since then, venture capital has been the driving force behind some of the most innovative and fastest-growing industries of the US economy. Today, the US continues to be home to the largest venture-capital industry in the world, investing $20 billion in 2010.[25] This has generated a particular culture of innovation within the US private sector, whereby the threshold for risk is high and failure is tolerated, the relationship between companies and investors is close, and collaborative R&D is common. According to one commentator, the US 'has depended on this rich ecosystem [...] where many of the biggest innovations stem from the work of the community, rather than a lone innovator'.[26]

While the UK venture-capital industry is the largest and most developed in Europe, it is understandably much smaller than its US counterpart, investing a total of $1 billion in 2010.[27] It also suffers from significant shortcomings, recognised by government itself which is 'mindful of the recent relative weakness in the [venture capital trust] market'.[28] The biggest challenge relates to an increased concentration of larger investments in well-established business, which contributes to an ongoing shortage of funds to support smaller-scale investments, consequently creating a barrier to business formation and growth.[29]

As a result, 'Private sector finance is not always easy to find for businesses with innovative ideas, which may be seen as high risk', according to Innovate UK, which is mindful of the 'well-recognised seed finance gap for start-up and early-stage companies, as well as for small innovative enterprises that want to invest in their own development and growth'.[30] Several schemes have been set up in the UK in support of the venture-capital industry and to address the significant funding gaps not being addressed by the market, particularly

23. *Ibid.*, p. 9.
24. John Reinert, 'In-Q-Tel: The Central Intelligence Agency as Venture Capitalist', *Northwestern Journal of International Law and Business* (Vol. 33, No. 3, Spring 2013), p. 691.
25. Lerner *et al.,* 'Atlantic Drift', p. 6.
26. Peter Singer, 'Federally Supported Innovations: 22 Examples of Major Technology Advances that Stem from Federal Research Support', Innovation Technology and Innovation Foundation, February 2014, p. 4.
27. Lerner *et al.,* 'Atlantic Drift', p. 6.
28. HM Treasury, *Bridging the Finance Gap,* p. 7.
29. *Ibid.,* p. 6.
30. Technology Strategy Board, *Delivery Plan,* p. 19.

for small, high-technology start-ups. According to one assessment, however, many past interventions have 'fallen foul of a few common problems: trying to achieve too many goals; being sub-scale; limiting the pool of potential investments; and having unrealistic time horizons'.[31]

31. Lerner *et al.,* 'Atlantic Drift', p. 29.

III. Current Investment Landscape and R&D in Critical Capabilities

The UK's security and intelligence sector has undergone significant changes over the last decade. It is noteworthy that, conscious of some of the challenges outlined in Chapter II, there have been efforts by government to improve communication and engagement between it, its agencies and industry. In March 2007, the Security and Resilience Industry Suppliers' Community (RISC) was established – an alliance of suppliers, trade associations and academics, which aims to provide a focal point for government to liaise with industry on national-security requirements.

In 2009 the Home Office published the UK's Science and Technology Strategy for Countering International Terrorism, setting out objectives for defining the relationship between government and industry. Most notably, the strategy aimed to 'ensure the development and delivery of effective counter-terrorism solutions by identifying and sharing priority science and technology requirements'; it also sought 'greater partnership and engagement with industry and academia and commits us to more openness and transparency' in this field.[1] One of the means to achieve this goal was the Innovative Science and Technology in Counter-Terrorism programme (INSTINCT). Led by the OSCT, INSTINCT sought to attract innovative solutions to support the counter-terrorism strategy by providing 'a greater understanding of the innovation community, smarter influence over external innovation and better coordination of investments in new ideas and solutions'.[2] While the aims of the Science and Technology Strategy and INSTINCT programme were commendable, feedback from both government and industry stakeholders revealed that implementation was poor and there had been little demonstrable programmatic success.

Through the publication of the MoD's *National Security through Technology* White Paper, there have also been efforts to clarify and simplify the government's defence and security procurement policy, thereby making the national-security sector more attractive to external investment. As noted, the security and intelligence agencies – and GCHQ in particular – have taken steps to improve their engagement with both research institutes and industry partners.

These efforts culminated in 2014 in the creation of the Security Innovation and Demonstration Centre (SIDC), a partnership between the Home Office and RISC. Housed in the Centre for Applied Science and Technology (CAST),

1. Home Office, *The United Kingdom's Science and Technology Strategy for Countering International Terrorism,* p. 7.
2. *Ibid.,* p. 13.

it is hoped SIDC will provide government with better understanding of commercial technology evolution in this sector. Its main aims are to outline 'grand challenges' in order to encourage industry innovation in particular areas, to run funding calls in support of existing and newly emerging large-scale government programmes, and to provide successful bidders with access to end-users, test beds and data sets to facilitate the development and exploitation of capabilities.[3] While the initiative is in its earliest days, government sources were cautiously optimistic that it would help overcome barriers to R&D collaboration.

Self-Inflicted Wounds

In spite of this optimism, overcoming barriers to R&D collaboration will remain a major challenge given the fragmented nature of R&D in the national-security sector. This largely reflects the range of departments, agencies, law-enforcement bodies and local delivery partners involved in this work, as well as the broad range of requirements stemming from the relevant strategies.[4] While many of the macro-level issues such as government R&D funding are beyond the control of the sector, we have found that many of the challenges specific to the sector are largely self-inflicted. Given budgetary restraints, questions have been raised as to whether the money available is being spent in the most efficient way, whether the number of stakeholders could be reduced, and whether support is being targeted in the right areas.

Leveraging Private-Sector Expertise to Meet Set Requirements

In the *National Security through Technology* White Paper, the government sets out its intention to 'work with the science and technology supplier base by sharing our capability requirements and investment priorities early on'.[5] This necessitates formulating a so-called 'make-buy' policy, whereby key capabilities to be required over a set time period are identified, before a decision is made on what should be developed internally and what should be procured from industry. Throughout our research, however, representatives from both the public and private sectors raised concerns that the government's strategic make-buy policy was not being clearly articulated, potentially because the requirements were not being clearly delineated by the security agencies in the first place.

This may be partly due to the speed of technological development, which leads to calls for industry solutions that are fairly specific and must be turned around in a short period of time, making it difficult to establish longer-term requirements. With new technology needing to be developed over ever-

3. Security, Innovation and Demonstration Centre, 'What We Do', <https://www.gov.uk/government/groups/security-innovation-and-demonstration-centre>, accessed 3 November 2014.
4. Ministry of Defence, *National Security through Technology,* p. 44.
5. *Ibid.*, p. 36.

shorter time horizons, the instinct seems to be to turn to trusted industry primes to fill short-term capability gaps. While this method offers the path of least resistance for government and its agencies, it overlooks the importance of developing longer-term, disruptive technology, and is not conducive to encouraging growth and innovation within the ecosystem. The result is a relatively closed marketplace where a small number of large firms dominate, and there is a reliance on a small number of established and 'trusted' suppliers to support technology and capability needs.

This paper's concern is that this reliance on primes is cutting off the oxygen to help grow the SME market for national security. Feedback from the agencies and some industry primes suggested that they have often been disappointed by the level of innovation demonstrated by SMEs and start-ups operating in this sector. Yet according to *National Security through Technology*, 'SMEs typically possess characteristics that are particularly important when meeting defence and security requirements. These include agility, flexibility, genuine innovation, commitment, customer focus, lower overheads, and often niche or specialist skills and capabilities'.[6]

According to government figures, the national-security market employs around 140,000 people and comprises 9,000 companies,[7] though it is unclear what government considers the boundaries of the market to be, and whether these figures include the UK's rapidly increasing number of hi-tech SMEs. Conversations with both public- and private-sector stakeholders provide reason to doubt the extent to which government and its agencies correctly assess the scale and capability of the market, and venture out to identify innovative companies operating across different sectors. This may be one of the objectives of the newly formed SIDC, but its quarterly calls are likely only to offer a snapshot of the 'known' portion of the market, continuing the government's inclination to turn to the 'usual suspects' for innovation. We therefore fear that overall knowledge of the size, quality and innovation of the SME market for national security remains limited.

Breaking Down the Culture of Secrecy and Becoming an Attractive Customer
In an area such as national security, where there are obvious sensitivities around revealing capability gaps, there is understandable hesitation from government and the agencies to provide capability roadmaps or similar indications of future technological procurement. This veil of secrecy presents significant challenges for industry, however. Knowledge of general requirements is currently poor, and there is no means to feed back capability performance or connect the user community with the supplier. Calls for industry solutions can be quite specific, but this is not a good model as technology often moves too quickly and businesses are unable to concentrate

6. *Ibid.*, p. 22.
7. *Ibid*.

on longer-term, more disruptive capabilities. Industry bodies have therefore called for long-term technology strategies to be better articulated so that R&D investments are not made in vain.

The siloed nature of the departments in question means that decision-making and procurement processes are often disparate and slow. This is something that even government admits particularly affects the security sector, where it recognises that 'arrangements for working with suppliers are not ideal, with responsibility dispersed across government from the Home Office to the security and intelligence agencies'.[8] Once contracts are awarded, there can still be significant regulatory and procurement hurdles to overcome, something that smaller companies typically find more challenging than the large primes and systems integrators. Feedback from industry sources suggests that government is therefore low on the list of potential customers for SMEs, not only because margins tend to be smaller than the commercial sector, but also because government is seen as a 'difficult customer'.

Encouraging Private Investment

The national-security market is not only invisible to non-traditional suppliers, but also impenetrable to investors, who perceive it to be small, problematic and particularly high-risk. The government is the foremost customer of the security market, yet without clear signalling over future requirements, investments in this sector are regarded as particularly high-risk, since it is difficult for private investors to see what the returns on these investments would ultimately be. This is acknowledged by government, which recognises that:

> Private investment in defence- and security-related science & technology has a vital role in developing technology markets and ensuring equipment, systems, and services have the technical edge to meet the UK's defence and security needs.

It also recognises, however, that industry 'will only put private investment into science & technology where there is a clear understanding of the route to market, to exploit this into products'.[9] Investment in this sector is likely to remain ad hoc and disjointed until there is a more mature relationship between government and investors, and government can increase confidence in the market.

As noted in Chapter II, the venture-capital sector in the UK is much smaller that its US counterpart; the UK invests 0.05 per cent of its GDP in venture capital, compared with 0.14 per cent in the US.[10] The types of industry

8. *Ibid.*, p. 50.
9. *Ibid.*, p. 36.
10. Lerner *et al., Atlantic Drift*, p. 6.

on which each country focuses also tend to be different, with US funds prioritising 'internet/computers and communications/electronics', while European funds 'instead invest relatively larger proportions in other sectors such as business/industrial and consumer'.[11] A further difference is that the UK sector is more risk-averse than the 'fail fast, fail often' approach in the US. While the UK tends to play it safe, avoiding disruptive technologies, the US is more willing to entertain ideas, take greater risks and accept failure. As a result, 'The UK and the European venture capital industry more generally are perceived to be the poor cousins of the US industry, consistently delivering lower returns to their investors'.[12]

These issues are particularly felt in such an opaque area as national security, where the culture of secrecy outlined above results in low investor confidence in the market. As they do not understand the requirements, investors and their advisers often lack the level of expertise necessary to judge whether a product is likely to be successful in this market. This is problematic since, as previously noted, venture capital plays an important role in supporting innovation and risk in the early-stage companies that typically develop the disruptive technologies and capabilities required by the security and intelligence agencies.

An alternative route for SMEs to access investment is through corporate venture capital (whereby the corporate funds of large systems integrators are invested in external start-up companies) and the venture-capital arms of large multinational organisations. These can either be specific to the defence and security market (for example, Lockheed Martin's Technology Ventures Corporation or Raytheon Commercial Ventures) or broader in scope (for example, Google Ventures). However, it was often suggested to us that SMEs are seen as disruptive to longstanding relationships, and struggle to break into this closed supplier model. They are also more wary of investment from these organisations given the likelihood of being bought out early, or simply quashed as competitors.

Managing the Innovation Ecosystem

These three challenges – a low capacity to leverage private-sector expertise, a culture of secrecy, and a risk-averse venture-capital market – represent major hurdles to sustaining adequate levels of investment in R&D for the security and intelligence sector and, in particular, supporting the small firms which are key players in bringing new technology to market.

The UK's funding landscape for R&D is also weak and fragmented, to the point where many perceive the valley of death to be wider in the UK than in many other countries. There are pockets of funding available, but these

11. *Ibid.*, p. 13.
12. *Ibid.*, p. 6.

are often not the easiest to track and the different support mechanisms available can be complex for industry to navigate. The result is that SMEs are both disconnected from the requirements of the agencies and lack access to the R&D 'infrastructure' of financial and non-financial resources to help them to commercialise their products. The sensitive nature of the agencies' work and limited information on market requirements and trends also mean that start-ups and companies developing new technologies aligning with the work of the agencies are often caught in a vicious circle of a lack of investment and confidence.

Some in the commercial sector may question whether it is appropriate for government to exert influence over, or somehow manage, innovative companies operating in the free market. With the exception of BIS, government departments and agencies are not generally interested in stimulating the market or encouraging innovation in particular sectors. Nonetheless, government remains the leading customer for defence and security and thus invariably shapes the market. The agencies will always have their own internal R&D programmes which address most of their challenges. At the same time, however, they have a vested interest in a healthy private-sector R&D ecosystem serving national security, working on long-term, disruptive technology and which the agencies can periodically leverage to overcome operational capability requirements.

Government and its agencies do not necessarily need to fund this R&D directly; private investors have the potential to fill any funding gap, but only if they have clearer indications of the agencies' future requirements, technology strategy and what is likely to be required from industry. In the words of the STC, 'Without a definite commitment from Government, business is more reticent about making its own financial commitment to the levels of risk that innovation requires'.[13] Clearer policy, requirements and procurement procedures would help both industry and venture-capital community gauge the size of the market and have the confidence to invest in the security sector.

13. House of Commons Science and Technology Committee, *Bridging the Valley of Death,* p. 54.

IV. Bridging the Investment and Capability Gap

There is a wide range of models available, drawing on various funding sources, to enhance collaboration on R&D in a sector such as national security. These include, among others: government R&D contracts; dedicated government research agencies such as the UK Defence Science and Technology Laboratory (DSTL) or US Defense Advanced Research Projects Agency (DARPA); joint ventures; public–private partnerships; technology incubators; corporate venture capital; consortia and university–industry collaborations. One of the most original models developed in recent years is In-Q-Tel, the not-for-profit venture-capital body set up by the CIA.

In the late 1990s the CIA recognised that it suffered from what has been referred to as a 'volume problem' and 'information gap'.[1] The pace of ICT change meant that its systems were struggling to manage the rapidly increasing flow of information the CIA collected. It also became clear that spending by private industry on innovation and technology considerably outpaced that of the intelligence community, and the agency needed to face the reality that 'the private sector – not government – was pacing the information technology (IT) revolution'.[2] The solution proposed was to create an independent agency that bridged this investment gap between the agencies, national laboratories and the private sector.

Learning from In-Q-Tel's Example

In-Q-Tel is described as 'most analogous to a corporate strategic venture capital entity – like those maintained by major technology firms'.[3] Operating as an independent and not-for-profit organisation (any returns are re-invested), In-Q-Tel identifies start-up companies and businesses developing technologies relevant to the CIA's mission, providing private equity and product development funding. The organisation makes an average of twelve to fifteen investments per year, of between $250,000 and $3 million each, receiving an annual contract of between $30 million and $37 million as a line item in the CIA's Directorate of Science and Technology budget since 1999.[4]

According to representatives from the US intelligence community, In-Q-Tel offers the most advantageous model in offering rapid, tactical investments that accelerate the development of mission-critical capabilities; alternative models would not be able to meet the fast pace and change demonstrated

1. Josh Lerner, Felda Hardymon, Kevin Book, and Ann Leamon, 'In-Q-Tel', Harvard Business School Case 804-146, February 2004 (Revised May 2005), p. 2.
2. Business Executives for National Security, *Accelerating the Acquisition and Implementation of New Technologies for Intelligence: The Report of the Independent Panel on the Central Intelligence Agency In-Q-Tel Venture*, June 2011, <http://www.bens.org/document.doc?id=42>, accessed 3 November 2014, p. vii.
3. Reinert, 'In-Q-Tel', p. 694.
4. Lerner *et al.*, 'In-Q-Tel', p. 8.

by the commercial IT sector. While many of its investments may be higher risk than typical investments in this sector, an analysis conducted two years after its inception concluded that 'In-Q-Tel's potential advantage to the CIA outweighs the risk'.[5] Former CIA director George Tenet has also claimed that 'The In-Q-Tel alliance has put the agency back at the leading edge of technology, a frontier we never should have retreated from in the first place'.[6]

The idea of establishing a similar organisation in the UK has been considered and subsequently dismissed. Transposing the In-Q-Tel model into the UK context would be inadvisable; In-Q-Tel was set up to address specific R&D challenges in the US, and both the R&D landscape and venture-capital sector in each country are very different. That said, the organisation has been successful in overcoming many of the challenges currently experienced by the UK. It is also regarded as 'essential to helping identify and deliver groundbreaking technologies with mission-critical applications to the CIA and ... partner agencies'.[7] It is therefore worth identifying what transferable lessons can be learned from In-Q-Tel.

Leveraging Private-Sector Expertise to Meet Set Requirements

One of the principal advantages of In-Q-Tel is that it both collates the requirements of the US intelligence community and houses responsibility for identifying new and innovative technology being developed by the private sector that may help the agencies to meet these requirements.

In-Q-Tel was initially designed to assess the best commercial off-the-shelf technology in the belief that 'there was more than enough technology in the marketplace, and the CIA only needed In-Q-Tel to pick the best technology and bring it into the Agency'.[8] It was soon realised, however, that a requirements-based approach, which leveraged private-sector expertise to solve specific problem sets, was more suited to achieving the CIA's objectives. Whereas requirements-setting in the UK is often dispersed among different individuals and bodies, In-Q-Tel's ability to centrally co-ordinate agency requirements is a significant asset, allowing it to target its resources and investments more efficiently.

Given its focus on emerging technology for the intelligence community, the organisation possesses more technical expertise than the typical venture-capital firm. It is also able to leverage this expertise to extend its reach and

5. Business Executives for National Security, *Accelerating the Acquisition and Implementation of New Technologies for Intelligence,* p. v.
6. Reinert, 'In-Q-Tel', p. 699.
7. 'Remarks by Director David H. Petraeus at In-Q-Tel CEO Summit', 1 March 2012, <https://www.cia.gov/news-information/speeches-testimony/2012-speeches-testimony/in-q-tel-summit-remarks.html> accessed 3 November 2014.
8. Business Executives for National Security, *Accelerating the Acquisition and Implementation of New Technologies for Intelligence,* p. 8.

tap into the innovation produced by the private sector, whose ability to 'rapidly prototype new products and get them to market – especially our market – is a skill that government simply cannot match'.[9] The CIA may not be able to keep pace with the 'Internet time' and profit-driven innovation of commercial businesses,[10] but, as a private company, In-Q-Tel is able to structure itself 'in a manner that will be familiar to many of the information technology companies we hope to attract as partners', in the words of its former director, Gilman Louie.[11] It is also thereby able to bridge the 'potential disconnect between the world of the government contractor and the venture capitalist'.[12]

Breaking Down the Culture of Secrecy and Becoming an Attractive Customer
In its role as an intermediary between government, private industry and investors, In-Q-Tel is able to help companies penetrate what is historically a closed and opaque market, providing young start-up companies in particular with access to the specialised needs and customer base of the intelligence community.[13] An independent evaluation of In-Q-Tel in 2001 concluded that it had 'indeed succeeded in doing business with companies who would not have considered contracting with the government due to the tedious procurement process, reporting requirements and regulations'.[14]

One of the primary reasons why it has managed to open up the security market to new business is the publication of CIA and other agency requirements in the form of 'problem sets', a 'corollary benefit to the formation of In-Q-Tel'.[15] The problem set is a list of unclassified technology needs, translated for industry in the form of targeted investment areas. The advantage of this system is that it gives industry and investors confidence to pursue R&D in specific areas, without them knowing 'whether the targeted technology is aligned with the Agencies' future IT vision or if it will directly address a specific agency requirement'.[16] This ambiguity avoids the need to publish sensitive details of what are otherwise highly confidential capability gaps.

This increased level of communication further allows the agencies to build relationships with industry, to procure on a continuous rather than transactional basis, and to secure technology that will be updated 'according

9. 'Remarks by Director David H. Petraeus at In-Q-Tel CEO Summit'.
10. Reinert, 'In-Q-Tel', p. 687.
11. *Ibid.*, p. 697.
12. Lerner *et al.*, 'In-Q-Tel', p. 4.
13. *Ibid.*, p. 6.
14. Business Executives for National Security, *Accelerating the Acquisition and Implementation of New Technologies for Intelligence,* p. x.
15. *Ibid.,* p. 27.
16. *Ibid.,* p. xii.

to the constantly developing needs of the commercial market rather than the intermittent needs of a single government agency'.[17]

Encouraging Private Investment

The third strength of the In-Q-Tel model is its ability to stimulate private investment in the US security and intelligence market, acting as a 'valley of death avoidance mechanism', in the words of one interviewee. As noted, the publication of clearer agency requirements gives investors more confidence to invest in this area. In-Q-Tel is also seen as having a 'halo effect', whereby 'In-Q-Tel's interest in a company signalled technical excellence to other VC firms, improving overall funding prospects'.[18] In other words, any investment it makes in a company draws the attention of private-sector venture-capital funds, thereby raising the chances of the company receiving further investment. This is partly thanks to In-Q-Tel's strict due-diligence process; its investigation into the structure of the company, financial status, and ability to develop solutions that align with CIA missions acts as a 'Good Housekeeping' seal of approval for other firms. According to the organisation's own figures, venture capitalists invest more than $9 for every $1 invested by In-Q-Tel.

While the In-Q-Tel model offers particular benefits, it is not a perfect system and has drawn criticism, which also offers valuable lessons for the UK's approach. According to one critic, 'The CIA is not equipped to succeed in the notoriously perilous business of venture capital, and heightened ethical concerns surround the making of government-sponsored equity investments in private companies'.[19] One of the biggest criticisms centres on the 'disagreement and confusion over the level of In-Q-Tel's success and progress', with the absence of 'an agreed upon set of criteria to evaluate In-Q-Tel's performance'.[20] Since the organisation is not for profit and returns on investment cannot be used as a performance metric, the report therefore recommends that its success should be measured by its ability to accelerate technology insertion into the CIA, transfer solutions to the point of implementation, and improve the overall capabilities of the agency and its employees.[21]

Technology-adoption rates have proved a challenge for In-Q-Tel, however. No preference is given to technologies developed by In-Q-Tel at the acquisition stage and, according to feedback from one current intelligence official, 'transitioning In-Q-Tel investments has been largely ad-hoc in the past'. They went on to note the significant cultural, organisational and technological

17. Reinert, 'In-Q-Tel', p. 696.
18. Lerner *et al.,* 'In-Q-Tel', p. 6.
19. *Ibid.*, p. 680.
20. Business Executives for National Security, *Accelerating the Acquisition and Implementation of New Technologies for Intelligence,* p. xv.
21. *Ibid.,* p. vi.

hurdles that must be overcome before the technology can be adopted by the CIA; one report has noted that the current process 'seems extremely complicated and time consuming'.[22]

There are also indications that communication between the CIA and In-Q-Tel could be improved. 'Little awareness exists of In-Q-Tel activities in the Agency at large', claims one report, and 'analysts learn more about In-Q-Tel by reading media reports than from internal "marketing" on what In-Q-Tel technologies might do for them'.[23] The responsibility for liaising between the CIA and In-Q-Tel lies with the In-Q-Tel Interface Center (QIC), a team of a dozen or so agency employees. 'Innovations delivered by In-Q-Tel's portfolio companies will never assist the CIA with its mission if QIC does not function properly and efficiently',[24] according to one commentator, and efforts have therefore been made to improve alignment of the CIA's technology and business strategies, as well as the communication between end-users and senior executive leadership.

As previously noted, the idea of setting up a UK variation on In-Q-Tel is inadvisable, given the differences in market conditions between the two nations, but the organisation embodies the culture of risk and attitude towards innovation that is required within the UK security and intelligence sector. While it may not solve the issue of integrating new and innovative technologies into the security and intelligence agencies, the In-Q-Tel model has provided obvious benefits for the wider US ecosystem, by communicating the agency requirements more effectively, attracting funding from private investors, and improving collaboration between the agencies, investors and industry. While the primary goal in establishing In-Q-Tel was to identify emerging private-sector innovations to solve the CIA's problem set, 'the secondary goal for In-Q-Tel was, and continues to be, to help create new IT markets, stimulate competition, and develop multiple commercialized solutions to help the Agency obtain better technologies more efficiently with a lower overall cost of ownership'.[25]

22. *Ibid.,* p. x.
23. *Ibid.*, p. xi.
24. Reinert, 'In-Q-Tel', p. 704.
25. Business Executives for National Security, *Accelerating the Acquisition and Implementation of New Technologies for Intelligence,* p. 9.

Conclusion: A Future R&D Roadmap

In the past, government has traditionally taken the lead on R&D and 'it has not been uncommon for industry – particularly in the security and defence sectors – to be regarded as a strategic asset ready to be co-opted into the national effort at times of emergency'.[1] Yet never before has there been as much need to align the R&D activities of the public and private sectors, and make the relationship between the two less transactional and more collaborative. Given the multifaceted threats that the UK faces and the requirement for sophisticated, technology-intensive intelligence capabilities, new solutions are needed at a pace that can only achieved by the private sector.

The security and intelligence agencies will always have their own internal R&D programmes to address the majority of their challenges. However, the source of the most innovative technologies and solutions are often developed via the niche expertise of SMEs and technology start-ups. The agencies therefore have a vested interest in a healthy and dynamic industry ecosystem, working on long-term, disruptive technology for the security market and which the agencies can periodically leverage to overcome operational requirements. This can only happen if the level of funding for R&D is increased and sustained, and the three weak points within this ecosystem identified by this report are addressed.

Recommendations

Investment for R&D in security and intelligence should be increased: there was widespread consensus among both public- and private-sector stakeholders that current levels were insufficient to ensure the development of long-term, disruptive technology.

Government needs to attract private investors to this sector by increasing market confidence: The absence of private investors hinders the sector's ability to sustain high levels of R&D funding within the ecosystem. The UK venture-capital market tends to be more risk-averse than its US counterpart, and government needs to offer clearer signalling to attract external investment; Innovate UK has discovered that 'private sector investors see companies that have been awarded Technology Strategy Board support as good investment prospects, carrying less risk because their ideas have been independently assessed and backed by government funding'.[2]

Articulate requirements and make-buy policy more effectively: Clearer indications from the government on technology policy, strategy and procurement would improve investor confidence and help industry to

1. Cornish, 'Technology, Strategy and Counterterrorism', p. 886.
2. Technology Strategy Board, *Delivery Report 2014,* p. 23.

better allocate their R&D resources in priority areas. The requirements of the three security and intelligence agencies need to be better co-ordinated; the publication of US-style problem sets would enable the agencies to communicate their collective needs without revealing sensitive capability gaps.

Break down the culture of secrecy: This culture of secrecy is particularly problematic for investors, who are unable to gauge the market requirements and the ultimate return on their investments. There are signs that dialogue between the agencies and industry is beginning to increase, albeit intermittently. Conversations must take place at an earlier stage in the innovation process to encourage R&D collaboration and improve overall efficiencies.

Open up the market and be flexible enough to make tactical investments: SMEs are deterred by the challenges of operating a market that is dominated by a small number of large companies and which they struggle to penetrate. At the same time, the level of innovation within the SME market and the potential of technologies being developed in other sectors need to be better understood. The ability to regularly scope the market and make targeted investments in capabilities would enable government to remain at the forefront of technology development without carrying the financial burden of large, long-term R&D programmes.

About the Authors

Charlie Edwards is Director of the National Security and Resilience Studies Group at RUSI. Charlie conducts a broad range of research and analysis on counter-terrorism, organised crime, cyber-security, and resilience in the UK and overseas. Prior to RUSI he was a Research Leader at the RAND Corporation and a Senior Civil Servant in the Office for Security and Counter Terrorism (Home Office). He has undertaken extensive fieldwork in Europe, Middle East and East Africa.

Calum Jeffray is a Research Analyst within the National Security and Resilience Studies Group. His research interests include cyber-crime, the nature and impact of organised crime within the UK, and counter-violent extremism. Calum completed his MPhil in International Relations at the University of Cambridge, where his dissertation examined the role of international organisations in improving cyber-security. He also holds a first-class MA in French from the University of St Andrews.

RUSI Membership

RUSI membership packages provide privileged networking opportunities and benefits tailored to meet the needs of both individuals and large organisations.

Individual Memberships
Individual memberships are suitable for those individuals who wish to join RUSI's growing network of policy-makers and practitioners. Benefits include regular updates from RUSI, including invitations to members' lectures and seminars, subscription to the *RUSI Journal* and *RUSI Defence Systems*. This package also offers members access to our renowned Library of Military History.

Corporate Membership
RUSI's corporate-level membership packages, offering discounts to all RUSI conferences, are open to all organisations concerned with defence and security matters, and can be tailored to meet the business interests of both public and private sectors.

Concessions
Discounted student and young persons rates are available for those under the age of 35. Concessions are also available for those over the age of 65. We also offer online membership to those wishing to access RUSI's content of analysis and commentary.

www.rusi.org/membership