BASC WORKING PAPER SERIES

UK CYBER SECURITY POLICY: THE SOCIO-TECHNICAL FACTORS

Madeline Carr
Leonie Tanczer

Working Paper 2018-09

BERKELEY APEC STUDY CENTER
552 Barrows Hall
University of California
Berkeley, California 94720-1950
September 2018

This paper is part of a project "Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications," organized by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center and funded by the Center for Long-Term Cybersecurity at the University of California, Berkeley. The authors wish to acknowledge the Engineering and Physical Sciences Research Council (EPSRC) and the Department of Digital, Culture, Media and Sport (DCMS) which provided funding for this work through the PETRAS Research Hub into the Cyber Security of the Internet of Things. We would also like to thank the Center for Long-Term Cybersecurity, BASC, UC San Diego's Institute on Global Conflict and Cooperation and UC Berkeley's Institute for East Asian Studies for supporting the broader project. For helpful comments in the drafting of this manuscript, we'd like to thank Stephan Haggard, Michael Adams, and Andrew Reddie.

UK Cyber Security Policy: The Socio-technical Factors
Madeleine Carr and Leonie Tanczer
BASC Working Paper No. 2018-09

Abstract

The UK has the largest internet economy in the G20 and has the stated ambition of making the UK the 'safest place in the world to live and work online'. Cyber security has been elevated to a 'tier one' threat and is regarded by the government as both a challenge and as an opportunity for exporting UK expertise. Since the publication of the UK's National Cyber Security Strategy (NCSS) in November 2011, the government has implemented many proactive as well as reactive measures to enhance both its cyber security capabilities as well as its market power. This article provides an analysis of the shift away from a reliance on market forces that dominated Western approaches to cyber security over the early years of this century. Specifically, it highlights three 'market failures' that have prompted UK policy responses: ongoing data breaches, the skills gap and inadequate private investment in cyber security. An analysis of these drivers as well as the responses demonstrates that the UK's cyber security strategy has evolved from an initial heavy reliance on market forces and the public-private partnership to mitigate against threats into what is now a confident, rounded approach to balancing threats and opportunities.

Madeleine Carr[1]
University College London STEaPP
Boston House
36-37 Fitzroy Square
London W1T 6EY
m.carr@ucl.ac.uk

Leonie Tanczer[2]
University College London STEaPP
Boston House
36-37 Fitzroy Square
London W1T 6E
l.tanczer@ucl.ac.uk

[1] Madeline Carr is Associate Professor in International Relations and Cyber Security at University College London with a focus on global cyber security and Internet governance. She is also the Director of the UCL Research Institute in Science of Cyber Security (RISCS). Her research is embedded in a broad study of the ways in which new technology both reinforces and disrupts conventional frameworks for understanding International Relations and the implications of this for state and global security, order and governance.

[2] Leonie Maria Tanczer is a Lecturer in International Security and Emerging Technologies and has a research interest on the intersection of technology, security, and gender.
Prior to her lectureship appointment, she was Postdoctoral Research Associate for the EPSRC-funded PETRAS Internet of Things (IoT) Research Hub, where she was part of the "Standards, Governance and Policy" research stream.Dr Tanczer holds a PhD from the School of History, Anthropology, Philosophy and Politics at Queen's University Belfast (QUB).

1. Introduction

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

The UK government upholds an active commitment to fostering its international status in this sector. Since the publication of the UK's National Cyber Security Strategy (NCSS) in November 2011, the government has implemented many proactive as well as reactive measures to enhance both its cyber security capabilities as well as its market power. 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 cyber security vision from 2016 to 2021 (Cabinet Office 2016a). 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 and the public-private partnership to mitigate against threats into what is now a confident, rounded approach to balancing threats and opportunities. The UK is therefore a useful case study as it can be expected to be emulated by others.

Having been nominated as a 'tier one' threat, cyber security is now central to UK national security. Over the years, the government's efforts to improve cyber security 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, Innovation and Skills, the Government Communications Headquarters (GCHQ), the Department for Digital, Culture, Media and Sport (DCMS) and most recently, the Department for International Trade. These and other institutions and agencies are at the forefront of the attempts to make the UK not only resilient to digital attacks or system failures, but also to promote the UK's cyber security industry and enhance development and growth in this space.

Cyber security is central to the UK government's aim to make the UK 'the safest place in the world to live and work online' and one of the world's leading digital nations (NCA 2018, 2). This theme runs through major policy documents including the Digital Strategy, the Digital Charter, the Cyber Security Export Strategy and the National Cyber Security Strategy. However, one of the discursive challenges one faces in discussing cyber security is the breadth and depth of the landscape that the term can refer to. This introduces a number of complexities facing those responsible for developing national cyber security strategies and corresponding policies. First, cyber security intersects with a wide range of sectors, economic factors and issue areas. Second, and relatedly, it affects diverse groups of actors in different ways. Third, and critically for policy makers, these sectors and actors can have competing or even conflicting interests and agendas – all of which need to be taken into account, balanced and addressed in a (hopefully) cohesive manner. Complicating all of this, is the rapid pace that digital technologies continue to be developed and incorporated into societal practices, processes and institutions.

There are a number of key issues that drive UK policy on cyber security. These include domestic level factors common to many states, an ambition to grow the cyber security industry including as an export sector, and the expectation that the UK will continue to play a global leadership role in cyber security. In the following, we examine the UK's development of industrial policy to configure its cybersecurity market (Aggarwal and Reddie 2018).

Domestic Cyber Security

In common with every industrialized state, ensuring a level of cyber security in the domestic context is a high priority in 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. 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. The broader implications of this law and order element for social stability and the enforcement of the social contract are as important online as they are in the physical world.

Critically for governments like the UK, addressing these expectations is understood to be fundamental to further optimizing the benefits of the digital economy and the future of innovation. Maintaining public confidence in the uptake of emerging technologies is seen as central to their widespread adoption and this, in turn, is central to maximizing the considerable public benefits believed to derive from intensified implementation of digital technologies. Technological adoption and acceptability is also believed to have significant implications for the 'digital economy' and this creates a direct link to national security. 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' (BEIS 2017, 40).

Growing the Cyber Security Industry

The imperative of providing cyber security support to UK businesses is linked to the future prospects of the digital economy. Of particular concern are small and medium enterprises (SMEs) which often lack the resources and expertise that larger firms draw upon for their own cyber security (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.

In addition, the UK also regards the cyber security industry as a global export service that has implications for continuing to build the reputation of the UK as a global leader in the cyber security sector. In 2018, the Department for International Trade produced its *Cyber Security Export Strategy* in which it projects exports growing to £2.6B by 2021 (DFIT 2018, 12). However, growing both the internally and externally facing cyber security sectors is hampered by recruitment and retention challenges as relevant personnel are highly valued and operate within a fluid and dynamic job market. These recruitment and retention challenges are often expressed in terms of the 'skills gap' which is addressed through multiple initiatives including the £20M Cyber Discovery Programme announced in the *Industrial Strategy* which is expected to engage 6,000 school children by 2021 (BEIS 2017, 109).

International Dimension

The UK has played (and aspires to continue to play) a global leadership role in terms of international cooperation on cyber security debates and negotiations. This is evident in its prominent role in various international fora where cyber security is negotiated such as the UN Group of Governmental Experts on Developments in the field of information and telecommunications in the context of international security (UNGGE) which works to develop consensus on exactly what constitutes responsible state behaviour in cyberspace. This ambition to global leadership is also evident in the UK's establishment of the Global Conference on Cyber Security – otherwise known as the 'London Process'. This meeting was initiated to provide a space for political actors (and industry/third sector) to discuss mechanisms for practical cooperation, to develop cyber norms, and to work on capacity building measures that will enhance global cyber security.

The UK's engagement with international aspects of cyber security 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 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 project is that of market failures and responses to those market failures. The three key issues of concern outlined above have been analysed in this paper through a comprehensive study of UK cyber security initiatives. In the UK case, market failures have been identified and drawn out through the analysis of two consecutive National Cyber Security Strategy documents.

The first UK National Cyber Security Strategy was published in 2011 and covered the five subsequent years to 2016. The second UK National Cyber Security Strategy 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 paper proceeds as follows. First, we outline three major market failures that emerged from the comparison of these two strategy documents. These include ongoing data breaches, failure of the private sector to invest adequately, and the skills gap. We then introduce the major initiatives that the UK has implemented to address those market failures. Following this, we discuss the state-society dynamics particular to the UK which influence decision making on approaches to cyber security market failures and we highlight some of the effects of the initiatives undertaken before drawing conclusions about the UK's overall posture.

2. Market Failures in the UK

As discussed earlier, governments are engaged with cyber security on so many levels and in so many ways that discussing any dimension of it in a homogenous way is not possible. A recent mapping study of cyber security 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, forthcoming 2018). 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 National Cyber Security Strategy issued in 2011 to its second issued in 2016.

National Cyber Security Strategies reveal much about the way a government perceives the issue at a less granular level. They are carefully crafted to draw out the issues of most significance to the state and provide insight into perceptions of the UK's place in an international order as well as its domestic conditions. 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 cyber security more quickly and efficiently than they would with the burden of government intervention.

While the UK still takes a relatively light touch to cyber security regulation, the failure of the market to adequately resolve persistent and wide spread cyber insecurity resulted in a notable shift from the National Cyber Security Strategy produced in 2011 to the follow-on strategy released in 2016. In 2011, much was left to the market to 'drive the right behaviours' (Cabinet Office 2016a, 27) but in 2016, it was explicitly acknowledged that 'the combination of market forces and government encouragement has not been sufficient in itself to secure our long-term interests in cyberspace at the pace required' (Cabinet Office 2016a, 27). 'The market is not valuing, and therefore not managing, cyber risk correctly' (Cabinet Office 2016a, 27). While there are many dimensions of cyber security that the UK government recognizes as within its own mandate and sphere of responsibility, there are some aspects that are considered critical to the national interest but remain in the dominion of the private sector.

The 2016 NCSS states that in 2011, the government expected that a combination of 'commercial pressures and government-instigated incentives to ensure adequate business investment in appropriate cyber security' would 'stimulate a flow of investment into our industry' and 'encourage an adequate pipeline of skills into the sector' (Cabinet Office 2016a, 27). Despite some progress, 'the combination of market forces and government encouragement has not been sufficient' and consequently, while the market continues to have a role to play, the government must now 'set the pace in meeting the country's national cyber security needs' (Cabinet Office 2016a, 27). The language of this document could not be more clear - the UK recognized and responded to a market failure in cyber security.

These two documents highlight what the UK government's expectations were in terms of the cyber security sector, which of those expectations were not met in the five-year interim period, and what measures the UK government planned to put in place in order to mitigate against these 'market failures'. Three primary (and related) issues emerged as requiring additional government intervention: continued insecurity of private sector networks, a lack of private investment in the sector, and the skills shortage.

Ongoing Data Breaches

Like the US and other countries with major digital economies, the UK has experienced a number of high profile data breaches, notable both for the scale of the data lost and for the sensitivity of the exposed data. Global incidents like the Uber, Yahoo and Equifax breaches affected many UK citizens by exposing their personal and financial data. A 2018 attack on UK ticket re-seller Ticketmaster further exposed the vulnerabilities inherent in complex supply chains as a sub-contractor operating a service on the Ticketmaster website was found to be responsible. (Priday 2018). The problem goes beyond large firms though. The 2018 UK Data Breaches Survey found that 43% of UK businesses identified at least one breach or attack in the last year (DCMS 2018, 1).

While there is some agreement that eliminating the potential for data breaches altogether is perhaps not realistic, each of these events raised questions about whether the business in question had acted responsibly or in line with government and societal expectations to protect sensitive data. A joint report published by the National Crime Agency and the National Cyber Security Centre detailed the UK response to some of the biggest recent data breaches. It explained that in the case of the Verizon data breach that exposed the customer data of 14 million people, the access was obtained simply by guessing the correct web address. The Uber breach involved the data of 57 million accounts which was 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' (NCA, 2018, p.10).

In October 2015, UK telco TalkTalk suffered a significant breach. Although the number of affected customers was not especially high, this event marked a shift in government and public tolerance for data breaches – especially those seen to have been easily preventable. 'Too 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 suggestion that businesses had been lacking was part of a narrative around a failure at the board level to invest adequately in cyber security.

Lack of Private Investment

The new National Cyber Security Strategy is explicit that organizations and company boards must invest – in technology, staff, systems their supply chains in order to 'maintain a level of cyber security proportionate to the risk' (Cabinet Office 2016a, 41). However, exactly *how* boards understand and evaluate cyber risk is not clear. Government perceptions of cyber risk as well as the appropriate measures and levels of investment to mitigate against that risk can vary significantly from those of the private sector (Carr 2016). Boards view cyber security as any other business risk and assess it in terms of factors like business continuity, return on investment and risk management – factors that do not always align with the views of governments that take a broader view of the relationship between the digital economy, national security and the national interest.

In addition, it has become clear that there can be a significant disjuncture between the motivation for boards to invest in cyber security and the drivers presented to them from their technical executives. In recent work carried out as part of a larger research project into board incentives for cyber security investment, it was found that the providers of cyber security metrics focused on technical factors that are not (or are unable to be) translated into business relevant metrics (Carr and ?? 2018). For example, providers noted that useful metrics for the board include 'DNS trace data above recursive resolver', 'number of detected network intrusions' and 'number of password reset requests'. Consumers of metrics on the other hand (board and policy community), recorded their preferences as including 'return on investment', 'metrics in terms they understand, e.g. business language' and 'what their uninsured risk is' (Carr and ?? 2018).

Skills Gap

One of the key challenges facing these governmental efforts to shape the industrial structure of the cybersecurity sector involves the recruitment of personnel. According to the Global Information Security Workforce Study (GISWS) study, there is expected to be a global cybersecurity workfare shortage of 1.8 million cybersecurity professionals by 2022 (Center for Cyber Safety and Education and (ISC)2, 2017). The demand for these professionals would be strongest in Israel, followed by Ireland and the UK (Culbertson et al., 2017). A competitive analysis of the UK cybersecurity sector by Pierre Audoin Consultants for the Department for Business, Innovation and Skills in (2013) revealed that one of the key barriers to UK's cybersecurity growth is the availability of skills. Similarly, the National Audit Office expressed concern over the lack of suitable cybersecurity employees (Morse, 2013). Low numbers of professionally accredited practitioners and the relatively high salaries commanded by those with experience are some of the dilemmas that the UK market is facing.

The UK government has put significant resources towards this with many, many initiatives, programs and funding but the problem persists (Tanczer and Carr 2018). The skills gap continues to be perceived as a key market failure in the UK and to some extent, this skills gap is seen as undermining all other efforts to develop a stronger cybersecurity industry as businesses and the public sector alike continue to struggle to recruit and retain talent.

The UK government approaches these three distinct but related market failures in cyber security through a combination of incentives, guidelines, and pressure points. These can be understood at 'market modifying', 'market facilitating' and 'market substituting' initiatives. These are outlined below and help to further illustrate current UK industrial policy in cyber security.

3. Inventory of Measures

There have been a number of initiatives introduced in the UK in order to address the market failures described above. The 2016 NCSS explains that further government investment and initiatives are motivated by an understanding that ‘the current approach will not in itself be sufficient to keep [the UK] safe’ (Cabinet Office, 2016a, p.13). In addition, ‘a market based approach to the promotion of cyber hygiene has not produced the required pace and scale of change’ and ‘the UK needs a vibrant cyber security sector and supporting skills base’ (Cabinet Office, 2016a, p.13-14).

Some of these initiatives include regulatory mechanisms to mitigate against data breaches, specifically the EU General Data Protection Regulation (GDPR), the EU Network and Information Systems (NIS) Directive for critical infrastructure, (both of which are expected to be adopted if the UK exits the EU), and the UK Data Protection bill. There has also been a range of skills and education initiatives intended to grow an educated and able cyber security workforce. There have also been some 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 cyber security frameworks. As the world becomes ever more reliant on data flows (and the integrity of those data flows) through innovations like the Internet of Things, automation and machine learning, data becomes a more and more integral element of the smooth functioning of a state and more valuable target for malicious activity. In addition, personally identifiable data is recognized to hold the potential for a range of violations of individual safety, security, and human rights. This means that data breaches take on a new and more substantive significance as they are perceived as a threat to social stability and human rights. They are also perceived as one of the possible barriers to wider uptake of still emerging technologies and thus, a threat to the digital economy based on continuous innovation.

Regulatory approaches to data protection and privacy are currently (June 2018) under transition in the UK. The General Data Protection Regulation (GDPR) took effect on May 25, 2018. The Queen’s speech in June 2017 contained an announcement that the UK would be replacing the existing data protection legislation with a new Data Protection Bill which would effectively implement the GDPR (HRH Queen Elizabeth, 2017). This was confirmed in September 2017, when the Information Commissioner issued a statement to confirm that the UK’s departure from the EU would not affect the implementation of the GDPR (ICO, 2017).

These regulatory responses to market failures in cyber security can be understood as ‘market modifying’ initiatives. They involve the creation of regulations that attempt to change the conduct of key actors, the objects, medium or terms of exchange, in order to produce outcomes different from those the market would otherwise produce.

The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a European response to several decades of market failure to protect and uphold human rights online. It is intended to empower EU consumers and data subjects in a range of ways including enhanced consent, knowledge of data flow destinations, and control over personal data use. 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 doing business in the EU regardless of where they are headquartered.

Significantly this means that non-EU firms that handle personal data of EU citizens must now comply with the regulatory framework or face consequences. From May 2018, organizations that suffer a breach of personal data can attract a penalty of up to 4% 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 is an example of innovation in regulation that moves beyond the 'transnational corporation' model to an approach to market provision that recognizes the global nature of an individual's data footprint – a shift that will be important in terms of accommodating still emerging technologies and intensified data flows.

The 2016 NCSS refers to the GDPR as a lever to 'drive up standards of cyber security' (Cabinet Office 2016a, 27). The National Cyber Security Centre stipulates that this approach 'does not mandate a specific set of cyber security measures'. Rather, it places the expectation on organisations to take 'appropriate' action. This leaves the responsibility for managing risk in the hands of the board but it provides much more clarity about how that risk is to be understood and perceived (NCSC 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 had achieved its main objectives and whether these rules were still fit for purpose in an evolving regulatory and technological context. 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 paper, 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' (VoIP) services like Skype or instant messaging. This was creating a 'regulatory asymmetry' and an unintended market advantage for the providers of OTT services (European Commission 2017, 3). The Directive ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector.

The ePrivacy Directive forms the basis for the UK implementation of the Privacy and Electronic Communications Regulations (PECR). The deadline for updating these initiatives was the same as the GDPR – May 2018.

Networks and Information Systems (NIS) Directive

The UK is also implementing the EU directive on the security of Networks and Information Systems (known as the NIS Directive). This 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' (NCSC 2018b). The NIS Directive 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'. Again, as with the GDPR, these measures are not specified and 'appropriate and proportionate' are not defined. This leaves organisations to assess their risk independently and justify the measures they take to mitigate against it. Failure to do so would expose them 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 cyber security – both in terms of protecting data and in terms of protecting critical systems. In other areas of market failure like the 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. 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* (Department for Business, Innovation & Skills and Department for Digital, Culture, Media & Sport 2016) as well as the *Digital Skills Crisis Report* which were published in the same year (Science and Technology Committee 2016). Both documents revealed the mismatch between the types of skills on offer in the present 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.

Summary of the UK Government's Skills and Education Initiatives (2016)

Initiative/Policy/Publication	**Description**

Digital Skills for the UK Economy	Report aimed to improve the understanding of the current and future demand for, and supply of, digital skills in the UK economy
Cyber Aware Teacher Continuing Professional Development (CPD)	Course and accreditation for primary and secondary school teachers to gain more knowledge about cybersecurity and share it with their students
Digital Skills Crisis Report	A Science and Technology Committee report which highlighted that the UK faces a digital skills crisis
Certified Cyber Security Consultancy Scheme	Scheme to certify services providing proof that they meet the NCSC's standard for high quality, tailored cyber security advice
Cyber Retraining Academy	Initiative is run in partnership with SANS Institute and helps those already in the labour market to change careers and become cybersecurity professionals
National Cyber Security Strategy	UK’s second National Cyber Security Strategy was released in November
Digital, Data and Technology Profession	Commissioned by the Civil Service to lead on a number of cross-government actions, including the development of a national framework of digital, data and technology job roles
Cybersecurity in Computer Science	Cybersecurity becomes mandatory subject in UK’s computer science degrees

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, rather than a broad range, of subjects. 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 programs and research initiatives. These activities have been largely linked to investments in the academic community with the establishment of dedicated research centres and institutes.

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. This 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. These centres have good relations with the UK's National Cyber Security Centre (NCSC); although they were formally selected by the GCHQ and the Engineering and Physical Sciences Research Council (EPSRC) (National Cyber Security Centre 2017) which is the UK's main agency for funding research in engineering and the physical sciences.

At the primary and secondary school level, a dedicated guide for teachers was produced and disseminated, outlining the range of cybersecurity programs, learning resources, and activities for schools and further education (Department for Business, Energy & Industrial Strategy 2015). The guide was meant to support teachers in incorporating cybersecurity into their daily practices. Additionally, an accreditation program for primary and secondary teachers who wish to gain more knowledge about cybersecurity and disseminate skills to students was set in place. The Cyber Aware Teacher Continuing Professional Development (CPD) is run by Tech Partnership[3] and is a series of free online resources ranging from modules on password security to information about malware and other cybersecurity threats.

Some of the groundwork laid out in the earlier mentioned NCSS found implementation in 2017. It marked a time of heightened efforts to increase the diversity of the future talent pool and the stronger involvement of industry actors in the educational programs that were hitherto proposed.

A core piece in these efforts was the publication of a dedicated UK Digital Strategy, released in February 2017 (Department for Digital, 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, the UK Digital Strategy has been criticized by industry actors for not having provided enough detail to make its proposals credible (Reeve 2017). The Digital Skills Partnership marks a corner piece of the Strategy and pledges millions of free digital training opportunities, offered by large private sector organizations such as Google, Lloyds Banking Group and Barclays. It ties in with a £20 million initiative that aims to fund extracurricular school programs aimed at developing skills at the secondary school level.

Summary of the UK Government's Skills and Education Initiatives (2017)

Initiative/Policy/Publication	**Description**

[3] The Tech Partnership is a UK network of employers collaborating to create the skills for the digital economy.

CyberFirst Girls Competition	First dedicated competition to inspire and encourage young girls as part of the CyberFirst scheme in January
UK Digital Skills Strategy	Released in February, the strategy sets out how the UK will develop a world-leading digital economy
Cyber Security Apprenticeships for Critical Sectors	Scheme aims to develop and recruit security professionals which will be employed in energy, water and transport companies
Digital Skills and Inclusion Policy	Released in April, the policy provides an overview of government digital skills and inclusion work
Academic Centres of Excellence in Cyber Security Research	Two further UK universities recognised as ACE-CSRs (Edinburg and Warwick)
Extra Curricular Cyber Schools Programme	Government committed £20m to fund an extracurricular school programme aimed at developing the cyber skills of secondary school students which is to begin in September
Digital Skills Partnership (DSP)	DSP brings together partners from public, private and charity sectors to offer free skill trainings

The 2016 NCSS further emphasized an objective to sustain “the best possible home-grown cyber security talent” (Cabinet Office 2016a, 55). It outlines five points upon which the government will measure the success of its ambition, including (a) effective and clear entry routes into the cybersecurity profession which are attractive to a diverse range of people; that cybersecurity (b) has become an integral part of relevant courses from primary to postgraduate level; (c) is an acknowledged profession and achieved Royal Chartered Status; (d) is integral part of continual professional development even for non-cybersecurity professionals; and (e) that both the government and the Armed Forces have access to cyber specialists. It remains to be seen if these objectives will be achieved within the remaining three years of the Strategy.

4. State Society Dynamics

As this analysis demonstrates, the cyber security industry in the UK has been in fairly close engagement with the government. A collegial relationship marks their cooperation, considering that both the public and the private sector equally share the recruitment problems in this space and equally profit from these investments. The Digital Skills Partnership is one of the most recent outcomes of this intensified liaison. It aims to link the government with business, charities and voluntary organizations and resulted in a range of training courses offered from private sector organizations. While these activities raise the responsibility for industry stakeholders to a new level, many of the earlier outlined programs were already developed in close exchange with business representatives and carried the handwriting of both public and private players.

In terms of regulatory shifts, many companies have expressed concern at the cost and complexity of GDPR compliance but 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 resulted in increased awareness among the general public. It is too early to gauge the impact of these recently introduced initiatives but it is reasonable to conclude that the introduction of them in itself registers a shift in the dynamics between state, society and the private sector. They certainly reflect a growing recognition that the private sector has not been stimulated by market drivers to implement the levels or type of cyber security expected by other actors.

In terms of skills development, past efforts may have yielded fruit. The most recent A level (final high school examination) results lists maths as the most popular A level with maths and further maths having nearly 25% more entries than in 2010 (SC Media UK 2017). Whether the rising numbers of students interested in this subject are due to the greater awareness of career opportunities associated with cyber security 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 emphasis on education as a form of industrial policy and the breadth of measures taken by the government to close the skills gap can also be a helpful tool for fostering multilateral cooperation in this space. The first NCSP invested over the course of its period £8.1 million in international engagement and capacity building (Cabinet Office 2016b). These initiatives were primarily focused on strengthening trans-border cooperation to reduce cybercrime and the UK's participation in multi-national exercises to strengthened skills and operational links with other nations. Some specific initiatives that underpinned these international engagements included the UK's participation (along with all Security Council members and a rotating list of additional states) in the UN Group of Governmental Experts process, which was active in developing recommendations for responsible state behaviour online. The UK took a lead in initiating the Global Conference on Cyber Space – otherwise known as the London Process, that began in London in 2011 (Cabinet Office 2016b). Specifically, the Global Forum on Cyber Expertise (GFCE) is thereby noteworthy. It is an international platform to coordinate and share best practice in cybersecurity capacity building, which can feed back to strengthening best practices and cybersecurity expertise nationally. Through these and certainly many other international activities, the UK has built a consensus among like-minded states on a range of cybersecurity issues and cybersecurity capacity building in particular (Cabinet Office 2016b).

In spite of these successes, some essential issues remain unaddressed and stand in the way to further expand and diversify the UK's talent pool of the future. Firstly, many of the above outlined measures are predominantly citizen-centric, with programs being restricted to UK nationals. In 2016, around 1 in 7 (14%) of the 64,727 million residents in the UK were born abroad and 1 in 11 (9%) held a non-British nationality (Office for National Statistics 2017). While many of these non-British nationals account for European Union (EU) citizens who, at the moment, can participate in these schemes, the emerging exit of the UK from the EU (i.e., Brexit) may create unexpected challenges, both when it comes to non-citizens ability to participate in such initiatives as well as their chance to engage in the cybersecurity labour market that desperately requires suitable employees. Although such restrictions may seem reasonable in light of the fear of a potential "brain drain" when investing in foreign nationals who potentially return to their home countries (Pierre Audoin Consultants, 2013), tackling global problems can only profit from a global workforce. Brexit, thus, has the potential to decrease attraction of an international talent pool and may negatively affect UK's relationship with Europe. The restrictive inward-looking worldview the UK is currently pursuing may therefore be one emerging market failure that the UK's industrial policy will be facing in the near future.

A second point of concern is the England-centric approach that the UK government is pursuing. Earlier mentioned curriculum changes apply solely to the English schooling system, as Wales, Scotland and Northern Ireland have sovereign power over educational decisions (Crick and Moller 2015; Morris 2012). Thus, statements such as that "cyber security is now included at every level of the UK's education system" (Cabinet Office 2016b, 26) effectively translate into 'at every level of the English education system'. As a result, skewed attention may be paid to the needs and demands of the rest of the UK's education system with the potential of unequal skill developments across the nation.

5. Conclusion

The UK case provides some interesting contrasts from the past to the present (and likely future). The key shifts in industrial policy for cyber security have emerged through the sentiment that the market has not delivered adequately – either in scale or in scope. This has been explicitly expressed in the 2016 National Cyber Security Strategy which highlights the nature of market failures that have characterized the sector in the UK. These are characterized by three key issues: continued breaches, the skills gap and the failure of UK PLC to invest.

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 General Data Protection Regulation, the ePrivacy Act and the Network and Information Systems Directive all take a more assertive approach to directing the private sector to deliver data security and network security that is more aligned to expectations of society. They are also more aligned with the government's expectations of the potential for the digital economy to deliver benefits to the UK.

Essentially, designing and implementing an industrial strategy for cyber security 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 of an increasingly globalized market, an international and interdependent data/network ecosystem, and the expectations of society as we move closer and further into the fourth industrial revolution.

References:

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," BASC Working Paper Series, 2018-01.

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: The U.S. Case," BASC Working Paper Series, 2018-02.

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

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

Cabinet Office, 2014. The UK Cyber Security Strategy Report on Progress and Forward Plans – December 2014. HM Government, London.

Cabinet Office, 2013. Progress against the Objectives of the National Cyber Security Strategy – December 2013. HM Government, London.

Cabinet Office, 2012. Progress against the Objectives of the National Cyber Security Strategy - 2012. HM Government, London.

Cabinet Office, 2011. The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. HM Government, London.

Carr, Madeline. 2016. 'Public Private Partnerships in National Cyber Security Strategies', *International Affairs.* 92: 1, pp.43-62.

Carr, Madeline, Sneha Dawda, Alex Chung, Atif Hussain and Siraj Shaikh. 2018. 'Mapping the UK Cyber Security Policy Landscape'. *Digital Policy Lab Paper Series.* UCL STEaPP.

Carr, Madeline and ??. 2018. 'Cyber Security Metrics: The view from both sides of the board table'. *Digital Policy Lab Paper Series*, UCL STEaPP.

Center for Cyber Safety and Education, (ISC)2, 2017. Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher [WWW Document]. Cision. URL http://www.prnewswire.com/news-releases/global-cybersecurity-workforce-shortage-to-reach-18-million-as-threats-loom-larger-and-stakes-rise-higher-300469866.html (accessed 9.2.17).

Center for Cyber Safety and Education, (ISC)2, 2017. The 2017 Global Information Security Workforce Study: Women in Cybersecurity. Center for Cyber Safety and Education, Clearwater, FL.

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

Crick, T., Moller, F., 2015. Technocamps: Advancing Computer Science Education in Wales, in: Proceedings of the Workshop in Primary and Secondary Computing Education, WiPSCE '15. ACM, London, UK, pp. 121–126. doi:10.1145/2818314.2818341

Culbertson, D., Humphries, D., Ivy, G.M., Kolko, J., Rodden, V., 2017. Indeed Spotlight: The Global Cybersecurity Skills Gap [WWW Document]. Indeed Blog. URL http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/ (accessed 9.2.17).

Cyber Security Challenge UK, 2017. Could You Hack into a Car? If so, a Cyber Security Career Awaits! [WWW Document]. Cyber Secur. Chall. UK. URL https://www.cybersecuritychallenge.org.uk/news-events/hack-car-cyber-security-career-awaits (accessed 9.3.17).

Department for Business, Energy & Industrial Strategy, 2015. Cyber security: guide to programmes and resources for schools and further education. HM Government, London.

Department for Business, Energy & Industrial Strategy, 2017. *Industrial Strategy: Building a Britain fit for the future*. HM Government, London.

Department for Business, Innovation & Skills, Cabinet Office, Government Communications Headquarters, 2014a. Cyber Security Skills: Business perspectives and Government's next steps. HM Government, London.

Department for Business, Innovation & Skills, Cabinet Office, Government Communications Headquarters, 2014b. Cyber Security skills: Business perspectives and Government's next steps. Supporting Evidence. HM Government, London.

Department for Business, Innovation & Skills, Department for Digital, Culture, Media & Sport, 2016. Digital Skills for the UK Economy. HM Government, London.

Department for Business, Innovation and Skills, Cabinet Office, Government Communications Headquarters, 2014. Cyber Security Skills: a guide for business. Getting involved with skills and research initiatives. HM Government, London.

Department for Business, Innovation and Skills, Government Communications Headquarters, Engineering and Physical Sciences Research Council, Cabinet Office, 2013. Working with academia to increase the UK's capability in cyber security. HM Government, London.

Department for Culture, Media and Sport, 2017. UK Digital Strategy 2017. Department for Culture, Media and Sport, London.

Department for Digital, Culture, Media & Sport, 2015. Code clubs for children in Croydon, Ealing, Harrow, and Hounslow - Case study [WWW Document]. GOV.UK. URL https://www.gov.uk/government/case-studies/code-clubs-for-children-in-croydon-ealing-harrow-and-hounslow (accessed 9.5.17).

Department for Digital, Culture Media & Sport, 2017. A New Data Protection Bill: Our Planned Reforms. Department for Digital, Culture Media & Sport, London.

Department for Digital, Culture Media & Sport, 2018. Cyber Security Breaches Survey 2018. Department for Digital, Culture Media & Sport, London.

Department for Education, 2017. "Harmful" ICT curriculum set to be dropped to make way for rigorous computer science [WWW Document]. GOV.UK. URL https://www.gov.uk/government/news/harmful-ict-curriculum-set-to-be-dropped-to-make-way-for-rigorous-computer-science (accessed 9.5.17).

Department for International Trade, 2018. Cyber Security Export Strategy. Department for International Trade, London.

European Commission. 2017. 'Executive Summary of the Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC'. Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0005&from=EN

European Union Agency for Network and Information Security, 2012. National Cyber Security Strategies. European Network Information Security Agency, Heraklion, Greece.

HM Government, 2015. National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom (No. Cm 9161). HM Government, London.

HM Government, 2017. Building Our Industrial Strategy: Green Paper. HM Government, London, UK.

HM Government, 2018. Digital Charter. HM Government, London.

HRH Queen Elizabeth. 2017. 'Queen's Speech 2017: what it means for you'. 21 June 2017. https://www.gov.uk/government/publications/queens-speech-2017-what-it-means-for-you/queens-speech-2017-what-it-means-for-you .

The Information Commissioner's Office. September 2017. 'Response to Consultation on updating Ofcom's guidance on security requirements in sections 105A to D of the Communications Act 2003'. Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0028/106957/ICO.pdf

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.

Morse, A., 2013. The UK cyber security strategy: Landscape review (No. HC 890). National Audit Office, London.

National Crime Agency and National Cyber Security Centre. 2018. ‘The Cyber Threat to UK Business: 2017 – 2018 Report’. London.

National Cyber Security Centre, 2017. Academic Centres of Excellence in Cyber Security Research [WWW Document]. NCSC. URL https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research (accessed 9.5.17).

National Cyber Security Centre. 2018a. ‘General Data Protection Regulation’ May 18, 2018. https://www.ncsc.gov.uk/GDPR.

National Cyber Security Centre. 2018b. ‘Introduction to the NIS Directive’, 30 April, 2018. https://www.ncsc.gov.uk/guidance/introduction-nis-directive .

Office for National Statistics, 2017. Annual Population Survey (APS): Population of the UK by country of birth and nationality: 2016. Office for National Statistics, London.

Pierre Audoin Consultants, 2013. Competitive analysis of the UK cyber security sector. Department for Business, Innovation and Skills, London.

Priday, Richard, 2018. ‘The Ticketmaster hack is a perfect storm of bad IT and bad comms’. *Wired.* June 28, 2018. http://www.wired.co.uk/article/ticketmaster-data-breach-monzo-inbenta

Reeve, T., 2017. UK post-Brexit Digital Strategy criticised by cyber-security industry [WWW Document]. SC Media UK. URL https://www.scmagazineuk.com/news/uk-post-brexit-digital-strategy-criticised-by-cyber-security-industry/article/641036/ (accessed 9.6.17).

Research Institute for Science of Cyber Security (RISCS), 2018. ‘Analysis of Cyber Metrics Workshop’. London, May 23, 2018.

SC Media UK, 2017. Students offer hope for narrowing of skills gap in cyber-security [WWW Document]. SC Media UK. URL https://www.scmagazineuk.com/news/students-offer-hope-for-narrowing-of-skills-gap-in-cyber-security/article/682418/ (accessed 9.9.17).

Science and Technology Committee, 2016. Digital skills crisis: Second Report of Session 2016–17 (No. HC 270). House of Commons, London.

Tanczer, Leonie and Madeline Carr. 2018 (forthcoming). ‘Survey of Cyber Security Skills and Education Initiatives in the UK’. *Digital Policy Lab Paper Series.* UCL STEaPP.

The Institution of Engineering and Technology, 2013. “Industry first” seeks to address cyber security skills gap [WWW Document]. URL http://www.theiet.org/policy/media/press-releases/20130607.cfm (accessed 9.5.17).

University College London, 2012. UK’s first Cyber Security Institute to be based at UCL [WWW Document]. UCL News. URL http://www.ucl.ac.uk/news/news-articles/1209/130912-UK-first-cyber-security-institute (accessed 9.5.17).

Walker, W.E., Rahman, S.A., Cave, J., 2001. Adaptive policies, policy analysis, and policy-making. Eur. J. Oper. Res., Complex Societal Problems 128, 282–289. doi:10.1016/S0377-2217(00)00071-0

Weimer, D., Vining, A., 2014. Policy analysis: concepts and practice / David Weimer, Aidan R. Vining., 5th edition. ed. Pearson Education Limited, Harlow, Essex, England.