UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions

ABSTRACT

The United Kingdom (UK) forms the largest internet economy in the G20 and has the stated ambition of being the 'safest place in the world to live and work online'. Cybersecurity is, thus, regarded as both a challenge as much as an opportunity. Since the publication of UK's first National Cyber Security Strategy (NCSS) in November 2011, the government has implemented many proactive as well as reactive measures to enhance both its cybersecurity capabilities as well as its market power in this space. This article provides an analysis of the shift away from a reliance on market forces that dominated Western approaches to cybersecurity over the recent years. Specifically, it highlights three 'market failures' that have prompted UK's industrial policy responses: ongoing data breaches; inadequate private cybersecurity investments; and a continuous digital skills gap. An analysis of these drivers as well as UK government's responses demonstrates that the UK's cybersecurity strategy has evolved from an initial heavy reliance on market forces towards a more state-driven public-private partnership.

Introduction

The United Kingdom (UK) is at the forefront in several aspects of cybersecurity. Of the G20 countries, the UK has the largest internet economy as a percentage of gross domestic product and has extended its lead since it was first measured in 2010 (Department for Culture, Media and Sport 2017). The digital sector accounts for 16 per cent of the UK domestic output, 10 per cent of its employment and 24 per cent of the UK's exports (Chakravorti and Chaturvedi 2017, 40). With companies such as BAE Systems and Qinetiq as well as the country's engagement in offensive cyber programs, the UK has emerged as a core player in the cybersecurity industrial complex.

The UK government upholds an active commitment to fostering its international information security status. Having been nominated as a 'tier one' threat, cybersecurity is now regarded as central to the UK's national security. It is the UK government's aim to be one of the world's leading digital nations and to make the UK 'the safest place in the world to live and work online' (National Crime Agency and National Cyber Security Centre 2018, 2). This theme runs through major policy documents including the Digital Strategy (2017), the Digital Charter (2018) or the Cyber Security Export Strategy (2018).

Over the years, the government's efforts to improve cybersecurity and promote growth in its corresponding industrial sector have been led by a number of departments with changing names, roles and functions. These have generally included the Cabinet Office, the Department for Business, Energy and Industrial Strategy (BEIS), the Government Communications Headquarters

(GCHQ), the Department for Digital, Culture, Media and Sport (DCMS) and most recently, the Department for International Trade (DIT). These, alongside other institutions and agencies, are at the forefront of attempts to make the UK not only more resilient to digital attacks or system failures, but also to promote the UK's cybersecurity industry and enhance development and growth in this space.

Since the publication of UK's first National Cyber Security Strategy (NCSS) in November 2011, the government has implemented many proactive and reactive measures to enhance both its cybersecurity capabilities as well as its market power in this domain. The government released investments of £860 million for its National Cyber Security Program (NCSP) for the period from 2011 to 2016 (Cabinet Office 2011),and boosted its spending to £1.9 billion for its cybersecurity vision from 2016 to 2021 (Cabinet Office 2016a). This included the establishment of a new National Cyber Security Centre (NCSC) that acts as the public facing arm of GCHQ. The NCSC offers an interface between government and industry and provides guidance as well as advice (Tanczer et al. forthcoming).

The UK's success in digitizing its economy has made it an exemplar for other states with similar ambitions. Its policy approach has evolved from an initial heavy reliance on market forces towards a more state-driven public-private partnership. This evolution aligns with a process that many other countries have recently undergone (Matania, Yoffe, and Goldstein 2017). However, one of the discursive challenges one faces in discussing 'cybersecurity' is the breadth and depth of the factors that the term can refer to. This introduces a number of complexities for those responsible for developing national cybersecurity strategies and corresponding policies. First, cybersecurity intersects with a wide range of sectors, economic factors and issue areas. Second, and relatedly, it affects diverse groups of actors, and does so in different ways. Third, and critically for policymakers, these sectors and actors can have competing or even conflicting interests and agendas – all of which need to be considered, balanced and addressed. Complicating all of this, is the rapid pace in which digital technologies continue to be developed and incorporated into societal practices, processes and institutions. Considering these factors and UK's level of maturity in this space (Bada et al. 2016), the UK offers a useful case study which can be expected to be emulated by others.

In particular, there are a number of key issues that drive UK's industrial policy on cybersecurity. These include: (a) domestic security considerations shared among many states; (b) an aspiration to grow the indigenous cybersecurity sector; and (c) the anticipation that the UK will continue to play a global leadership role in the cybersecurity realm. These three factors are outlined in more depth below and will be followed by an analysis of market failures that currently overshadow the UK's cybersecurity status.

Domestic cybersecurity

In common with every industrialized state, ensuring a sufficient level of cybersecurity in the domestic context is a high priority for the UK. Citizens have the right to feel safe online (as they do in the physical world) and, to some extent at least, this is regarded as a responsibility or even the *purpose* of the state (Couzigou 2018). Protecting vulnerable sections of the community like children, ensuring financial transactions are secure, and preventing identity theft are expectations of the state held by civil society in the 21st century.

Critically for governments like the UK, addressing these expectations is understood to be fundamental to further optimize the benefits of the digital economy and the future of innovation. Maintaining public confidence in emerging technologies and their uptake is seen as central to their widespread adoption and is, in turn, central to maximizing the considerable public benefits believed to derive from their intensified implementation (Corrales and Westhoff 2006; Taylor et al. 2018). Thus, the latest UK *Industrial Strategy* explicitly states that the UK will seek to 'strengthen overall data security, reinforcing the UK's position as a global centre for cybersecurity (Department for Business, Energy and Industrial Strategy 2017, 40).

Growing the cybersecurity industry

The UK government is both a provider and a consumer of cybersecurity. In particular, the imperative of offering cybersecurity support to UK businesses is linked to the imminent prospects the digital economy can bring. Of particular concern are small and medium enterprises (SMEs) which often lack the resources and expertise that larger firms can draw upon (Carr 2016). Efforts to deliver this support is channelled through a number of public and private initiatives which are frequently revised and re-evaluated to ensure maximum efficacy and impact (Business, Innovation and Skills Committee 2016). In addition, the UK also regards the cybersecurity industry as a global export service that has positive effects for continuing to build UK's reputation as a global leader in the cybersecurity sector. In 2018, the Department for International Trade produced its *Cyber Security Export Strategy* in which it projects exports growing to £2.6 billion by 2021 (Department for International Trade 2018, 12).

International dimension

The UK has played (and aspires to continue to play) a global leadership role in terms of international cooperation on cybersecurity debates. This is evident in its prominent role in various international fora where cybersecurity is negotiated. These include, the UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, which works to develop consensus on exactly what constitutes responsible state behaviour in cyberspace (Kane 2014). This ambition to global leadership is also evident in the UK's establishment of the

Global Conference on Cybersecurity – otherwise known as the 'London Process'. The UK's engagement with international aspects of cybersecurity is also bolstered by its membership of the intelligence sharing group, the 'Five Eyes' – consisting also of the US, Canada, Australia and New Zealand. This network has proven to be one of the most important intelligence sharing communities in the post-WWII era and continues to be highly valued by its members in the context of the information age.

The central lens applied to all articles in this special issue is that of market failures and subsequent government's responses. In the UK case, market failures have been identified and drawn out through the analysis of two consecutive NCSS documents. Indeed, the UK is considered to have one of the most advanced cybersecurity strategies amongst EU and NATO members (Štitilis, Pakutinskas, and Malinauskaitė 2016). The first UK NCSS was published in 2011 and covered the five subsequent years to 2016. The second NCSS was released in 2016 and runs until 2021. There was a significant shift in tone from the first to the second which clearly highlights how the UK government perceived the market as having failed to deliver on expected goals.

The article proceeds as follows. First, we outline three major market failures that emerge from the comparison of these two strategies. These include: (a) ongoing data breaches; (b) a failure of the private sector to invest adequately in cybersecurity; and (c) a continuous digital skills gap. We then introduce the major initiatives that the UK has implemented to address those market failures. Following this, we discuss the statesociety dynamics particular to the UK which influence decision-making to tackle these shortcomings and highlight some of the effects these initiatives have upon the UK's overall industrial posture.

Market failures in the UK

As emphasized earlier, governments are engaged with cybersecurity on many levels and discussing all of its different dimensions in a holistic and comprehensible manner is nearly impossible. A recent mapping study of cybersecurity policy in the UK government identified hundreds of nodes and initiatives, ranging from data protection, network security, privacy concerns, national security, defence, economic security, infrastructure, innovation and many more (Carr et al. 2018a, forthcoming). In order to narrow the scope of analysis, this article focuses on market failures perceived by the UK government through the changes from its first to its second NCSS.

In general, these strategies reveal much about the way a particular government perceives information security and its corresponding market's performance. They are carefully crafted to draw out the issues of most significance to that state and provide insight into perceptions of the state's place in an international order as well as its domestic conditions (ITU et al. 2018). In the UK, as in many other states, the first two decades of cyber insecurity were approached by the government as a public problem that would be best addressed by the private sector through market forces (Carr 2016). Indeed, this belief in market forces meant that the government's role was understood chiefly

to ‘stay out of the way’ of private actors which, if left unencumbered by regulation, would address the challenges of cybersecurity more quickly and efficiently than they would with the burden of government intervention (Matania, Yoffe, and Goldstein 2017).

While the UK still takes a relatively light touch attitude to cybersecurity regulation (Brass et al. 2017), the failure of the market to adequately resolve persistent and widespread cyber insecurity resulted in a notable shift from the NCSS produced in 2011 to the follow-on strategy released in 2016. In 2011, there was hope that the market would ‘drive the right behaviours’ (Cabinet Office 2016a, 27). By 2016, it was explicitly acknowledged that ‘the combination of market forces and government encouragement has not been sufficient in itself to secure our [the UK’s] long-term interests in cyberspace at the pace required’ (Cabinet Office 2016a, 27). The strategy went on to note that the ‘market is not valuing, and therefore not managing, cyber risk correctly’ (Cabinet Office 2016a, 27). Had the UK initially expected that a combination of ‘commercial pressures and government-instigated incentives’ would ‘ensure adequate business investment in appropriate cybersecurity’, progress was considerably lacking and government’s expectations in the five-year interim period were not met (Cabinet Office 2016a, 27).

The UK therefore recognized and actively responded in the 2016 NCSS to the market’s shortcomings and accepted that the government must now ‘set the pace in meeting the country’s national cybersecurity needs’ (Cabinet Office 2016a, 27). While the state acknowledged that the market continues to play an essential role, considering that many dimensions of cybersecurity lay beyond any government’s mandate and sphere of responsibility, there were aspects considered too critical to UK’s national interest to remain solely in the dominion of the private sector.

Thus, three primary (and related) issues emerge as requiring additional government intervention. These market failures are explored in more depth below and frame the measures used to interject when observing commercial failings (Aggarwal and Reddie 2018) as well as point to the delicate interplay of publicprivate partnerships in cybersecurity (Bossong and Wagner 2017). The following pages analyse the driving forces that underpin industrial policy on cybersecurity in the UK and offer a rationale for the socio-technical policies and actions pursued by the country.

Ongoing data breaches

Like the US and other nations with major digital economies, the UK has experienced a number of high-profile data breaches, notable both for the scale of the data lost as well as for the sensitivity of the data exposed. Global incidents like the Uber, Yahoo and Equifax breaches affected many UK residents, revealing personal and financial information. Indeed, further UK-based incidents such as the TalkTalk hack in October 2015 or the Ticketmaster breach in 2018 uncovered not only poor security practices across the market, but vulnerabilities inherent to the complex global supply chain (Priday, 2018).

These insights are unsettling, considering that the 2018 UK Data Breaches Survey found that 43 per cent of UK businesses identified at least one breach or attack in the last year (Department for Digital, Culture, Media and Sport 2018, 1).

The accumulation of these events in recent times marked a shift in government and public tolerance for data breaches – especially those seen to have been easily avoidable. While there is agreement that eliminating the potential for data infringements altogether is not realistic, each of these events raised questions about the extent to which affected businesses had been employing sufficient protective measures to inhibit such exposures from happening.

A joint report published by the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC) 2018, highlighted how frequently affected parties were also failing to prevent misuse under the most basic conditions. In the case of the Verizon data breach, access was obtained by perpetrators simply guessing the correct web address. The Uber breach involved the data of 57 million accounts which were left unencrypted. And an aggregated database collated from multiple breaches was found to contain '1.4 billion credentials in clear text including unencrypted and valid passwords' (National Crime Agency and the National Cyber Security Centre NCSC 2018, 10). Clearly, there were internal weaknesses that, at least in part, left these organizations more exposed to an attack than they should have been. This led to the UK government observing that '[t]oo many networks, including in critical sectors, are still insecure… Too many organizations are still suffering breaches at even the most basic level' (Cabinet Office 2016a, 27).

The insight that businesses had been lacking elementary security practices was part of a narrative around a failure of the board level to adequately devote themselves to cybersecurity. In response, the NCSC established a research stream to investigate how boards could be better supported and incentivized to take this aspect more seriously (RISCS 2018). This is closely related to the second market failure which warranted government attention: the lack of private investment in cybersecurity.

Lack of private investment

The 2016 NCSS was explicit that organizations and company boards must invest – in technology, staff, systems and their supply chains in order to 'maintain a level of cybersecurity proportionate to the risk' (Cabinet Office 2016a, 41). This was in light of the fact that vulnerabilities are expected to significantly increase as interconnected systems are progressively being deployed (Tanczer et al. 2018).

While the question of how exactly boards understand and evaluate cyber risk is not yet clear, some useful research is emerging (Schatz and Bashroush 2017). Surveys such as the PWC *Global Investor Review* show that cyberthreats are the number one concern for investors and number three for CEOs (PwC 2018). And the NYSE Governance Services (2015) identified that

cybersecurity is discussed at 80 per cent of all board meetings with yet, a mere 11 per cent of corporate directors believing their boards possess a high-level of understanding of cybersecurity risk. So, with cybersecurity clearly on boards' agendas, the reasons for failure to achieve the level of investment expected by the government most likely reside elsewhere.

For one, government perceptions of cyber risk as well as the appropriate measures and levels of investment to mitigate against them may vary significantly from those of the private sector. Boards tend to view cybersecurity as they do any other business risk and assess them in terms of, for example, business continuity, return on investment and risk management. These factors do not always align with the views of governments, who take a broader perspective and consider the close relationship between the digital economy, national security and societal interests.

For another, there can be a significant disjuncture between the information that boards feel they need to base their decisions on and the amount of information that is available to them in the information security context. In early work carried out as part of an NCSC-supported research project, it was found that the providers of cybersecurity primarily focused on technical factors that are not easily translated into business relevant measures (Carr et al. 2018b). For example, security practitioners noted that useful metrics for the board include information like 'number of detected network intrusions' and 'number of password resets requested'. Consumers of such metrics on the other hand (from the board and policy community), recorded their preference for information as 'return on investment', 'impact on business continuity' and 'what their uninsured risk is' (Carr et al. 2018b).

Equally overlooked has been the role of the SME sector, partially due to anxiety about critical infrastructure protection and the need for collaboration with the owners and operators of critical information infrastructure (Stoddart 2016). Hence, the SMEs were, until recently, less considered in the context of national cybersecurity (Bell 2017). This was problematic for several reasons. First, SMEs frequently lack the resources to employ security practitioners. Consequently, these organizations tend to be disproportionately vulnerable. Second, SMEs are often part of the supply chain for larger firms and therefore can add weakness to otherwise strong security postures. Acknowledging these vulnerabilities, the NCSC focused its efforts on supporting this sector (National Cyber Security Centre 2017) and encouraged initiatives such as the DCMS-backed National Security Strategic Investment Fund (NSSIF).

Digital skills gap

The third market failure that drew the attention of the UK government was the cybersecurity skills gap. One of the key challenges facing governmental efforts to shape the industrial structure of the cybersecurity sector involves the recruitment and retention of skilled personnel. Midway through the first NCSS period, a competitive analysis of the UK cybersecurity sector identified the skills gap as one of the key barriers to UK's cybersecurity growth (Pierre Audoin

Consultants 2013). According to the Global Information Security Workforce Study (GISWS) study, there is expected to be a global cyber security workforce shortage of 1.8 million cybersecurity professionals by 2022 (Center for Cyber Safety and Education and ISC(2) 2017). Low numbers of professionally accredited practitioners and the relatively high salaries commanded by those with experience pose challenges to the UK. The country shares these concerns with other states currently leading on cybersecurity, including Israel and the US (Culbertson et al. 2017).

The UK government has put significant resources, funding and programs towards addressing the skills gap but the problem persists. The skills gap, thus, continues to be perceived as a key market failure in the UK and to some extent, is seen as undermining all other efforts to develop a stronger cyber security industry as businesses and the public sector alike continue to struggle to recruit and retain talent. Diversity of the workforce is another key area for improvement, with computer science degrees continuing to attract far more male than female students (The Guardian 2016). The 2018 Cyber UK forum hosted by the NCSC was organized around the topic of diversity and extended the discussion beyond 'conventional' concepts such as gender, race or sexuality to include considerations such as 'neurological' diversity (National Cyber Security Centre 2018c).

Inventory of measures

There have been a number of initiatives introduced in the UK in order to address the market failures described above. These 'market modifying' and 'market substituting' approaches (Aggarwal and Reddie 2018) are outlined in more depth below and help to illustrate UK's industrial policy in cybersecurity. The 2016 NCSS explained that further government investment in the cybersecurity space is motivated by an understanding that 'the current approach will not in itself be sufficient to keep [the UK] safe' (Cabinet Office 2016a,13). In addition, 'a market based approach to the promotion of cyber hygiene has not produced the required pace and scale of change' and failed to guarantee that the UK has the vibrant cybersecurity sector and supporting skills base it needs (Cabinet Office 2016a,13-14).

Some of these market interventions include regulatory mechanisms to mitigate against data breaches and data exploitation. These activities were frequently driven by developments happening on the EU level and form a consequence of global pressure points on questions concerning privacy and security. Furthermore, there have been a range of skills and education initiatives intended to grow an indigenous cybersecurity workforce in the UK. The latter should help to improve the operations, composition and practices that are prevalent as well as lacking in this space. Lastly – although not a focus of the analysis here – there have been some 'market facilitating' measures to counter the lack of private investment by supporting promising start-ups to reach market viability.

Regulatory measures

Data breaches are an increasingly important element of overall cybersecurity frameworks. Through innovations like the Internet of Things, automation and machine learning, data and the integrity of data flows become ever more integral for the smooth functioning of organizations or states (Tanczer et al. forthcoming). Conversely, data also becomes a more valuable target for malicious activity. In addition, personally identifiable information is recognized to hold the potential for a range of violations of individual safety, privacy and security. This means that data breaches take on a new and more substantive significance. They are perceived not simply as a possible economic loss but also as a threat to social stability, human rights, and the delivery of critical services. Data breaches are also considered as one of the possible barriers to the wider uptake of emerging technologies and, thus, a threat to a digital economy premised on continuous innovation. Market interventions to address the earlier mentioned scale of data breaches have therefore increased in recent years and are a means to guarantee a fair playing field for consumers and industry stakeholders alike.

The General Data Protection Regulation

Most fundamentally, UK's transposition of the General Data Protection Regulation (GDPR (EU)2016/679) into a new Data Protection Bill in 2018 acted as a profound market modifying measure that will affect the UK beyond its exit of the European Union (EU and ICO 2017). The GDPR is a European response to several decades of market failure to protect and uphold rights online. It is intended to empower EU consumers and data subjects in a range of ways, including through the guarantee of informed consent, knowledge of data flows, and control over personal data use (Veale, Binns, and Ausloos 2018). The GDPR is also intended to provide an additional incentive to invest in the prevention of data breaches for organizations that collect and share personal data. The GDPR applies to any organization handling personally identifiable data of citizens of the EU as well as all organizations headquartered in the EU and the European Economic Area (EEA), regardless of the residence status of those who use their services.

Significantly this means that non-EU firms that handle personal data of EU citizens must now comply with the regulatory framework of the Union or face consequences. Since May 2018, organizations that suffer a breach of personal data can attract a penalty of up to 4 per cent of total global annual revenue or €20 million (whichever is greater). In effect, this is a fundamentally new approach to the territory of the market. It shifts the regulatory jurisdiction from simply territorially bound to a subject focused approach. It is an example of a regulatory innovation that moves beyond the 'transnational corporation' model to a market provision that recognizes the global nature of an individual's data footprint – a change of great importance in terms of accommodating emerging technologies that will further intensify data collection and usage.

The 2016 NCSS refers to the GDPR as a lever to ‘drive up standards of cyber security’ (Cabinet Office 2016a, 27). The NCSC stipulates that this approach ‘does not mandate a specific set of cyber security measures’. Rather, it places the expectation on organizations to take ‘appropriate’ action. While this leaves the responsibility for managing risk in the hands of the organization, it provides much more clarity to boards and investors about how that risk is to be understood and perceived (National Cyber Security Centre 2018a).

ePrivacy Directive

In 2015, the European Commission undertook a Regulatory Fitness and Performance (REFIT2) evaluation in order to assess the extent to which the ePrivacy Directive (2009/136/EC) – which deals with the regulation of a number of important issues such as the treatment of traffic data, spam and cookies – was still applicable. The evaluation found that although the Directive continued to be relevant to the objectives of ensuring privacy and confidentiality of communications, ‘some of its rules are no longer fit for purpose in light of technological and market developments and changes in the legal framework’ (European Commission 2017, 2).

Significantly for this article, the ePrivacy Directive was found to be placing an unfair burden on some market players over others. Providers of electronic communication services were subject to rules that did not apply to Over-the-Top services (OTT) such as Voice over Internet Protocol providers like Skype. This was creating a ‘regulatory asymmetry’ and an unintended market advantage for OTT services (European Commission 2017, 3). An updated Directive is currently under development and will soon add another market modifying measure to the UK’s industrial cybersecurity toolkit.

Networks and Information Systems (NIS) Directive

In May 2018, the UK transposed the EU Networks and Information Systems Directive (NIS Directive 2016/1148) into national law. This move reflects the understanding of the criticality of information infrastructure to the provision of essential services in the UK. The NIS Directive aims to ‘raise levels of the overall security and resilience of network and information systems’ (National Cyber Security Centre 2018b). It establishes a legal framework to ensure that the owners and operators of critical systems take ‘appropriate and proportionate security measures to manage risks to their network and information systems’.

As with the GDPR, these measures are not specified and what constitutes ‘appropriate and proportionate’ is not clearly defined. Thus, organizations have to assess their risk independently and propose methods to mitigate against it. This leaves owners and operators of essential services with an opportunity to propose methods and procedures that can foster innovation which may lead to a comparative market advantage. Failure to do so exposes organizations to

consequences and they are now required to notify serious incidents to their relevant national authority.

These shifts in regulatory approaches are indicative of a growing acknowledgement that the market has failed to deliver what is regarded as adequate levels of cybersecurity – both in terms of protecting data and in terms of protecting critical systems. While the UK has responded to these market failures with market modifying regulatory instruments, in other areas such as the continuous skills gap, market substituting initiatives have been implemented.

Skills initiatives

Market substituting initiatives are those that involve the allocation or redistribution of resources in pursuit of desired outcomes (Aggarwal and Reddie 2018). The clear link between the UK market's competitiveness and the update and application of technology in the workforce was highlighted in the *Digital Skills for the UK Economy Report* (Business, Innovation and Skills and Department for Digital, Culture, Media and Sport 2016) as well as the *Digital Skills Crisis Report* both of which were published in the same year (Science and Technology Committee 2016). The two documents revealed the mismatch between the types of skills on offer in the present UK labour market and those skills demanded in the field. The publications uncovered a market failure that the UK government would have to address. They re-emphasized points made repeatedly throughout the past years, bringing greater attention to cybersecurity education and heightening the pressure for additional government interventions.

There have been two clear points of focus in the UK's endeavours to improve indigenous skills through education. First, there have been some limited initiatives to enhance cybersecurity education for primary and secondary school students. This has been important because by late secondary school, UK students are typically specializing in only three subjects rather than a broad range as is common elsewhere. Hence, they begin to narrowly focus their education at a relatively young age. The second and much more extensive area of investment has come at the tertiary level through an array of funded PhD programmes and research initiatives. These activities have been largely linked to investments in the academic community with the establishment of dedicated research centres and institutes intended to work collaboratively with industry and government.

In terms of tertiary education and the academic research community, the establishment of Academic Centres of Excellence in Cyber Security Research (ACE-CSRs) was a major step and is supported by funded research activities such as the Cyber Security Body of Knowledge (CyBOK) project which aims to codify the foundational and generally recognized knowledge on cybersecurity (Rashid et al, 2018). ACE-CSR's establishment indicated a preference for concentrating resources and efforts rather than widely dispersing and potentially diluting them. Appointed institutions are considered to conduct

leading-edge, world-class research in cybersecurity and are expected to bid for both open research funding calls and some that are restricted to ACE-CSRs only.

At the primary and secondary school level, diverse initiatives such as a dedicated guide for teachers was produced and disseminated. The guide outlined the range of cybersecurity programmes, learning resources, and activities for schools and further education (Department for Business, Energy and Industrial Strategy 2015). It was meant to support teachers in incorporating cybersecurity into their daily practices. Additionally, an accreditation programme for primary and secondary teachers who wish to gain more knowledge about cybersecurity and disseminate skills to students was set in place. This Cyber Aware Teacher Continuing Professional Development (CPD) is a series of free online resources ranging from modules on password security to information about malware and other cybersecurity threats.

A core piece in all these efforts was the publication of a dedicated UK Digital Strategy, released in February 2017 (Department for Culture, Media and Sport 2017). The document proposed a range of initiatives and followed up on the earlier issued Industrial Strategy. In spite of its intentions, including training opportunities offered by large private sector organizations, the UK Digital Strategy has been criticized by industry actors for not having provided enough detail to make its proposals credible (Reeve 2017). While it remains to be seen if the Strategy and all the collective activates deployed over the past years will allow the UK to tackle the pressing cybersecurity skills gap, the government has certainly highlighted its active commitment to pursue interventions in this realm.

State society dynamics

As this article demonstrates, UK's drivers, market failures, and interventions are characteristic of a government that has been in fairly close engagement with the industrial sector. A collegial relationship marks their cooperation, considering that both the public and the private sector equally share data security concerns as well as recruitment problems.

Most recently the Digital Skills Partnership is one of the outcomes of this intensified public-private liaison. Part of a market substituting move which pledges £20 million for digital training and extracurricular school programmes (Department for Business, Energy and Industrial Strategy 2017, 109), the UK government also put forward a range of courses offered from private sector organizations such as Google, Lloyds Banking Group and Barclays. While these activities raise the responsibility for industry stakeholders to a new level, it still carries the handwriting of both public and private players.

In terms of regulatory shifts, many companies continue to express concern at the cost and complexity of cybersecurity and data protection compliance. Yet, as recent events such as the Cambridge Analytica/Facebook misuse of personal data and the allegations of public opinion shifts in US and UK elections

have showcased, there is a growing recognition that the private sector has not been sufficiently stimulated by market drivers to implement appropriate levels of either privacy or security. It is too early to gauge the impact of these recently introduced market interventions, but it is reasonable to conclude that their implementation marks a change in the dynamics between state, society and the private sector.

With regard to skills development, past efforts may have yielded fruit. The most recent A-level (final high school examination) results lists mathematics as the most popular A-level with mathematics and further mathematics having nearly 25 per cent more entries than in 2010 (SC Media UK 2017). Whether the rising number of students interested in this subject is due to the greater awareness of career opportunities associated with cybersecurity as a consequence of all government initiatives, remains unclear; but it is certainly an important and promising indicator of movement in the right direction.

The UK's strong emphasis on education as a form of industrial policy and the breadth of measures taken to close the digital skills gap can also be a helpful tool for fostering multilateral cooperation in this space. The first NCSP invested £8.1 million in international engagement and capacity building (Cabinet Office 2016b). These initiatives were primarily focused on strengthening transborder cooperation to reduce cybercrime (Saunders 2017) and UK's participation in multinational exercises to strengthen skills and operational links with other nations.

Conclusion

In closing, the UK case provides some interesting contrasts from the past to the present (and likely future). It offers an important analysis of the shift away from a reliance on market forces that dominated Western approaches to cybersecurity over the recent years. Key changes in UK's industrial policy for cybersecurity have emerged through the sentiment that the market has not delivered adequately – either in scale or in scope. This has been examined through the comparison of two consecutive NCSS, with the 2016 NCSS explicitly highlighting the nature of market failures that have characterized the sector in the UK. These market failures are seen through: (a) ongoing (preventable) data breaches; (b) a failure of the private sector to invest adequately in cybersecurity; and (c) a continuous digital skills gap.

The initiatives implemented to address these market failures have predominantly taken the form of market modifying and market substituting approaches. New regulatory frameworks like the GDPR, the ePrivacy, and the NIS Directive all take a more assertive tone and direct the private sector to deliver data security and data protection. They are also more aligned with the government's aim for the digital economy to yield benefits to the UK. Market substituting activities such as the outlined skills initiatives complement these regulatory measures and are meant to tackle the sustained recruitment and retention problems of skilled personnel.

Essentially, designing and implementing an industrial strategy for cybersecurity for any country is only a small part of the challenge. Rather, as this special issue highlights, the real challenge lies in understanding the particular dynamics and drivers which are fit for an increasingly globalized, interdependent market and align with the expectations of society that is moving further into the fourth industrial revolution.

References

Aggarwal, V.K., and A. Reddie. 2018. “Comparative Industrial Policy and Cybersecurity: A Framework for Analysis.” Working paper, September 2018. California: Berkeley APEC Study Center.

Bada, M., I. Arreguín-Toft, I. Brown, P. Cornish, S. Creese, W. Dutton, and D. Upton. 2016. *Cybersecurity Capacity Review of the United Kingdom*.pdf (1–74). Oxford: Global Cyber Security Capacity Centre. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf

Bell, S. 2017. “Cybersecurity is Not Just a ‘Big Business’ Issue.” *Governance Directions* 69(9): 536.

Brass I., L. Tanczer, M. Carr, and J. Blackstock. 2017. “Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things?”. *Risk and Regulation Magazine* 2017(3): 12-15.

Bossong, R., and B. Wagner. 2017. “A Typology of Cybersecurity and Public-private Partnerships in the Context of the EU. *Crime, Law and Social Change* 67(3): 265–288. https://doi.org/10.1007/s10611-016-9653-3

Business, Innovation and Skills Committee. 2016. *The Digital Economy* (HC87:37). London: House of Commons. Retrieved from https://publications.parliament.uk/pa/cm201617/cmselect/cmbis/87/87.pdf

Cabinet Office. 2011. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. London: HM Government.

Cabinet Office. 2016a. *National Cyber Security Strategy 2016-2021*. London: HM Government.

Cabinet Office. 2016b. *The UK Cyber Security Strategy 2011-2016*. Annual Report. London: Cabinet Office.

Carr, M. 2016. “Public-Private Partnerships in National Cyber Security Strategies.” *International Affairs* 92(1):43-62.

Carr, M., Dawda S., Chung, A., Hussain, A., & Shaikh, S.A. (2018). Cybersecurity in UK HMG: Mapping the Landscape. London: STEaPP Research Paper Series.

Carr, M., and B. Sam. 2018b. “Cyber Security Metrics: The View from Both Sides of the Board Table.” *Digital Policy Lab Paper Series*. London: UCL STEaPP.

Center for Cyber Safety and Education. 2017. *(ISC)2: Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes*

Rise Higher. Retrieved from http://www.prnewswire.com/news-releases/global-cybersecurity-workforce-shortage-to-reach-18-million-as-threats-loom-larger-and-stakes-rise-higher-300469866.html

Chakravorti, B., and R.S. Chaturvedi. 2017. *Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World*. Medford, Massachusetts: The Fletcher School, Tufts University.

Corrales, J., and F. Westhoff. 2006. "Information Technology Adoption and Political Regimes." *International Studies Quarterly* 50(4): 911–933. https://doi.org/10.1111/j.1468-2478.2006.00431.x

Couzigou, I. 2018. "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations. *International Review of Law, Computers & Technology* 32(1): 37–57. https://doi.org/10.1080/13600869.2018.1417763

Crick, T., and F. Moller. 2015. "Technocamps: Advancing Computer Science Education in Wales." In *Proceedings of the Workshop in Primary and Secondary Computing Education*, 121-126. doi:10.1145/2818314.2818341. London: ACM.

Culbertson, D., D. Humphries, G.M. Ivy, J. Kolko, and V. Rodden. 2017. *Indeed Spotlight: The Global Cybersecurity Skills Gap*. Retrieved from http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/

Department for Business, Energy and Industrial Strategy (BEIS). 2015. *Cyber Security: Guide to Programmes and Resources for Schools and Further Education*. London: HM Government.

Department for Business, Energy and Industrial Strategy (BEIS). 2017. *Industrial Strategy: Building a Britain Fit for the Future*. London: HM Government.

Department for Business, Innovation and Skills (BIS) and Department for Digital, Culture, Media and Sport (DCMS). 2016. *Digital Skills for the UK Economy*. London: HM Government.

Department for Culture, Media and Sport (DCMS). 2017. *UK Digital Strategy 2017*. London: Department for Culture, Media and Sport.

Department for Digital, Culture, Media and Sport (DCMS). 2018. *Cyber Security Breaches Survey 2018*. London: Department for Digital, Culture, Media and Sport.

Department for International Trade (DIT). 2018. *Cyber Security Export Strategy*. London: Department for International Trade.

European Commission. 2017. *Executive Summary of the Ex-post REFIT Evaluation of the ePrivacy Directive 2002/58/EC*. Brussels. Retrieved from

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0005&from=EN

European Union Agency for Network and Information Security (ENISA). 2012. *National Cyber Security Strategies*. Heraklion, Greece: European Union Agency for Network and Information Security.

The Guardian. 2016. “Gender Gap in UK Degree Subjects Doubles in Eight Years, Ucas Study Finds.” London: The Guardian.

The Information Commissioner’s Office (ICO). 2017. *Response to Consultation on Updating Ofcom’s Guidance on Security Requirements in Sections 105A to D of the Communications Act 2003*. September. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0028/106957/ICO.pdf

ITU, The World Bank, ComSec, CTO, and NATO CCD COE. 2018. *Guide to Developing a National Cybersecurity Strategy - Strategic Engagement in Cybersecurity*, 76. Geneva: International Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Kane, A. 2014. “The Rocky Road to Consensus: The Work of UN Groups of Governmental Experts in the Field of ICTs and in the Context of International Security, 1998–2013.” *American Foreign Policy Interests* 36(5): 314–321. https://doi.org/10.1080/10803920.2014.969175

Kleinhans, J.-P. 2017. *Internet of Insecure Things. Can Security Assessment Cure Market Failures?* Berlin: Stiftung Neue Verantwortung. Retrieved from https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf

Matania, E., L. Yoffe, and T. Goldstein. 2017. “Structuring the National Cyber Defence: in Evolution Towards a Central Cyber Authority.” *Journal of Cyber Policy* 2(1), 16–25. https://doi.org/10.1080/23738871.2017.129919

Morris, D. 2012. “ICT and Educational Policy in the UK: Are we on the Way Towards E-maturity or on the Road to Digital Disaster?” *Res. Teach. Educ*. 2: 308.

National Crime Agency (NCA) and National Cyber Security Centre (NCSC). 2018. *The Cyber Threat to UK Business: 2017 – 2018 Report*. London: NCA and NCSC.

National Cyber Security Centre (NCSC). 2017. *Cyber Security: Small Business Guide*. Retrieved from https://www.ncsc.gov.uk/smallbusiness

National Cyber Security Centre (NCSC). 2018a. *General Data Protection Regulation*. 18 May. Retrieved from https://www.ncsc.gov.uk/GDPR.

National Cyber Security Centre (NCSC). 2018b. *Introduction to the NIS Directive*. 30 April. Retrieved from https://www.ncsc.gov.uk/guidance/introduction-nis-directive.

National Cyber Security Centre. 2018c. 'Diversity and Inclusion at CYBERUK 2018', *NCSC Blog*. February 2, 2018. https://www.ncsc.gov.uk/blog-post/diversity-and-inclusion-cyberuk-2018

NYSE Governance Services. 2015. *Cyber Security in the Boardroom*. Retrieved from https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf

Office for National Statistics (ONS). 2017. *Annual Population Survey (APS): Population of the UK by Country of Birth and Nationality 2016*. London: Office for National Statistics.

Pierre Audoin Consultants. 2013. *Competitive Analysis of the UK Cyber Security Sector*. London: Department for Business, Innovation and Skills.

Priday, R. 2018. *The Ticketmaster Hack is a Perfect Storm of Bad IT and Bad Comms*. Wired. 28 June. Retrieved from http://www.wired.co.uk/article/ticketmaster-data-breach-monzo-inbenta

PwC (2018). 2018 Global investor survey 2018: Anxious optimism in a complex world. London: PwC. Retrieved from https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2018/gx/deep-dives/2018-global-investor-survey.html

Rashid, A., G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis, and C. Peersman. 2018. "Scoping the Cyber Security Body of Knowledge." *IEEE Security Privacy* 16(3): 96–102. https://doi.org/10.1109/MSP.2018.2701150

Reeve, T. 2017. *UK Post-Brexit Digital Strategy Criticised by Cyber-Security Industry*. [WWW Document]. SC Media UK. Retrieved from https://www.scmagazineuk.com/news/uk-post-brexit-digital-strategy-criticised-by-cyber-security-industry/article/641036/

Research Institute for Science of Cyber Security (RISCS). 2018. *Analysis of Cyber Metrics Workshop*. 23 May. London: RISCS.

Saunders, J. 2017. "Tackling Cybercrime – the UK Response." *Journal of Cyber Policy* 2(1): 4–15. https://doi.org/10.1080/23738871.2017.1293117

SC Media UK. 2017. *Students Offer Hope for Narrowing of Skills Gap in Cyber-security*. [WWW Document]. SC Media UK. Retrieved from https://www.scmagazineuk.com/news/students-offer-hope-for-narrowing-of-skills-gap-in-cyber-security/article/682418/

Schatz, D., and R. Bashroush. 2017. “Economic Valuation for Information Security Investment: A Systematic Literature Review.” *Information Systems Frontiers* 19(5): 1205–1228. https://doi.org/10.1007/s10796-016-9648-8

Science and Technology Committee. 2016. Digital Skills Crisis: Second Report of Session 2016–17 (HC 270). London: House of Commons.

Štitilis, D., P. Pakutinskas, and I. Malinauskaitė. 2016. “EU and NATO Cybersecurity Strategies and National Cyber Security Strategies: A Comparative Analysis.” *Security Journal* 30(4): 1151–1168. https://doi.org/10.1057/s41284-016-0083-9

Stoddart, Kristan. 2016. “Live Free or Die Hard: U.S.–UK Cybersecurity Policies.” *Political Science Quarterly* 131 (4): 803–42. https://doi.org/10.1002/polq.12535.

Tanczer, L., I. Brass, M. Elsden, M. Carr, and J. Blackstock. (forthcoming). “The United Kingdom’s Emerging Internet of Things (IoT) Policy Landscape. In *Rewired: Cybersecurity Governance*, edited by R. Ellis and V. Mohan. Hoboken, New Jersey: Wiley.

Tanczer, L., I. Steenmans, I., Brass, and M. Carr. 2018. *Interconnected World:* Emerging Risks and Opportunities in the Internet of Things (IoT). London: Lloyd’s of London.

Taylor, P., S. Allpress, M. Carr, E. Lupu, J. Norton, L. Smith, J. Blackstock, H. Boyes, A. Hudson-Smith, I. Brass, H. Chizari, R. Cooper, P. Coulton, B. Craggs, N. Davies, D. De Roure, M. Elsden, M. Huth, J. Lindley, C. Maple, B. Mittelstadt, R. Nicolescu, J. Nurse, R. Procter, P. Radanliev, A. Rashid, D. Sgandurra, A. Skatova, M. Taddeo, L. Tanczer, R. Vieira-Steiner, J.D.M. Watson, S. Wachter, S. Wakenshaw, G. Carvalho, R.J. Thompson, and P.S. Westbury. 2018. *Internet of Things: Realising the Potential of a Trusted Smart World*. London: Royal Academy of Engineering.

Veale, M., R. Binns, and J. Ausloos. 2018. “When Data Protection by Design and Data Subject Rights Clash.” *International Data Privacy Law* 8(2): 105–123. https://doi.org/10.1093/idpl/ipy002

Zerlang, J. 2017. “GDPR: A Milestone in Convergence for Cyber-security and Compliance.” *Network Security* 2017(6): 8–11. https://doi.org/10.1016/S1353-4858(17)30060-0