Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Organising a Government for Cyber

The Creation of the UK's National Cyber Security Centre

Robert Hannigan

Organising a Government for Cyber

The Creation of the UK's National Cyber Security Centre

Robert Hannigan

RUSI Occasional Paper, February 2019

Royal United Services Institute
for Defence and Security Studies

188 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, February 2019. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

Printed in the UK by Rapidity.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

Insofar as the UK is seen to have made progress on cyber security over the past 15 years, that is a tribute to the many individuals and institutions in the UK government, the private sector and international partners who have made it possible. I am particularly grateful to former colleagues at GCHQ, the National Cyber Security Centre and the National Security Agency in the US for their contributions and I have drawn heavily on their published documents, although the opinions here are obviously my own.

Foreword

NO ONE COULD be better placed than Robert Hannigan to write an account of the creation of our National Cyber Security Centre (NCSC) and to define the future challenges in this field for states based on democracy and the rule of law. In my time as foreign secretary, I knew Robert as a wise adviser on many security issues, and he went on to lead GCHQ and to oversee the establishment of the NCSC. He has been an outstanding public servant. Now, as Chairman of RUSI, I am pleased that we can publish this paper to increase understanding at home and abroad of the UK's approach to a subject that will grow further in importance, difficulty and public interest.

An effective national strategy on cyber security requires serious resources, which the British government recognised in the 2010 Strategic Defence and Security Review. Yet it also needs other attributes without which resources will be wasted – leadership, coordination, accumulated expertise, integration with intelligence work and strong support at the top of government. The most crucial decision in creating a strong cyber security centre was to place responsibility for it with the appropriate intelligence agency, GCHQ, but simultaneously to make part of its work open and accessible to the population we need to protect. This is an innovative way to develop intelligence work in an age of cyber, which other nations might well wish to follow.

Such a centre can still only work well if it is part of the creation of a strong culture of giving time and priority to cyber security across the public and private sectors. For example, Robert points rightly to the importance of working intimately with the National Crime Agency. Cyber cannot be placed in a separate box and neglected by cabinets of ministers or boards of directors, or they will discover a major attack is underway or defences are inadequate only when it is too late.

Robert also describes how, in recent years, responsibility for cyber has been given to a senior minister, with a strong personal commitment to the issue and proximity to the prime minister of the day. This is utterly indispensable. For as far as we can see into the future, ministerial responsibility for cyber must never be downgraded. Complacency at the top in the cyber world would be disastrous.

However we have organised and resourced ourselves, there will be major tests and challenges to come. This paper draws attention to them: how to regulate the design of products; how to integrate cyber security with military structures; and how to ensure a supply of home-grown skills. The recommendation to learn from Israel and intervene if necessary in the education system should be studied carefully by ministers.

More intractable are the other principal challenges described: how to ensure the integrity of supply chains and how to deter offensive cyber behaviour by other nation states. Both these issues are of immediate concern, and for good reason. Our open society and economy is

fundamental to freedom and prosperity, but it leaves us vulnerable to exploitation and attack. We will need to show that a country dedicated to fairness, legal authority and proportionate actions can nevertheless protect itself and make a robust response when necessary. In the longer term, we must maintain the effort to agree international 'rules of the road' in cyber space that we initiated in 2011.

This is a necessary, thoughtful and authoritative paper. I know that policymakers in the UK and many other nations will benefit from studying it.

Rt Hon William Hague
Chairman of RUSI
February 2019

Preface

THE UK'S NATIONAL Cyber Security Centre (NCSC) was officially opened by Her Majesty the Queen in February 2017. It was the first national cyber centre to bring together government, intelligence agencies and the private sector in one organisation, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. In doing so, the NCSC has improved understanding of, and the response to, the most important cyber threats to the UK.

Robert Hannigan was director GCHQ when the NCSC was created, and was closely involved before that in cyber and information security issues at a senior level in roles in the Foreign Office and Cabinet Office. In this Occasional Paper he provides a unique first-hand account of the development of the UK government's approach to cyber security, and the creation of the NCSC. In that sense, this is not a traditional research paper, but a personal perspective from someone who has been closely involved in these issues, aimed at informing policymakers, practitioners and researchers.

In the second half of the paper, the author offers thoughts on future cyber-related challenges. While governments, the private sector and researchers continue to develop different approaches to cyber security, the threat, policy and technology landscapes evolve at pace. This account of the creation of the NCSC, and the wider UK national strategy, offers perspectives relevant both to the further development of the UK's own cyber strategy and to those seeking to tackle the same challenges elsewhere.

Professor Malcolm Chalmers
Deputy Director-General
February 2019

Introduction

SINCE LEAVING GOVERNMENT service, almost wherever I have gone in a private sector cyber security capacity, I have been questioned about the creation of the UK's National Cyber Security Centre (NCSC). This is less surprising in the case of other governments, which naturally look for useful comparators, but more so in the case of large companies overseas. Their interest has tended to focus on how the private sector can interact with government and how to achieve coherence.

Since I have been involved in the UK's cyber journey throughout, I welcomed the invitation from RUSI to record my account of how the UK's approach to cyber security developed and how we came to create the NCSC.

Rather than write a detailed history, I have tried to draw out the thinking, principles and key policy, operational and political issues which might be applicable or useful elsewhere. I have resisted the temptation to set out 'five things for governments to think through', although it will be obvious that I regard some principles as foundational: identifying and capitalising on scarce technical skills; access to data and advanced analytics; harnessing the talent and resources of the private sector; and achieving wider behavioural change.

Cyber security is a global challenge which crosses borders and confounds many of the traditional legal frameworks because the internet sits across jurisdictions and is not in any case owned by governments. Anything which helps to raise the baseline of security of this global infrastructure helps us all. One of the great challenges of the next phase in the development of the internet is to persuade those countries which have behaved badly or recklessly in cyberspace, or have allowed cyber criminality to flourish, that they stand to gain more from a stable, secure and resilient internet. The other challenge for governments and the private sector together is to build in security by design and by default at every level and avoid repeating the mistakes of the past.

I do not suggest that the UK model is the right answer for all countries or that it is perfect even for the UK; all involved would agree that it has much further to go and, of course, the threat is constantly changing. Looking at the NCSC from the private sector, as I do now, I realise there is much more for government to do to fulfil its part of the government–industry partnership approach to cyber security.

I. Background to the National Cyber Security Centre

THE CYBER SECURITY challenge for any government in the first decade of this century was the gap between an escalating cyber threat and a nation's institutional readiness to meet it.

In facing a rising volume and sophistication of cyber attacks, both criminal and state-sponsored, there were two fundamental policy problems. In a cyber domain which cut across all sectors and increasingly underpinned the entire economy, it was difficult to define what the proper role of government should be, given that in reality the 'attack surface' was largely outside government networks. Even if this could be determined, deciding where responsibility lay for such an all-encompassing domain as 'cyber' was difficult. Nonetheless, the UK public had an expectation that the government would offer protection in cyberspace as it did in the physical world.

Operationally, government had its hands full securing its own networks, and protecting the wider economy and citizens seemed an impossible task. Underlying both was a chronic shortage of necessary skills and basic understanding.

The first attempt to scope the problem was commissioned by then Prime Minister Gordon Brown in 2007. As a former finance minister he instinctively grasped the UK's critical dependence on cyberspace, and as a driver of the early adoption of government digital services to citizens he saw a particular vulnerability. The UK's first Cyber Security Strategy, which Brown commissioned, was more of a scoping document than a useable strategy,[1] but it concluded that coherence and central control were necessary and identified a critical shortage of skills (see Appendix I). These were to be persistent themes, which we tried to address through the later creation of the NCSC.

As part of this strategy, the government established an Office for Cyber Security (OCS) in the Cabinet Office, to develop policy; and a Cyber Security Operations Centre (CSOC), 'to monitor developments in cyber space (ultimately providing collective situational awareness), analyse trends, and to improve technical response co-ordination to cyber incidents'.[2] The CSOC aimed to help 'ensure coherent dissemination of information across government, industry, international partners, and the public'.[3]

1. Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, Cm 7642 (London: The Stationery Office, 2009).
2. *Ibid.,* p. 17.
3. *Ibid.,* p. 17.

The OCS, renamed OCSIA (Office for Cyber Security and Information Assurance) in 2010,[4] was staffed by a small group of specialists and generalists, mostly on loan from government departments and agencies. The CSOC was to be located at GCHQ in Cheltenham, drawing on the expertise of GCHQ's longstanding information assurance arm, the Communication–Electronics Security Group (CESG).[5] Iain Lobban, then director GCHQ, had already begun to reshape the organisation for the cyber era.

This tentative first step towards coherence illustrated a number of key problems common to most governments. There were numerous players in the cyber domain: some 15 government departments, agencies and law enforcement bodies saw themselves as having a key role, and many others were attached to these. They covered a vast range of areas, illustrating the pervasive nature of cyberspace: domestic security; business and economic policy; education; foreign affairs; the law; intelligence and security; public safety; and law enforcement.

Together they had a role in giving public or private advice on cyber security to government, business and individual citizens. But very few of these individuals had any deep technical skills on which to base this advice. More alarmingly, in operational terms, as we began to see larger-scale cyber incidents emerge, it was unclear which body would handle any given incident.

Only two parts of government recruited and retained experts on 'cyber', broadly defined. The Centre for the Protection of National Infrastructure (CPNI), a part of MI5, was responsible for protective advice to key sectors, focusing mostly on physical terrorism. Until the creation of the NCSC it had a small expert group doing the same work on cyber security.

But the main centre for skills was the CESG. Throughout its history, GCHQ had attracted and developed world-class expertise in information assurance and security, notably in cryptography, from 1919 through Bletchley Park to the creation of public key cryptography by James Ellis and colleagues in the 1960s.[6]

But there were problems. First, while GCHQ/CESG was responsible for the protection of non-military UK government networks,[7] it had relatively limited powers. As the National Technical Authority for Information Assurance, providing advice on cryptographic standards and other measures to protect state information, the CESG acted as a kind of consultant, with varying levels of impact. The creation of the Government Secure Intranet (GSI) in 1997 was, for its time, a major step forward, but the CESG retained a mixed reputation with government customers. Internally, the information assurance role of GCHQ was often regarded as secondary

4. Now subsumed into the Cyber and Government Security Directorate of the Cabinet Office.
5. For details of the history of the CESG and the heritage of the National Cyber Security Centre (NCSC), see NCSC, 'Our History', 8 June 2017, <https://www.ncsc.gov.uk/information/our-history>, accessed 21 January 2018.
6. The GCHQ website is a good source for the history, with contributions by Tony Comer, GCHQ's historian: GCHQ, 'Welcome to GCHQ', <https://www.gchq.gov.uk/>, accessed 21 January 2019.
7. The CESG also advised the military and was responsible for key military cryptographic standards.

and unglamorous in comparison to signals intelligence gathering: the dry self-discipline required to manage good information security was less appealing than getting information on key targets of national interest. Outside a core group of dedicated experts, many GCHQ staff regarded a posting to the CESG as a step backwards or downwards. My predecessors as directors of GCHQ, David Pepper (2003–08) and Iain Lobban (2008–14), did a great deal to turn this round and rebalance GCHQ between intelligence and cyber security.[8] But the CESG was not at that stage ready to take a national, public leadership role.

8. Andrew France led the operational delivery of GCHQ's cyber defence.

II. The Coalition Government, 2010–15

FROM ITS ELECTION in 2010, the new UK coalition government gave cyber security a high priority. Political governance was an immediate issue, as it was clear that a minister with cross-cutting authority would need to convene the government's efforts. There was an internal debate, which still surfaces from time to time, about whether a cyber minister would be useful. The UK's experience of trying to solve a cross-cutting problem by giving a minister the titular responsibility has not been positive: they tend to be junior ministers rooted in a particular department, without leverage over their own departments, let alone the wider government system.

But it is nonetheless necessary to have a minister who can report to Parliament on general cyber issues and on the performance of government bodies such as the NCSC. This function has tended to fall to Cabinet Office ministers; at the time of writing it is the responsibility of the chancellor of the Duchy of Lancaster, currently David Lidington. He has lead responsibility for the National Cyber Security Strategy and the NCSC, although the CEO of the NCSC reports to the director GCHQ, who in turn reports to the foreign secretary. This illustrates the complexity of apportioning responsibility for cyber: in practice a workable solution needs to be found which respects the cross-cutting nature of cyber and finds a suitable way of convening and corralling the necessary departments and achieving an acceptable level of accountability to Parliament. This is still a work in progress, not least because the 'secret' part of the NCSC's work inevitably must be handled through arrangements established for the oversight of the intelligence community, in particular the Intelligence and Security Committee (ISC).[9] This will almost certainly need to be revisited as the NCSC's role develops further.

Prime Minister David Cameron solved this problem by appointing then Foreign Secretary William Hague to chair a Cabinet committee on cyber. Hague had the necessary seniority among his peers and closeness to Cameron and Chancellor George Osborne to make this work. The appointment was personal to Hague and after his retirement transferred to Osborne, for the same reasons. It helped that Hague was personally passionate about the opportunities and threats of cyber and had a high level of ambition on the subject. He wrote an early letter to the prime minister and the Cabinet setting the UK's objective of becoming 'the safest place to live and do business online',[10] which has become the government's and the NCSC's practical ambition. We debated the drafting of this objective at length. It is, of course, a relative ambition

9. Intelligence and Security Committee of Parliament, 'About the Committee', <http://isc.independent.gov.uk/>, accessed 21 January 2019.
10. The letter was unpublished, but the phrase has become a strapline for the NCSC. See NCSC, <https://www.ncsc.gov.uk/>, accessed 21 January 2019.

and does not imply that the UK can be 100% safe. It was based on the key assessment that the UK could harden its defences to the point that cybercrime would be displaced elsewhere to easier targets. While this may sound cynical, it assumed that an international raising of the baseline would make all economies harder targets and encourage others to up their game. The long-term bet was that good resilience and security would become a market differentiator for UK business and attractive for inward investors. The challenge of collecting meaningful metrics on cyber means this hypothesis will remain untested for some time, but it was not an unreasonable starting assumption.

As foreign secretary, Hague also felt strongly that we should begin to promote an international arms control approach to cyberspace. As a step towards this, he published some suggested norms of behaviour,[11] and convened the first international governmental conference on cyberspace, with industry and civil society participation, in London in November 2011.[12]

More importantly, the coalition government launched a £650-million National Cyber Security Programme (NCSP) as part of its incoming 2010 Strategic Defence and Security Review.[13] Given the extreme constraints on public spending at that time, this figure, added to the funding already given to GCHQ through the Single Intelligence Account (the funding vehicle for MI6, GCHQ and MI5), sent a powerful signal about the importance of cyber security. The NCSP was overseen by OCSIA in the Cabinet Office and at a higher level by Hague's Cabinet committee. Details of how this money was to be spent were given in a new Cyber Security Strategy in 2011.[14] Its subtitle – 'Protecting and Promoting the UK in a Digital World' – pointed to its focus. The strategy rested on a collaborative approach, both between parts of government and with industry and international partners. But it also began to suggest practical ways to tackle cybercrime and make the UK more resilient at a national level; the bulk of the spending, nearly 60%, went to GCHQ for those purposes. It led to some early experiments with UK telecommunications companies in active defence (see Appendix II).

In the next few years, GCHQ not only increased its focus on cyber but began to take a more active role in issuing public advice. Then Director Iain Lobban launched a successful '10 Steps to Cyber Security' in 2012.[15] Produced jointly with the Department for Business, the Cabinet Office and the CPNI, it was a practical guide for businesses at board level. The key insight and approach

11. UK Government, 'Foreign Secretary Opens the London Conference on Cyberspace', 1 November 2011, <www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace>, accessed 21 January 2019. Tim Dowse, a Foreign and Commonwealth Office expert with a deep knowledge of deterrent policy, played a key role in drafting these norms.
12. *Ibid.*
13. HM Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (SDSR), Cm 7948 (London: The Stationery Office, October 2010).
14. Cabinet Office, 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World', November 2011.
15. NCSC, '10 Steps to Cyber Security', <www.ncsc.gov.uk/guidance/10-steps-cyber-security>, accessed 21 January 2019. The '10 Steps' are: risk-management regime; secure configuration; network

was that businesses needed help in seeing cyber as a manageable risk, parallel to many other risks. It emphasised cultural and behavioural change as strongly as technical fixes, which is commonplace now, but was rare at the time, when cyber security was still seen as 'a problem for the IT department'. The '10 Steps' has gone through many versions and has been underpinned by technical materials and guides, but remains a key high-level measure for risk management. The public event for FTSE 100 CEOs addressed by Lobban and Jonathan Evans, then Director General of MI5 and responsible for CPNI, made a significant impact in boardrooms, long before global incidents had grabbed their attention.

Figure 1: The NCSC's 10 Steps to Cyber Security

Source: National Cyber Security Centre, <www.ncsc.gov.uk>.

security; user privileges; user education/awareness; incident management; malware prevention; monitoring; removable media controls; and home and mobile working.

The government also established a Centre for Cyber Assessment (CCA) in 2013, announcing its existence in 2015.[16] The CCA was based in GCHQ, answerable to the director, with staff from various sources across government, copying the model of the successful Joint Terrorism Analysis Centre, based in MI5.[17] It was intended 'to provide independent all-source cyber assessments for government departments to inform operational and policy response'[18] and, in short, to tackle a perennial problem of how to quantify the cyber threat.

Cyber assessment is particularly difficult not just because it is a relatively new field but because it requires in-depth technical understanding alongside assessment of other sources. We found that ministers who had a framework for judging the seriousness of a terrorist threat or incident had no framework against which to measure cyber threats. The figures were always large, because all figures on the internet are, and no one knows what 100% is: internet data is hard to measure and not static. Traditional assessment bodies, notably the venerable UK Joint Intelligence Committee, simply did not have access to the right technical skills to make useful assessments or even to second-guess those made by others.

Two further significant initiatives were launched in this busy period as part of the implementation of the Cyber Security Strategy and the NCSP. In 2013 the government set up the Cyber Security Information Sharing Partnership (CiSP) as 'a joint industry and government initiative to exchange cyber threat information in real time, … increasing situational awareness and reducing the impact on UK business'.[19] The CiSP came to be hosted by Surevine, a private company supplying a secure platform for the exchange of information. It would also feed into a 'fusion cell' involving GCHQ, MI5 and the National Crime Agency (NCA). The CiSP has grown exponentially and spawned several sectoral versions, notably around financial services.

In 2014 the UK, rather belatedly in the view of some international partners, launched a national Computer Emergency Response Team (CERT)[20] to be the focal point for incident response, led by Chris Gibson, who came into government from the financial services sector. CERT-UK took

16. GCHQ, 'Foreign Secretary Highlights the Work of the Centre for Cyber Assessment', news article, 29 June 2015, <www.gchq.gov.uk/news-article/foreign-secretary-highlights-work-centre-cyber-assessment>, accessed 21 January 2019.
17. MI5, 'Joint Terrorism Analysis Centre', <www.mi5.gov.uk/joint-terrorism-analysis-centre>, accessed 21 January 2019.
18. GCHQ, 'Foreign Secretary Highlights the Work of the Centre for Cyber Assessment'.
19. NCSC, 'Cyber Security Information Sharing Partnership (CiSP)', 27 September 2016, <https://www.ncsc.gov.uk/cisp>, accessed 21 January 2019; UK Government, 'Government Launches Information Sharing Partnership on Cyber Security', press release, 27 March 2013, <www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security>, accessed 21 January 2019.
20. First launched in the US in the late 1980s, a Computer Emergency Response Team (CERT) became a badge of seriousness for national governments, but the UK always took the view that a CERT would not necessarily improve the UK's defences unless it was properly integrated into a more mature national approach.

responsibility for the CiSP as well as liaising with counterparts, principally GovCertUK, and the many overseas CERTs.

III. The Creation of the NCSC

THE ELECTION OF a new government in 2015 led to a new Comprehensive Spending Review,[21] and further discussions about how to take forward cyber security. The ministerial cyber committee was now chaired by Chancellor George Osborne, and OCSIA in the Cabinet Office was led by Matthew Gould, a former diplomat and UK ambassador to Israel, where he had become inspired by that country's deeply impressive approach to cyber skills and industry.

A number of events helped accelerate the trajectory towards creating the NCSC. First, ministers instinctively felt that there were far too many parts of government jostling for space in cyber, as a quick look around the meeting table confirmed. The most vocal critic of this was Mark Carney, the new governor of the Bank of England. In his first full year in the job, he had made it clear that cyber security and resilience for financial services was a priority and would be a key part of the bank's regulatory role. He came to GCHQ's London office and told me that there were too many sources of advice from government and too much confusion for industry, which was keen to engage with government. More importantly, he told George Osborne, who was already keen to rationalise.

More importantly at the strategic level, every survey of cyber readiness tended to tell us the same thing. Our approach, encouraging the private sector and individuals to get better, had achieved a significant improvement but had hit a plateau. There was a limit to how far businesses would or could progress and a security model that presupposed everyone would do the right thing was bound to fail. It pointed to a shift in the government's position towards greater intervention, taking some of the burden off individuals and companies. Government needed to get a better balance between what could be done at a national level with major parts of industry, and what needed to be done outside government.

Any new technology tends not to be developed with safety or security at the front of mind. A combination of government regulation, insurance and self-regulation through market forces tends to put this right over time, the automotive industry in the 20th Century being the obvious example. In cyber security, too much of the burden fell on consumers, whether companies or individuals.

The Scope and Role of a National Cyber Centre

During discussions at the Osborne-chaired committee in 2014–15, we put forward the idea of a national centre which would bring together in one place some key functions: major incident response and handling; threat information sharing; a single source of expert national advice and

21. HM Treasury, *Spending Review and Autumn Statement 2015*, Cm 9162 (London: The Stationery Office).

best practice; and practical measures to improve the resilience of the UK against cyber attacks. The latter was a key and, for reasons which will become clear, potentially politically sensitive part of the strategy, and became known as the Active Cyber Defence programme (see Appendix II). It was devised by Ian Levy, who was to become technical director of the NCSC. There was also lengthy discussion about other areas that might be in the scope of such a centre, notably the fostering of cyber skills, cyber industry and exports, and cyber policy.

Governance and Ownership

We toyed with the idea of co-locating all the relevant bodies under a coordinating mechanism, as governments such as Australia did at that time. Many departments favoured this, not least because it would leave them in clear control of their areas. While this might have improved coordination, it fell well short of the ambition ministers had expressed.

The final decision, to make the NCSC part of GCHQ, came about for several reasons. First, in the eyes of ministers, it was 'obvious'. In his speech announcing the creation of the NCSC, delivered at GCHQ in November 2015, Osborne talked about the history of GCHQ and put it bluntly: 'GCHQ is rightly known as equal to the best in the world. And I am clear that the answer to the question "who does cyber?" for the British government is – to very large degree – "GCHQ" … It is the point of deep expertise for the UK government. It has an unmatched understanding of the internet and of how to keep information safe'.[22] Cameron made a similar point to me: when a cyber incident happened there were lots of departments represented at the table, but most of the questions gravitated to GCHQ.

Expertise and skills made this obvious, along with the secret data and advanced analytical capabilities to which GCHQ had access. While for some years we had proceeded on the assumption that non-secret bodies, such as the CERTs, could deal with most incidents and GCHQ/CESG could be brought in for the most sophisticated nation state attacks, in reality it was GCHQ that was detecting and then defending against a rising tide of high-grade attacks. Moreover, it was increasingly clear to all of us that the scale of the challenge meant that we needed to blend the skills and data from the secret world with the skills, data and resources of the private sector.

Although obvious to ministers, making the NCSC part of GCHQ and under the ultimate control of the director was not obvious to all involved in government nor in GCHQ. There were reservations on all sides. Departments worried about the loss of their own control and accountability to a part of the secret world and its unusual culture. It was the decision of Andrew Parker, director general of MI5, to put his own CPNI cyber staff into the NCSC and under its control that made the difference in persuading others that the common good required some loss of institutional sovereignty. Complete ownership by GCHQ was also key to making the NCSC acceptable to

22. UK Government, 'Chancellor's Speech to GCHQ on Cyber Security', 17 November 2015, <www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security>, accessed 21 January 2019.

foreign intelligence allies, who could be reassured about the security of data exchange and who would not have been able to deal easily with a new civil service bureaucracy, however good or well intentioned.

There were also some political concerns, following the revelations by former US intelligence analyst Edward Snowden, that placing the NCSC inside and under GCHQ would be difficult for industry partners. But in fact, industry was universally in favour of a solution driven by deep expertise, and public opinion had always been supportive of GCHQ.

The greater challenge was probably within GCHQ. The realisation that cyber security cannot be done solely 'inside the wire' and at top-secret classification was not news to the dedicated core of CESG, but it was challenging to the rest of an organisation which was even less public than its sister agencies, MI5 and MI6. Making a much larger part of the organisation public-facing had severe practical implications for future careers. Both sides had strong incentives to pull away from each other and even CESG was uncertain that it wanted to step up and take on responsibility for cyber at a national level, a very different proposition from offering consultancy to government customers.

For all these reasons, it was decided during the course of 2015 that the NCSC and all its staff would be a full part of GCHQ, and it would subsume the CERT-UK team, the CCA, the CPNI cyber team and other functions. It was also agreed that the first CEO would be the existing director-general for cyber in GCHQ, Ciaran Martin. Martin was a career civil servant brought in to GCHQ to run the cyber security side and had made huge strides in reforming CESG and focusing it on consistent delivery to its government customers. He welcomed the chance to do this at a national scale and his background and style were reassuring to those on all sides. The CEO of the NCSC is therefore a member of the GCHQ Board and reports directly to the director GCHQ. The current complement of the NCSC stands at around 740 staff, although this is a complex picture and mirrors the opaqueness of the NCSP funding.[23]

The only exception to this clear line of command was law enforcement. We knew that, because of the independence of policing and prosecuting authorities in the UK, it would be impossible and inappropriate to put law enforcement within the NCSC as full members of staff under the direction of the CEO. But at the same time, since almost all cyber attacks are a crime of some sort, mounted increasingly by organised criminal groups, excluding law enforcement agencies made no sense. They rightly had the lead on cyber as crime and fraud. This could have been an area of great tension, but thanks to pragmatic leadership in the NCA, the Metropolitan Police

23. Ciaran Martin answered questions on funding and staffing in 2018, but an exact breakdown of funding remains opaque, partly because of the inclusion of capabilities funded by the Single Intelligence Account. See UK Parliament, Joint Committee on the National Security Strategy, 'Oral Evidence: Cyber Security, Critical National Infrastructure', 25 June 2018, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/oral/86108.html>, accessed 21 January 2019.

and other agencies, a workable and mutually reinforcing relationship has developed.[24] The NCA became closely linked with the NCSC and integrated into its work, without being part of its command structure. Given the shortage of cyber skills, including in law enforcement, this has been welcomed on all sides.

Focus and Responsibilities

Once a decision had been made on governance, there was inevitably much debate about what the NCSC should concentrate on in its early years. It brought with it responsibility for protecting government networks and for key parts of the Critical National Infrastructure and Defence, a challenge assigned to Jacqui Chard as deputy director. Deciding exactly what is critical is, of course, a difficult task in an increasingly complex economy, but it was important not to overload the centre.

While it should be the arbiter of coherent cyber security advice, from the highest level to consumer safety, the NCSC could not become a call centre for every complaint or fraud incident. Most would remain the responsibility of local law enforcement. Nor should it raise expectations that it would 'do' security for everyone – that would negate the progress made in getting companies and individuals to own the risk and take action.

Self-evidently the NCSC would lead the handling of major incidents above a certain threshold of national-scale significance. In practice, we underestimated the volume of these and the first director of incident response, John Noble, found himself handling around 600 in his first year. Although the NCSC has not yet had to face a Tier 1/C1 catastrophic incident,[25] the 2017 WannaCry ransomware attack came close in scale and was a useful test case.[26]

The NCSC also brought with it responsibility for assessment of the cyber threat at a national level (through what had been the CCA) and for information sharing (through the CiSP and CERT-UK). There were widely differing views about the importance of information sharing. Some

24. Keith Bristow and Lynne Owens, as successive directors-general of the National Crime Agency, and Bernard Hogan-Howe, as the Metropolitan Police Commissioner, were critical to making the complex law enforcement relationship work on cyber.
25. Tier 1 has now been reclassified as C1 under a more coherent Incident Classification System. C1 attacks are national emergencies, causing sustained disruption of essential services, leading to severe economic or social consequences, or to loss of life. C2 attacks can have a serious impact on a large portion of the population, economy or government. C3 attacks can have a serious impact on a large organisation or wider government. C4 attacks could threaten a medium-sized organisation. C5 attacks include threats to a small organisation. C6 attacks are those on individuals, for which the response would be led by law enforcement agencies, such as the local police force. For details, see 'New Categorisation System' in NCSC, 'Annual Review 2018', 2018.
26. The NCSC podcast on this incident is a useful snapshot. See NCSC, 'Podcast: Behind the Scenes of an Incident', 16 October 2018, <https://www.ncsc.gov.uk/incidents-podcast>, accessed 21 January 2019; see also NCSC, 'Annual Review 2018', pp. 22–25.

regarded this as pivotal, taking the view that if only all organisations pooled threats we would be halfway there. Our own experts were more equivocal: aggregating vast amounts of threat data from widely differing but often duplicative sources is a huge integration task and only helpful if clear, prioritised action can be taken on the back of it. Paul Chichester, now director of operations at the NCSC, had the international and industry credibility to make sense of this.

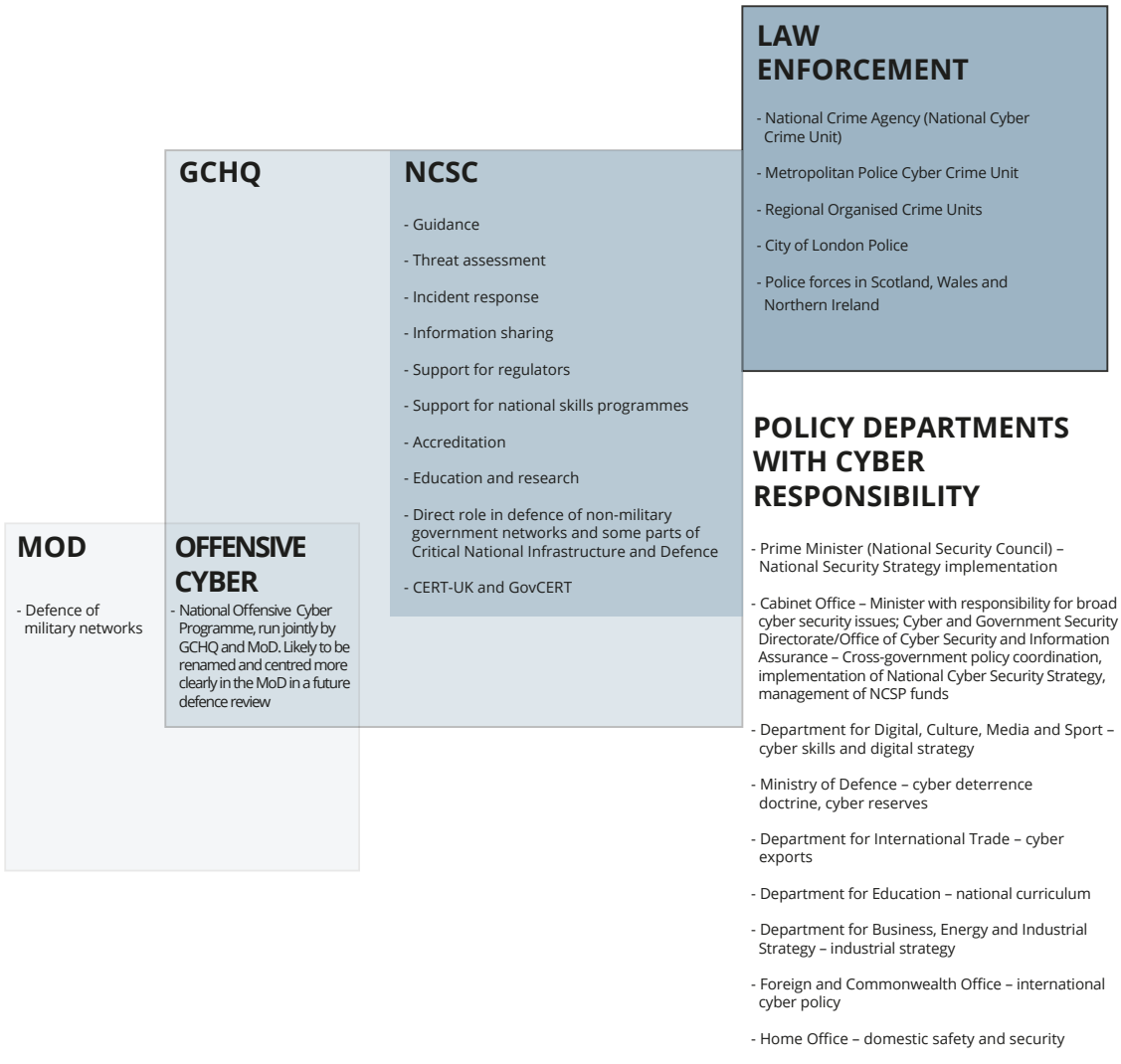
We resisted attempts to pile further responsibilities into the NCSC. Although cyber skills are critical, and the NCSC has a key role, the national policy leadership needed to lie with a mainstream department, and Matthew Gould built a dynamic and well-funded programme within the Department for Digital, Culture, Media and Sport.

We also resisted suggestions that the NCSC should become some sort of cyber regulator. Regulation is important, but best left to sectoral bodies with an understanding of the appropriate domain. Regulators also tend to have a chilling effect on information sharing from the private sector, which would have undermined a key function of the NCSC, as a neutral broker of information. The NCSC's approach of setting out principles and outcomes, rather than prescriptive regulation, also seemed more likely to change behaviour beyond tick-box compliance.

The NCSC has, however, become a key adviser to sectoral regulators in the UK, sometimes playing a formal role, notably in the UK implementation of the EU Network and Information Systems Directive,[27] arguably the first cyber legislation at EU level. It has also worked with the Information Commissioner's Office (ICO) to develop joint guidance on the cyber security implications of EU GDPR (General Data Protection Regulation) implementation.[28] Cyber security is a subset of data privacy, but an important one: failure to take reasonable steps to keep information secure is now punishable by heavy fines. The NCSC's role in this is clear: it can help both companies and the ICO judge what are reasonable steps, although enforcement falls to the ICO.

27. NCSC, 'The NIS Guidance Collection', updated 31 October 2018, <www.ncsc.gov.uk/guidance/nis-guidance-collection>, accessed 21 January 2019.
28. NCSC, 'GDPR Security Outcomes', 18 May 2018, <www.ncsc.gov.uk/guidance/gdpr-security-outcomes>, accessed 21 January 2019.

Figure 2: Chart Showing UK Cyber Responsibilities



Source: The author.

Culture and Location

It was clear that to be successful, the NCSC could not simply rely on the machinery of government change. It had to work in a completely new way, blending open source and top secret, public sector and private. It also needed to win over the wider technical community as a centre of expertise and to allay concerns about secrecy.

The NCSC set out to be collaborative in a new way, between government and the private sector. It launched the Industry 100 scheme,[29] bringing in secondees from a wide range of sectors to sit alongside NCSC officials. While it will take time to work out the full benefits for both sides, the potential gains are great. Government cyber policy needs to be shaped by deep industry expertise from diverse sectors, while industry can benefit from government technical expertise and data, and show itself to be at the forefront of cyber awareness.

The NCSC also aims to foster collaboration with the third sector and with academia, notably in helping to sustain and improve the national cyber skills pipeline, and with international partners. Cyber security is uniquely blind to sovereignty and jurisdictions and improving the landscape for all is the only sensible goal.

If the NCSC was to be respected as housing world-class experts and generating thought leadership on cyber, it had to be open and accountable in a way not normally possible in the intelligence community. The tech community, by contrast, routinely shares much of its thinking and software, as the use of open source hosting sites like GitHub illustrates. The NCSC has maintained an open dialogue explaining the thinking behind its technical advice and inviting responses and discussion on its website. There is a lively series of blogs by experts on a very wide range of cyber issues, mostly anonymised to protect identities.[30] This very public engagement requires a high degree of technical expertise and self-confidence for staff used to working in secret. It also requires a large and active communications department.

It follows from this and from the scope of the NCSC that its location was important. George Osborne was clear that it should feel different from a government department, closer to and welcoming to the private sector. Despite some opposition, we were given permission to locate the NCSC headquarters in a new private sector building in Victoria, within the Government Security Zone and close enough to Whitehall for incident handling and Cabinet Office Briefing Room (COBR) meetings, but in a new private sector development. While equipped to deal with top-secret information, most of the NCSC's work would be unclassified and open and accessible to those without security clearance, including, of course, the industry secondees. In practice, several hundred of the NCSC's staff will probably always need to be located at GCHQ's high-classification buildings in Cheltenham and elsewhere, and that has its own benefits. Although integration of and exchange between the two workforces will remain important to the cyber security mission for the foreseeable future, civil service HR practices are notoriously complex and slow, and the challenge will be to give the NCSC the freedom necessary to recruit and retain talent, and to allow it to flourish.

The NCSC started work in shadow form in 2016 and the headquarters building was officially opened by Her Majesty Queen Elizabeth II and the Duke of Edinburgh on 14 February 2017. In welcoming them, I tried to draw a line between the achievement of Bletchley Park, for which the

29. NCSC, 'Introduction to Industry 100', updated 14 March 2018, <https://www.ncsc.gov.uk/information/industry-100>, accessed 21 January 2019.
30. NCSC, 'National Cyber Security Centre Blog', <www.ncsc.gov.uk/blog>, accessed 21 January 2019.

Queen has a great personal affection, and the contemporary challenges for GCHQ and others in the cyber era.[31]

31. Robert Hannigan, 'Director GCHQ Speaks at the Official Opening of the National Cyber Security Centre', NCSC, 14 February 2017, <www.gchq.gov.uk/speech/director-gchq-speaks-official-opening-national-cyber-security-centre>, accessed 21 January 2019.

IV. The Future for the NCSC

LOOKING NOW AT the NCSC as an outsider, and hearing feedback from private sector colleagues, has been broadly encouraging. The institution has quickly embedded itself as a leading authority, giving a single source of coherent advice and defining 'what good looks like' in a large number of areas. It has produced a wide range of readable, practical guidance, for example for small businesses and charities, or the legal sector, as well as blogging on key current topics from cloud security to quantum-safe cryptography. It has successfully pitched its materials at deep experts and foreign partners, as well as to businesses and members of the public. This is a tribute to former Head of Engagement Alison Whitney and the whole team.

The centre has also managed incident response well, coordinating across the public sector and assisting industry on most of the high-profile incidents since it began its shadow operations in 2016, and many others that are less newsworthy. Getting the threshold for NCSC involvement right will be a long and constantly shifting challenge.

The NCSC's work on skills and education has been impressive. Chris Ensor, deputy director for skills and growth, has a long-established credibility in higher education, and under his direction the list of accredited Academic Centres of Excellence has grown, the Cyber First schemes have expanded, and incubators and accelerators for cyber start-ups, private and government-sponsored, have launched in various parts of the UK. He and his team have driven the NCSC's diversity agenda, trying to reach those untapped areas of skills across the UK. The NCSC increasingly focuses on long-term schemes to set standards, for example working with the Department for Digital, Culture, Media and Sport on developing a cyber security profession for the future,[32] and the Cyber Security Body of Knowledge project.[33] Led by academics, this aims to lay the foundations of cyber security training by defining what areas of knowledge are essential to this newly established area of science.

In general, accreditation by the NCSC of cyber services and products is sought after as a trusted mark of at least baseline quality. Non-cyber companies have also used the Cyber Essentials certification scheme[34] in large numbers to test themselves and show customers they have taken cyber security seriously. In practice, any vendor wishing to work with the UK government must meet at least this baseline of cyber readiness.

---

32. UK Government, 'Developing the UK Cyber Security Profession', updated 31 August 2018, <www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession>, accessed 21 January 2019.
33. CyBOK, 'The Cyber Security Body of Knowledge', <www.cybok.org/>, accessed 21 January 2019.
34. NCSC, 'Cyber Essentials', <https://www.cyberessentials.ncsc.gov.uk/>, accessed 21 January 2019.

There are many areas where the NCSC will need to develop further. It needs to scale up to meet customer demand and rising threats, but like all organisations it struggles to recruit enough of the right skills. It remains over-dependent on a small number of world-class technical experts on its management board, and their immediate teams. The organisation will also need to establish a longer-term funding mechanism beyond the NCSP programme's life and the end date of the current Cyber Security Strategy in 2021. Its relationship with its parent, GCHQ, will continue to evolve and there will be pressures to adapt governance arrangements further.

At the operational level, the NCSC has not yet been tested by a C1 cyber attack affecting the UK. Nor has it had adverse publicity for perceived failures, which is bound to come at some stage. The CiSP information sharing platform has worked well, with more than 4,000 companies and organisations and 9,000 individuals participating, but its scale may affect its utility. The proliferation of other sectoral and industry sharing mechanisms in the UK, as in most countries, needs to be rationalised.

There is also further to go to streamline the various accreditation mechanisms to make them simpler and more coherent. The industry partnership, which sits at the heart of the NCSC concept, has made a good start, but needs to demonstrate value to both sides, especially to private sector organisations dedicating precious resources.

All these challenges are symptoms of the same problem: huge demand and expectation from customers; growing cyber threats; and too few skills. The NCSC was a key part of the UK government's strategic answer to these and has made significant headway in tackling them in the last two years. The struggle for government is in meeting high-volume cyber-enabled fraud; law enforcement is still not in a position to do much at scale and lacks the skills to meet the tidal wave of requests from the public.

If the NCSC is to keep up with the cyber threat and meet rising expectations, it will need to keep behaving in non-traditional ways, busting through public sector norms. It needs to take its lead as much from the disrupters, whether they are legitimate tech industries or innovative cyber criminals, as from traditional civil-service practices. Culturally, the NCSC has been refreshingly open in explaining its thinking and inviting challenge, particularly from other security experts; it has recognised that this is a valuable coalition and that government does not have all the answers.

The conviction that cyber defence must be done collaboratively and outside the bounds of secrecy is the right one. But the NCSC has further to go to convince the private sector that threat information sharing is two way and that government will release information quickly enough to be useful. Companies who release resources to the NCSC need to feel this is of value to their own defence as well as contributing to the national good.

V. The Proper Role of Government in Cyber Security

GOVERNMENTS ARE TORN between extremes in setting their level of ambition about cyber security. At one end there are unreasonable expectations that they can somehow provide comprehensive national protection from cyber attacks, particularly cybercrime, and at the other a sense that government is relatively powerless and that anything of value must be done in the private sector.

The reality is somewhere in between. It is true that some governments can draw on sophisticated intelligence capabilities and classified data, which can make a significant tactical difference to threat detection and incident handling, but government's most important contribution is at the strategic level. There are several strategic interventions open to most governments, in which the UK's experience has been mixed.

National-Level Defence

Governments can begin to harden the existing infrastructure at a national level if they work with telecommunications companies and internet service providers (ISPs), as the Active Cyber Defence programme has demonstrated (see Appendix II). The NCSC's experiments have been innovative and promising. Although without international agreement this will only raise the baseline so far, anything which challenges the business model of cyber criminals and hardens the national cyber environment is worth doing.

Behavioural Change

More significantly, governments can not only encourage behavioural change, but have the regulatory levers to accelerate it. Since much of the problem in cyber security stems from poor user awareness and behaviour, this is a key area for intervention. The UK has spent a great deal of effort in trying to educate the private sector and individuals on cyber security. The numerous surveys published every year on cyber readiness confirm that there has been some improvement at board level in major companies and greater awareness in small and medium-sized enterprises (SMEs), much of it driven by headline-grabbing cyber incidents rather than government initiatives. But there is a limit to how much further awareness levels will climb and, more seriously, a lack of correlation between awareness of the problem, knowing what to do, and doing it.

Security by Design and Regulation

The great prize of the next phase of the internet's development will be to ensure that cyber security is built in by default and by design. Governments and multilateral alliances have a clear role here. My own view is that the UK has been too slow to use regulatory levers and too reliant on exhortation, risk management and micro interventions. For example, New York State's 2017 cyber security regulations are prescriptive and, for all the criticism of their detail, have had a significant impact on the spending priorities and policies of financial institutions.[35] California appears to be leading the way in imposing regulation on the Internet of Things (IoT) – connected devices, which have been a persistent source of vulnerability, given their often weak or non-existent security features.[36] US federal legislation has also been drafted along similar lines.

By contrast, the UK has chosen a softer approach. The Department for Digital, Culture, Media and Sport, in cooperation with the NCSC, has published very sensible guidance on consumer IoT devices.[37] Its Secure by Design objective could do more to improve security than almost any other initiative, but without regulatory force, manufacturers seem likely to resist the extra costs. This is an area where the market does not easily correct because there is no immediate cost to the consumer or manufacturer from poor security: a cheap CCTV camera hijacked for criminal purposes will probably still work as a camera.

The main pressure for cyber regulation in the UK has been from the EU, notably through its Security of Network and Information Systems Directive,[38] which came into force in 2018. This covers some high-level cyber security requirements in critical sectors and industries. Each member state has incorporated this directive separately and the UK's approach, set out by the NCSC, has been 'outcome-based' and reliant on 'principles', rather than being prescriptive. There are, of course, dangers in being prescriptive: technology develops so quickly that prescriptive solutions need constant updating, and achieving an outcome in cyber security depends greatly on the specifics of the network and the context. However, a high-level outcome-based approach can end up with broad aspirations and not enough detail to be of use to practitioners. This tends to be the criticism levelled at the NCSC's guidance in general and there is certainly a demand for more specific action points.

---

35. New York State Department of Financial Services, 'Cybersecurity Requirements for Financial Services Companies', 23 NYCRR500, 1 March 2017, <www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf>, accessed 21 January 2019.
36. California Legislative Information, 'SB-327 Information Privacy: Connected Devices', Senate Bill No. 327, <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327>, accessed 21 January 2019.
37. UK Government, 'Code of Practice for Consumer IoT Security', updated 14 October 2018, <www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security>, accessed 21 January 2019.
38. NCSC, 'Introduction to the NIS Directive', updated 31 October 2018, <www.ncsc.gov.uk/guidance/introduction-nis-directive>, accessed 21 January 2019.

In the future it seems likely that the EU will drive further detailed cyber security legislation which many other countries, including the UK, will have to follow if they wish to do business with Europe. It also seems likely that regulators will increasingly look to make IT providers liable for vulnerabilities that open users up to attack. There is something to be said for this: we should not expect cyber security to be an 'extra' service or product, paid for separately. All companies, and especially IT providers, will have a responsibility to build in and constantly improve security. But there will inevitably be a debate about the degree to which reasonable steps have been taken and concerns that an approach that is too restrictive will stifle innovation. For example, each new version of Windows or iOS has vulnerabilities and flaws, but deciding whether a particular version has been reckless or careless in cyber security terms could lead to an endless legal and technical debate. Equally, waiting for perfect software would mean waiting forever. Nonetheless, using liability to drive improvement is likely to be a powerful secondary lever for governments in the future.

Supply-Chain Integrity and Inward Investment

A key aspect of the debate about regulation has been a growing international concern about the integrity and security of the global IT supply chain. Geopolitical instability has brought to the fore longstanding concerns in the intelligence community that hostile states could use the manipulation of hardware or software to launch cyber attacks.[39] This has always been true, but the growing reliance on IT products and services manufactured or administered from outside Western democracies, notably in China, has accelerated the debate. There is unquestionably some protectionism and trade conflict thrown into this mix, but the fundamental problem for all states is clear: how to assure themselves that the IT infrastructure on which their economies rely is not being subverted, whether for espionage, intellectual property theft, or some more active cyber intervention. It is hard to overstate the scale of the challenge. Even understanding a modern supply chain is difficult: most hardware is made in China, whatever the brand, and software is likely to be subcontracted many times over. Complete visibility is difficult, still less assurance at every stage.

I have written a number of times about the strategic challenge of the IT supply chain to Western governments. Even the largest state will struggle to assure itself about more than a fraction of hardware and software.[40] This will become exponentially more difficult as China leads the world in an increasing number of technologies, notably in areas of artificial intelligence (AI). Simply

39. The most sensational example of this issue is a story run by *Bloomberg Businessweek* in October 2018, alleging that an 'extra chip' had been inserted into the 'motherboards' made by a particular US company during the manufacturing process in China. While the story itself has been widely discredited, it has at least drawn attention to the wider issue of supply-chain integrity. See Jordan Robertson and Michael Riley, 'The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies', *Bloomberg Businessweek*, 4 October 2018.
40. Robert Hannigan, 'Wake up to the Security Risks in Chinese Tech Dominance', *Financial Times*, 27 July 2018; Robert Hannigan, 'The Strategic Threat to U.S. Tech Companies', *Washington Post*, 12 October 2018.

banning hardware or software from certain countries in the hope that a domestic industry will suddenly be revived is not a sustainable response, but neither is giving up on assurance.

The UK's policy approach has been uncertain. Successive UK governments have championed their openness to inward investment and have in any case lacked the kind of powers to intervene which are available to the US administration and to Congress or to many other countries, from France to Australia.[41]

The UK's approach to Chinese telecommunications giant Huawei's involvement in national telephony networks is a case in point (see Box 1). It attempted to take a middle line between banning Huawei products and giving the company unmonitored access. There are many reasons to be critical of the UK's choices, most of them set out in an ISC parliamentary report in 2012.[42] The most serious conclusion is that the Huawei Cyber Security Evaluation Centre (see Box 1) cannot give complete assurance that risks to national security have been mitigated. But it was never intended to do so, and indeed total assurance is unachievable. The real question is whether the assurance is adequate and better than the alternatives.

Whatever the judgement on the UK's approach, this is undeniably an area where government intervention will become increasingly critical. Nor will it be confined to threats from nation states. Manipulation of software by VW to subvert emissions tests,[43] and Uber's attempts to evade regulatory authorities using the Greyball programme, illustrate the scale of the wider challenge.[44]

Box 1: The Huawei Experiment

The Inward Investment Story

Having waited until the decision had been made by BT to install Chinese telecommunications company Huawei's equipment into the heart of its telecommunications networks in 2003, the UK government at the time set about finding a way of reassuring itself about the risks to national security. As a result, and after a number of iterations, the Huawei Cyber Security Evaluation Centre (HCSEC) was established, funded by Huawei but with staff vetted by GCHQ. In response to a critical parliamentary report by the ISC in 2012, the governance of this body (sometimes referred to as the 'cell') was revised with the

41. Following a consultation in 2017, the UK government published a white paper outlining how these intervention powers would be strengthened. See UK Government, *National Security and Investment: A Consultation on Proposed Legislative Reforms* (London: The Stationery Office, 2018).
42. Intelligence and Security Committee of Parliament, *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security*, Cm 8629 (London: The Stationery Office, 2013).
43. Russell Hotten, 'Volkswagen: The Scandal Explained', *BBC News*, 10 December 2015.
44. Julia Carrie Wong, 'Greyball: How Uber Used Secret Software to Dodge the Law', *The Guardian*, 4 March 2017.

establishment of an oversight board chaired by GCHQ. It published an annual report to the national security adviser, the first appearing in 2015, although work had been going on for some years. Along with other cyber responsibilities, this passed (within GCHQ) to the NCSC in 2016.

The cell was and is innovative to the extent that it looked for new ways of detecting vulnerabilities that could lead to national security risk. Arguably, it therefore spent its early years improving Huawei's engineering. But it did provide a high degree of reassurance. A number of problems emerged, the most persistent being 'binary equivalence' (crudely, whether the code being inspected by the HCSEC is the same as that actually deployed). Added to that, Huawei's own use of third-party suppliers has illustrated the security risk of unsupported software. These issues eventually led the HCSEC to issue its first critical report in 2018, in which it concluded that 'only limited assurance' could be given that risks to national security had been mitigated. This was an understated but, in the context of earlier reports, radical conclusion, and was widely interpreted as a warning shot to Huawei to take government concerns more seriously. But it remains the case that the HCSEC has at no point expressed concern about Chinese state activity through Huawei and has found no evidence of this.

A full and convoluted story of the national security oversight of Huawei in the UK can be read in the ISC report and the annual reports of the HCSEC since 2015. But having been involved in the process and ultimately responsible for the technical oversight while director GCHQ, I think it worth making some brief comments, without drawing on classified material.

Conclusions

There is no question that the cell has developed world-class methods and expertise for vetting products and software installed into UK networks. These may well be useful and applicable elsewhere. As a result of the HCSEC's creation, the UK government understands Huawei – its code, policies, management and culture – better than any other government or customer outside China. The HCSEC has not been naive: the cell always understood the nature of the Chinese Communist Party's reach into the Chinese private sector. For that reason, among others, Huawei had little presence in the core of UK 3G/4G networks.

However, the HCSEC cannot provide total assurance, partly for the reasons set out in the reports, but also because deciding what is a vulnerability or a flaw, and what is a deliberately designed 'backdoor' to allow illicit access, is a matter of judgement. This is particularly true when one is trying to judge possible vulnerabilities that could emerge or be exploited in some years' time, several upgrades down the line, or to make assessments of managed services. To some extent this will be about political judgement, which is why the risk assessments in the HCSEC annual reports are partly political: they depend on the government's tolerance of risk and their assessment of future hostile intent.

More practically, the Huawei solution cannot be recreated for every company: the skills simply do not exist on that scale. Furthermore, not only is the solution not easily scalable, but the sanctions are limited. Beyond an extreme option of declaring a company untrustworthy, and expecting that this will damage its reputation internationally, there are few levers for the government to pull. Even if it

reaches that extreme conclusion, following through and removing equipment from networks would arguably be impossible.

My conclusion is that the UK's Huawei experiment suggests that we cannot scan or vet our way out of the supply-chain integrity problem, but neither can we simply ban things on the basis of their origin. We will need to find ways of working with and taking advantage of the world-class technology emanating from China. That will mean finding sensible mechanisms for reassurance and risk mitigation, a process in which the wider tech industry will need to be involved and which will demand ever-greater transparency.

Above all, we need judgements that are informed by deep technical knowledge, for example of 5G telephony and the possible risks arising from particular suppliers. The debate in recent months seems to be driven as much by protectionism and near-hysteria about all things Chinese. This is not a sensible basis for assessing risk and making policy: what is needed is a technically expert assessment of the technology matched with a clear-eyed view of the potential threat. That, in short, is what the HCSEC tries to achieve.

Sources: Huawei Cyber Security Evaluation Centre Oversight Board, 'Ist Annual Report 2015: A Report to the National Security Adviser of the United Kingdom', March 2015, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/416878/HCSEC_Report.pdf>, accessed 21 January 2019; Huawei Cyber Security Evaluation Centre Oversight Board, 'Annual Report 2018: A Report to the National Security Adviser of the United Kingdom', July 2018, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf>, accessed 21 January 2019; Intelligence and Security Committee of Parliament, Foreign Involvement in the National Critical Infrastructure *(London: The Stationery Office, 2013).*

Cyber Security Exports

Although outside the scope of this paper, it is worth noting that the UK government had been keen to develop and promote the UK cyber security industry for the export market for some years, publishing a strategy in 2013.[45] In the years that followed, government support increased significantly, particularly for government-to-government sales. This included the appointment of Conrad Prince, a former director-general for operations at GCHQ, as cyber security ambassador, in what subsequently became the Department for International Trade (DIT). In March 2018 DIT published a new strategy,[46] which predicted that UK cyber security exports would rise to £2.6 billion by 2021 and set out a number of ways in which government intended to support and promote that growth.

Cyber Deterrence and the Rise of Nation State Threats

The major state-backed ransomware attacks of recent years, and particular aggression from Russia, have highlighted the role of nation states in conducting sophisticated attacks. This has presented the UK with a dilemma over public attribution and, in common with other states, a policy challenge on how to raise the cost for adversaries. 'Cyber deterrence' has been much debated internationally, with little firm consensus except about the difficulties.[47]

In contrast to the US, where the FBI indicted Iranian hackers in 2012, and subsequently Chinese and Russian state-linked individuals, the UK was very resistant to attribute cyber attacks publicly. This was partly political caution, partly concern over the state of our defences against retaliation, and partly an ingrained instinct in intelligence services not to reveal the extent of knowledge of adversaries.

For example, the UK eventually followed the lead of the US in publicly voicing concerns about the potential for Russian state misuse of the anti-virus products of Kaspersky Labs in 2017,[48] and, following the extreme provocation of the Russian chemical weapons attack in Salisbury in 2018, the NCSC joined with US counterparts in 'outing' and attributing a number of Russian cyber

45. UK Trade and Investment, 'Cyber Security: The UK's Approach to Exports', April 2013, <https://www.gchq.gov.uk/sites/default/files/Cyber_Security-the_UKs_approach_to_exports.pdf>, accessed 21 January 2019.
46. Department for International Trade, 'Cyber Security: Export Strategy', March 2018, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/693989/CCS151_CCS0118810124-1_Cyber_Security_Export_Strategy_Brochure_Web_Accessible.pdf>, accessed 21 January 2019.
47. See George Perkovich and Ariel Levite (eds), *Understanding Cyber Conflict: 14 Analogies* (Washington, DC: Georgetown University Press, 2017).
48. NCSC, 'Letter to Permanent Secretaries Regarding the Issue of Supply Chain Risk in Cloud-Based Products', 1 December 2017, <https://www.ncsc.gov.uk/information/letter-permanent-secretaries-regarding-issue-supply-chain-risk-cloud-based-products>, accessed 21 January 2019.

activities, particularly those of the GRU military intelligence agency.[49] For many months after the Wannacry ransomware attack, the UK formally held back from attributing this to North Korea.

In December 2018, the UK joined the US in attributing to China a campaign of attacks against managed service providers worldwide,[50] stretching back at least three years and nicknamed 'Cloud Hopper' by security researchers.[51] Attributing the 'APT 10' group that carried out this attack to the Chinese Ministry of State Security was not new and the announcement was more significant for its timing and political intent.

The willingness to attribute and call out bad behaviour is a welcome development. A firmer and earlier attribution in some of these cases might have helped to constrain hostile activity.

Whether or not the UK's particularly soft approach to cyber attribution has been adequate, it is not alone in struggling to find an effective approach to cyber deterrence. There are some fundamental problems. Western economies and societies are by definition more open and vulnerable than the networks of state cyber aggressors, who tend to be under authoritarian rule. The risks of retaliation are therefore asymmetric. More importantly, 'hitting back' is rarely a feasible response, despite the salience of this headline in political terms. Outside a full conflict, Western democracies will not regard the kind of actions of, for example, Russia, as lawful or consistent with their values: for example, Russia targeting Ukrainian citizens by switching off their domestic power supply to exert political pressure. There may be targeted uses of offensive cyber weapons which can be limited to those individuals or organisations responsible for ordering, devising or executing cyber attacks, but in practice this is likely to be difficult. It has been suggested that offensive cyber techniques should be used simply to demonstrate Western power – a show of force – but it is hard to find targets that are both high enough profile to have impact, but low enough in impact not to breach what is lawful and ethically acceptable.

Beyond shedding light on Russian attacks and 'naming' them, a more rational response to cyber aggression is likely to involve other actions, for example economic sanctions and diplomatic isolation. The truth is that aggressive nation states behave online much as they do in the physical world, with the same degree of recklessness and disregard for collateral damage or unintended consequences. The objective of any Western deterrence or threat response should be to illustrate the consequences of stepping outside the civilised norms which govern relations

49. NCSC, 'Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed', news, 4 October 2018, <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed>, accessed 21 January 2019.
50. The victims reportedly included some of the world's largest IT companies. See Christopher Bing, Jack Stubbs and Joseph Menn, 'Exclusive: China Hacked HPE, IBM and Then Attacked Clients – Sources', *Reuters*, 20 December 2018.
51. UK Government, 'UK and Allies Reveal Global Scale of Chinese Cyber Campaign', press release, 20 December 2018, <https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign>, accessed 19 January 2019.

between states. The fact that these norms have not yet been codified or agreed for cyberspace does not change the basis of this approach.

Offensive Cyber and the Military

The National Cyber Security Strategy 2016–2021 is explicit that the UK has an offensive cyber capability:

> Through our National Offensive Cyber Programme (NOCP), we have a dedicated capability to act in cyberspace and we will commit the resources to develop and improve this capability. … We will ensure that we have at our disposal appropriate offensive cyber capabilities that can be deployed at a time and place of our choosing, for both deterrence and operational purposes, in accordance with national and international law. … To do this, we will: invest in our NOCP – the partnership between the Ministry of Defence and GCHQ that is harnessing the skills and talents of both organisations to deliver the tools, techniques and tradecraft required; develop our ability to use offensive cyber tools; and develop the ability of our Armed Forces to deploy offensive cyber capabilities as an integrated part of operations, thereby enhancing the overall impact we can achieve through military action.[52]

The high classification of offensive cyber capabilities makes it difficult to discuss in any detail, but ministers have avowed this programme and announced the first use of capability developed under NOCP in a battlefield context against Daesh (also known as the Islamic State of Iraq and Syria, ISIS) in 2017. The current director GCHQ, Jeremy Fleming, has also made public the long campaign against Daesh media which we launched at then Prime Minister David Cameron's direction in January 2016.

It is worth making some brief remarks about offensive cyber which might be relevant to others. The definition itself is problematic: not all computer network exploitation or hacking is necessarily 'offensive'. The term tends to be reserved for destructive effect, but it can cover a spectrum from intelligence and information operations to cyber-enabled physical destruction.

The NOCP was a joint MoD/GCHQ programme intended, as ministers said, to develop capabilities. In contrast to the National Security Agency (NSA) in the US, GCHQ had always had the legal authority to mount offensive cyber operations and had done so under ministerial authorisation in limited cases. The skills and access necessary to do this resided almost exclusively in GCHQ, and of course support for military operations has always been a key part of GCHQ's mission; it has had a large number of military officers as part of the workforce, funded by GCHQ. The challenge of NOCP was to broaden this into the UK military and improve and increase the skills. The UK single services have made great strides in cyber, but have much further to go. Unlike in the US, it is difficult to spend a whole career in cyber in the UK armed forces, for example; all involved know this will need to change. But career structures and incentives take time to modify and they lag behind the agility needed for personnel who are trained in the constantly advancing technologies applicable in cyber conflict.

52. HM Government, 'National Cyber Security Strategy 2016–2021', 2016, p. 51.

The other policy challenge was to define the priorities for use and therefore for the research and development of offensive cyber capabilities. There will always be a healthy tension between high-end military contingency requirements for warfighting and more tactical uses, for example in counterterrorism or countercrime. Ultimately those priorities need to be set by ministers and to be consistent with a wider National Security Strategy. The UK was fortunate to have in this period a series of military chiefs, under the Chief of the Defence Staff Stuart Peach, who not only understood cyber but were pragmatically committed to making NOCP work.[53] Peach personally championed the creation of a Cyber Reserve for the UK,[54] making use of talents beyond the serving military.

In governance and structural terms, we made an early decision not to imitate the US model of a separate Cyber Command alongside the NSA. Given the scale of the UK system, duplication was not viable or affordable, and an integrated military-civilian model seemed preferable. What was clear was that once NOCP became mature we would need something more than a funding programme but less than a Cyber Command. As has been widely speculated in the press,[55] some kind of Joint Cyber Force or National Cyber Force seems a sensible way forward.

Having a different structure from the US has not hampered formal four-way cooperation between the UK and its American counterparts – the MoD (Joint Forces Command), US Cyber Command, the NSA and GCHQ. Ministers have signed formal agreements to further this cooperation.[56]

Skills

Governments should, in principle, be able to make strategic interventions in the education system to effect long-term change. The UK's efforts here, consciously drawing on the Israeli cyber education programme, have been energetic and high profile. 'Cyber First' has been impressive (see Appendix I). But ultimately these are micro-interventions. The UK is a long way from fostering the excellence in STEM (science, technology, engineering and maths), let alone the entrepreneurial spirit, which underlies Israel's success in cyber. Changes to the national curriculum, training of teachers, support from the private sector, and a strategic focus on relevant skills at school and in the community are far from being addressed at a national level, despite some excellent individual initiatives such as Cyber First or the Cyber Security Challenge

53. Gordon Messenger, as Vice-Chief of the Defence Staff, was key to driving the offensive cyber project, along with Chris Deverell as Commander, Joint Forces Command.
54. Gov.UK, 'Working for JFC', <https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment>, accessed 21 January 2019.
55. Lucy Fisher, 'Britain Launches £250m Cyber-Force to Wage War on Terrorists', *The Times*, 21 September 2018.
56. Terri Moon Cronk, 'U.S.–U.K. Cyber Agreement Opens Doors for Both Nations', US Department of Defense, news article, 8 September 2016, <www.defense.gov/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/>, accessed 21 January 2019.

UK.[57] Without getting the pipeline right, the capacity of the UK cyber security industry will inevitably be constrained.

Organisational Change

The machineries of government changes are of course the preserve of governments and often a substitute for substantive action. Civil servants and politicians will always attach disproportionate significance to these for understandable reasons. But however well a system is organised, it will not of itself bring about tactical or strategic change to the threat landscape or to the nation's cyber defences. Arguably the UK took too long to reach the conclusion that centralising operational cyber activity in one institution and placing it under the control of experts was the right thing to do. Smaller states, such as Israel, and particularly those with strong central planning, such as Singapore, got there more easily. Governments can only move at their own pace, but the slow evolution experienced in the UK could be shortened by an audit of existing cyber capabilities and an honest conversation, driven from the top of government, about the organisational and governance structures that will be optimal for clarity, agility and impact in the areas described above.

International Partnerships

In creating the NCSC, we looked at or were already familiar with many international models. While our work was operationally closest to our US allies, the sheer scale of the US inter-agency cyber landscape, the domestic politics of intelligence gathering, differing legal authorities, and a number of other issues made comparison difficult. In practice, the NCSC was welcomed and supported by my counterpart, Mike Rogers, director of the NSA and head of cyber command. Without the NSA's support it would have been difficult to locate the NCSC within GCHQ. Other Five Eyes countries (Australia, Canada, New Zealand, the UK and the US) also had important models for cyber security, notably the Canadian government's excellent defence of Canada's public sector networks.[58] At the time of the NCSC's launch, Australia had already launched a similar body, the Australian Cyber Security Centre (ACSC), co-locating relevant agencies, although not under the complete command of the Australian Signals Directorate (ASD), GCHQ's equivalent. It has since reorganised the body as a result of Australia's 2017 intelligence review,[59] and in July 2018 placed the ACSC wholly under the ASD.

We also looked at impressive models in Israel and Singapore. A number of European countries have highly competent organisations, but in general there is a divide between civilian, and military or intelligence agencies. Each country has slightly different legal frameworks and

57. Cyber Security Challenge UK, 'Play the Challenge', <https://www.cybersecuritychallenge.org.uk/>, accessed 21 January 2019.
58. Canadian Centre for Cyber Security, <https://cyber.gc.ca/en/>, accessed 21 January 2019.
59. Australian Government, *2017 Independent Intelligence Review* (Canberra: Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2017).

authorities, and each has different constraints on information sharing between government agencies and with the private sector.

One of the key early requirements for the NCSC has been to establish strong and practical working relationships with counterparts around the world, although in some countries that will inevitably mean working with a variety of agencies in a single country.

Horizon Scanning

Governments should, of course, be leaders in horizon scanning and anticipating future trends and requirements. In cyber, as in many other areas, the UK has struggled to do this, and better answers are often found in the private sector, academia and think tanks. This is particularly true in technology, where governments no longer have primacy in new developments in a way they might have done 50 years ago. They have generally become the objects or even victims of technology change rather than the authors or drivers. This demands an ever-greater reliance on external expertise to predict the likely impact of technology trends on the safety and security of a networked society and economy, as well as the social and political impacts.

Conclusion: The Strategic Challenge

Any discussion about future trends in cyber security has a tendency to be reduced to a list of vague and fashionable buzzwords: AI; machine learning; blockchain; quantum computing; and so on. But the high-level challenge is to ensure that we build in safety and security to the next-generation networks, rather than having to retrofit security and play catch-up as we have over the last 30 years. The era when cyber security has been an ‘extra’, in which of course the cyber industry has had some self-interest, should be coming to an end.

The exponential rise in data volumes which will flow both from the IoT and the connection of the other half of the world’s population who are currently not online is part of the challenge. The other is the speed and sophistication of processing, including through the use of AI, which will inevitably render humans as bystanders rather than decision-makers in many areas. This puts a strategic premium on trust. How will we ensure that software, hardware and the algorithms dictating so much of the automation of the future can be trusted? Part of the answer will be intelligent regulation, and another will be in data science.

The truth is that cyber threats are visible precisely because they are on the internet, but they hide in the noise. Big data and the sheer scale of the internet has been used as an asymmetric advantage for criminals and nation state attackers; it needs to be employed even more effectively for defence. The private sector and the general public will be at the heart of this, because it is their data, but governments will have a convening and, where appropriate, a legislative role in facilitating it.

Appendix I: The UK Cyber Security Strategy

I have briefly described the first UK Cyber Security Strategy published in 2009,[60] and its successor in 2011.[61] Government strategies in the UK have a tendency to catalogue actions that are already underway and the same is true of the third National Cyber Security Strategy 2016–2021,[62] setting out plans for spending the £1.9 billion to be invested over the five-year spending period. It is an impressive and coherent piece of work and worthy of the translation it has received into many languages. Its key strategic change is that it is explicit about an expanded role for government, rebalancing what is reasonable to expect from business and the individual:

> Only Government can draw on the intelligence and other assets required to defend the country from the most sophisticated threats. Only Government can drive cooperation across the public and private sectors and ensure information is shared between the two. Government has a leading role, in consultation with industry, in defining what good cyber security looks like and ensuring it is implemented.[63]

The strategy sets out how government would incentivise change.

Having briefly surveyed the threat picture, highlighting the rise of a commodity market in hacking services, which was and still is transforming the scale and sophistication of cybercrime, the strategy sets out the national response under three headings: Defend; Deter; and Develop.

- The **Defend** strand sets out how the government intends to harden the UK's defences: 'together with citizens, education providers, academia, businesses and other governments, the UK can build layers of defence that will significantly reduce our exposure to cyber incidents'.[64]

This approach includes Active Cyber Defence (see Appendix II), a parallel programme to promote 'secure by default' technology,[65] designing security into products and services at the earliest stage, which was expanded into an excellent Secure by Design report from the Department

60. Cabinet Office, *Cyber Security Strategy of the United Kingdom.*
61. Cabinet Office, 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World'.
62. HM Government, 'National Cyber Security Strategy 2016–2021'.
63. *Ibid.,* p. 27.
64. *Ibid.,* p. 33.
65. NCSC, 'Secure by Default', <www.ncsc.gov.uk/topics/secure-default>, accessed 21 January 2019.

for Digital, Culture, Media and Sport, focused on the IoT.[66] The report outlines steps to raise standards across the whole of the public sector and a focus on the critical national infrastructure and other critical sectors, such as financial services.

A critical part of this strand was making available the best coherent advice and raising awareness, both among the public (for example, promoting innovative password advice) and launching a scheme, Cyber Essentials,[67] to help businesses measure their own readiness and improve their defences.

Under the Defend strand, the government also undertook to manage incidents in a way that was less 'fragmented' than in the past, through the NCSC providing 'a single, joined-up approach to incident management, based on an improved understanding and awareness of the threat and actions being taken against us. The NCSC will be a key enabler, as will partnership with the private sector, law enforcement and other government departments, authorities and agencies'.[68]

- The **Deter** strand is, not surprisingly, given the still nascent policy debate in this area, the shortest, and concentrates on the law enforcement response, led by the National Cyber Crime Unit of the NCA. It also mentions countering state threats, notably offensive cyber capability, and briefly outlines a commitment to further developing encryption and protecting sovereign cryptographic capabilities.

- The **Develop** strand is the most ambitious and long term, aiming to develop a cyber-skilled workforce, a dynamic academic sector, a thriving cyber start-up environment and a strong export market. The challenge for any government is to keep focused on this long-term strategic improvement and not to become swamped by the emphasis on cyber threat and defence.

This strand sets out a whole range of educational initiatives: a schools programme for talented 14 to 18 year olds; higher- and degree-level apprenticeships focused on particular sectors; cyber graduate and postgraduate education; accreditation of teacher professional development in cyber security; developing the cyber security profession, including through achieving Royal Chartered status by 2020; a Defence Cyber Academy; and setting standards for cyber education at every level of the national curriculum.

The strategy also commits to expanding the highly successful Cyber First programme of scholarships and training projects, which was consciously inspired by and copied from the Israeli

66. Department for Digital, Culture, Media and Sport, 'Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report', 7 March 2018, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf>, accessed 21 January 2019.
67. NCSC, 'Cyber Essentials'.
68. HM Government, 'National Cyber Security Strategy 2016–2021', p. 44.

equivalent.[69] The programme offers development at a range of levels from early secondary- to higher-level education and we expanded it in 2017 to host the first-ever girls-only cyber summer course and the first national cyber competition for school-age girls. Both have been extremely successful and gave the lie to the belief that girls were not interested in cyber: some 8,000 took part in the first competition. I visited one of the first girls-only summer schools in 2016 and it was clear that the participants found the approach empowering.

The Develop strand also outlines measures to support academia and to develop the cyber security sector, not least for export. GCHQ had effectively accredited universities as centres of excellence for cyber security in 2014;[70] this function was taken over by the NCSC on its creation and the relevant research arms of government. The intention is that by 2021 at least 150 PhDs in key areas of cyber security will have been completed.

The 2016–21 strategy also sets out ambitions for agreeing international norms on cyberspace, but without any firm hope of implementation.[71]

69. NCSC and Department for Digital, Culture, Media and Sport, 'Cyber First', <www.cyberfirst.ncsc.gov.uk/>, accessed 21 January 2019.
70. HM Government, 'Developing our Capability in Cyber Security: Academic Centres of Excellence in Cyber Security Research', updated July 2015, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496340/ACE-CSR_Brochure_accessible_2015.pdf>, accessed 21 January 2019.
71. HM Government, 'National Cyber Security Strategy 2016–2021', pp. 63–64.

Appendix II: Active Cyber Defence Programme for the UK

It is always tempting for public institutions to think that the machineries-of-government changes are an end in themselves. While reorganising government departments and capabilities was critical to enabling progress, it was clear that this alone would not improve the UK's cyber security. We were keen to take the opportunity offered by the creation of a National Cyber Security Centre to try to answer the bigger question of what would actually make the UK 'the safest place to live and do business online', a clear ambition set out by then Foreign Secretary William Hague in his letter to then Prime Minister David Cameron and other Cabinet colleagues in 2010.[72]

If the government was to become more interventionist, what should it actually do? The exam questions were tantalising for any technical person:

- Given a clean sheet of paper, what would you do at a national level to make the UK safer in cyberspace?
- How can we put right some of the security flaws built into the internet?
- How do we change the economic equation for cyber criminals and alter the attacker–defender landscape?

While discussions were continuing about the creation of the NCSC, Ciaran Martin and I put this question to Ian Levy, later the NCSC's first technical director, but at that point a key leader of the CESG within GCHQ. He was recognised in wider industry as a world-class talent and a genuine thought leader. He came back fairly quickly with a list of 12 actions which could make a long-term difference, automated and at scale, to the cyber health of the UK – the Active Cyber Defence (ACD) programme. They were subsequently refined to seven key strands, which Levy set out in a blog in November 2016 (see below).[73] It is noteworthy that the programme was essentially the creation of one deep expert. At a hearing of the parliamentary ISC, I was asked why ACD had not been thought of before. The answer, I thought, was simple: no one had asked the obvious question of the right experts. Particularly in the UK civil service, which tends to favour generalism over deep and long expertise, there simply were not individuals who could give creative technical advice, or indeed assess suggestions made by others.

---

72. The letter was unpublished, but the phrase has become a strapline for the NCSC. See NCSC, <https://www.ncsc.gov.uk/>, accessed 21 January 2019.
73. Ian Levy, 'Active Cyber Defence – Tackling Cyber Attacks on the UK', NCSC blog, 1 November 2016, <www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk>, accessed 21 January 2019.

Below is Levy's breakdown of the ACD programme into seven key strands.

1. **Fix the underlying infrastructure protocols**
   This focused on 'changing the implementation of Border Gateway Protocol (BGP), the protocol used to sort out IP routing between carriers, and SS7, the international telecoms signalling protocol, so that we can stop trivial re-routing of UK traffic',[74] with the ambition of making it harder to hijack a UK prefix by BGP and, in the longer term, to make DDoS (Distributed Denial of Service) and prefix hijacks globally much more difficult.

2. **Make email mean something again**
   This was probably the key example of the shift in the government's strategy away from blaming users and expecting individuals to bear all the strain of security. Email was, and is, a key delivery vector in a high proportion of cyber attacks – whether nation state or criminal in origin – and uses misplaced trust in the sender of the email to deliver malware. Asking users to make judgements about trusted sources was becoming untenable, as the government itself had discovered through the abuse of government institutions, notably the case of false emails from HMRC, the UK tax authority.[75]

   ACD promoted the use of internet standards to tackle spoofing, making Domain-Based Message Authentication, Reporting and Conformance (DMARC) mandatory for government, to prevent the spoofing of gov.uk and other public sector domains. If successful within government, the intention was to get industry to do the same at scale, essentially creating 'a reputation system for email domains and addresses, run by the industry'.[76]

3. **Go looking for badness and take it down**
   The ACD programme piloted a partnership with an innovative SME, tasked with 'looking for phishing hosted in the UK, webinject malware hosted in the UK and phishing anywhere in the world that targets a UK government brand'.[77] The partner dealt with the hosting provider to take down relevant domains, shortening their lifetime for potential victims.

4. **Filtering DNS to manage impact**
   Domain name system (DNS) filtering was at the heart of the ACD programme and the most potentially controversial part, because it could be portrayed as censoring or restricting the access of individuals. In Levy's words, it aimed to address an obvious question: 'is it OK for the infrastructure in the UK to allow users to unknowingly access

74. *Ibid.*
75. Described in detail by Ciaran Martin in his speech at the Billington Cyber Security Summit, 13 September 2016, <https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk>, accessed 21 January 2019.
76. Levy, 'Active Cyber Defence – Tackling Cyber Attacks on the UK'.
77. *Ibid.*

sites that are known to do them harm?'.[78] The key to addressing suspicions about surveillance or censorship would be to make this something from which there was an easy opt-out for citizens.

As a pilot, it was suggested that the NCSC would partner with Nominet, the .uk domain name registry, to build a large recursive DNS service for the public sector. That would have a response policy zone (RPZ) that stops users of the service accessing anything known to be harmful. If successful, the intention was to discuss with ISPs the possibility of doing the same at scale for their customers. This initiative has been implemented for government, but not for citizens yet.

5. **Drive the UK software ecosystem to be better**
   To address the other key vector for cyber attacks, the exploitation of unpatched software (operating systems and other software with known security weaknesses, vulnerable to cyber attacks), this DNS pilot intended to warn users visiting gov.uk websites if their software was out of date. In theory, this could go beyond simply warning users to denying access to those who have not updated software. For particularly sensitive transactions, whether involving personal data or payments, this might be particularly important, although there were clearly public policy implications in denying citizens access.

6. **Help government get better**
   This strand focused on providing practical protective solutions at scale for government services which would not naturally have the resources or expertise to run their own cyber security operations. An early example was the 'Web Check' service, a simple web vulnerability scanning service offered free to the government owners of public-facing websites and web services, providing a report on vulnerabilities and misconfigurations and how to address them.

7. **Encourage innovative alternatives for identity and authentication**
   A long-term strand addressing another key cause of cyber attacks, this was intended to encourage and trial new techniques to replace passwords as authentication. The UK was an early adopter of government digital services for citizens and this itself offered the possibility for piloting and de-risking innovative new technologies. It was part of a wider push to improve the default security of software and hardware, building in security at the design stage. This was subsequently launched as the Secure by Default initiative in 2017.[79]

With hindsight, the name of the programme – Active Cyber Defence – was probably not helpful. ACD covers a broad spectrum but has tended to be used to describe the aggressive end of

78. *Ibid.*
79. NCSC, 'Secure by Default', <www.ncsc.gov.uk/topics/secure-default>, accessed 21 January 2019.

defence or 'hacking back'.[80] However, our use of the term 'active' was simply to refer to a more active intervention by government and industry at a national level.

The ACD programme was discussed by ministers. It was clear that if it was to work, we needed to pre-empt any suggestion that we were constructing some sort of equivalent of the Great Firewall of China[81] for the UK or extending the reach of government. The key points in Levy's programme were that this must be technically transparent, delivered with and through industry, particularly the telecommunications companies and ISPs, and possible for anyone to opt out of. The last point was politically critical.

Another key to delivering the ACD experiment was to pilot the various elements on government departments first before reviewing and deciding whether to roll them out nationally.

Initial Results and Metrics

One year on from the launch of the ACD programme, the NCSC published a lengthy assessment paper by Ian Levy.[82] It is a model of the kind of open evaluation and detailed evidence which has been lacking in many government interventions on cyber security. Concluding that the ACD measures could be deployed at scale, Levy also presented this as 'a call to action for UK public sector organisations, UK industry and our international partners to implement these or similar measures so that collectively we make cyber crime less profitable and more risky globally'.[83]

The paper gave data on the outcomes for the various products and services offered to the UK private sector under four strands of the ACD:[84]

1. **Takedown Service** (**for malicious domains)**
   In 2017, the NCSC removed 18,067 unique phishing sites across 2,929 attack groups that pretended to be a UK government brand, reducing the median availability of a UK government-related phishing site from 42 hours to 10 hours. The NCSC also removed 121,479 unique phishing sites across 20,763 attack groups physically hosted in the UK. Internet statistics are notoriously elastic, and of course large numbers of takedowns need to be set against the relentless rise in phishing globally (up by an estimated 50% in the same year). But the key finding is that the share of phishing sites hosted in the UK reduced from 5.5% to 2.9% during the ACD programme's operation. This indicated

80. This spectrum is well described by Wyatt Hoffman and Ariel E Levite, 'Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?', Carnegie Endowment for International Peace, 2017, pp. 7–9.
81. Elizabeth C Economy, 'The Great Firewall of China', *The Guardian*, 29 June 2018.
82. Ian Levy, 'Active Cyber Defence – One Year On', NCSC, 5 February 2018, <www.ncsc.gov.uk/content/files/protected_files/article_files/ACD%20-%20one%20year%20on_0.pdf>, accessed 21 January 2019.
83. *Ibid.*, p. 1.
84. *Ibid.*, pp. 1–3.

that the objective of hardening the UK relative to other geographies was possible, although it also highlighted the importance of international cooperation to do this globally and at scale.

2. **DMARC**
   The study found that, while DMARC adoption by organisations took time and was sometimes complex, the results were encouraging where it had been deployed, giving back control to email domain owners and reducing spoofing. The number of messages spoofed from an @gov.uk address (for example, taxrefund@gov.uk) fell consistently during the first year, suggesting that criminal groups were tiring of them as increasingly fewer were delivered to end users. In one month some 30.3 million spoofed messages were not delivered to end users.

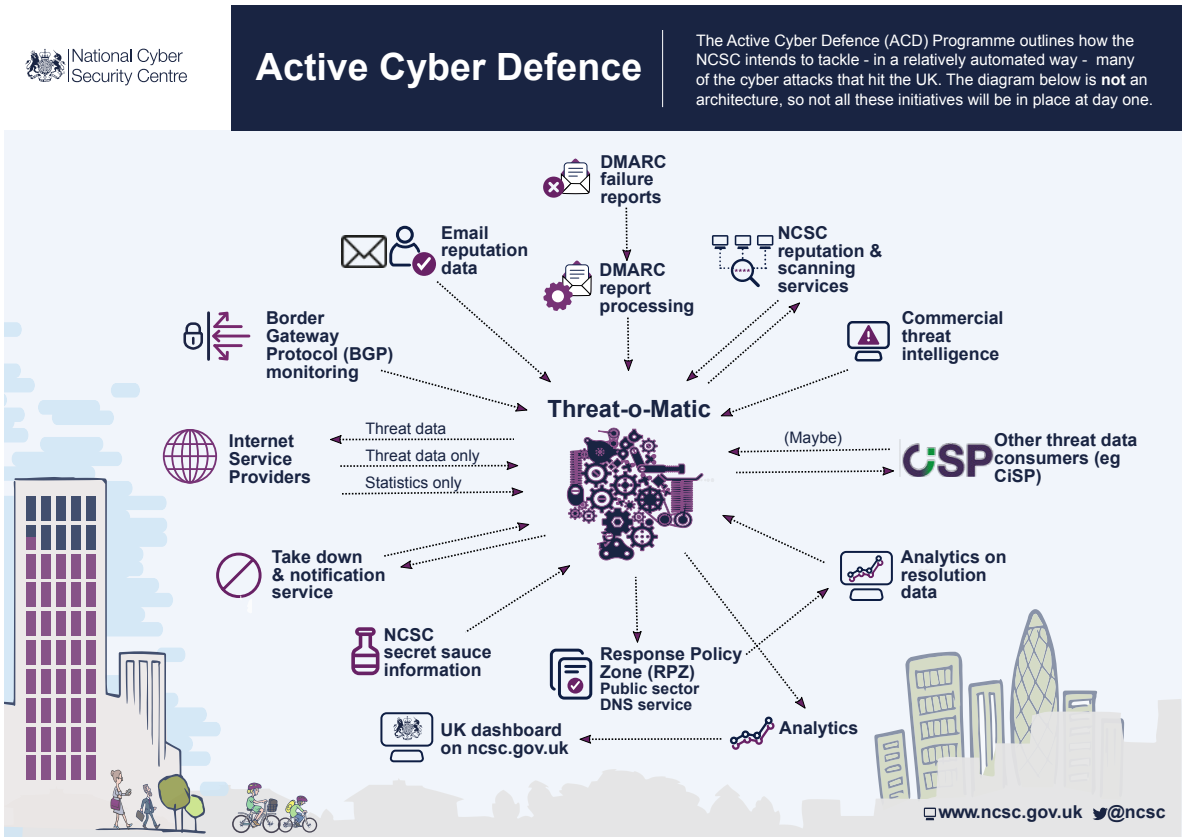
3. **Web Check**
   This fairly simple website-scanning service certainly appeared to have raised the baseline of security across a diverse range of government departments. The NCSC scanned 7,791 unique URLs across 6,910 unique domains, ingesting a total of 7,748 unique pages, and it produced 4,108 advisories for customers. Most of the issues were related to certificate management and out-of-date content management and server software.

4. **Public Sector DNS**
   Blocking of known bad domains was also productive. In December 2017, the public sector DNS service was responding to 1.23 billion requests a week. In a single week 273,329 requests were blocked, of which 5,768 were unique. In short, the metrics demonstrated clear cases where a malicious domain would have been accessed by a government user if ACD had not been in place.

5. **Signalling and Routing**
   Levy's paper also outlined progress in the longer-term experiments to put right 40 years of poorly secured infrastructure, in cooperation with industry, notably telecommunications providers. These are still in their early stages but hold out the possibility of making the malicious rerouting of traffic much more difficult, as well as reducing the options for launching large-scale DDoS attacks.

The ACD programme has been well received in technical circles, but it is unglamorous and not easy to describe for the wider public. It has, however, the potential to transform the threat landscape, particularly if adopted widely across international boundaries.

Figure 3: Active Cyber Defence



Source: National Cyber Security Centre, <www.ncsc.gov.uk>.

About the Author

Robert Hannigan is a Distinguished Fellow of RUSI. He is European Executive Chairman of BlueVoyant, the cyber security services company, and a Senior Adviser to McKinsey & Co.

He was director GCHQ, the UK's largest intelligence and security agency, from 2014 to 2017, and he was a member of the National Security Council.

Robert established the National Cyber Security Centre in 2016, having been responsible for the UK's first cyber strategy in 2009. He was also responsible for directing, with military colleagues, the National Offensive Cyber Programme. He is a leading authority on cyber security, cyber conflict and the application of technology in national security. He writes and speaks regularly on cyber issues.

Robert spent 20 years in UK government service, including as the Prime Minister's Security Adviser from 2007 to 2010. He was responsible in the Cabinet Office for the Single Intelligence Account (covering MI5, GCHQ and SIS/MI6), chaired COBR meetings through numerous crises and was a longstanding member of the Joint Intelligence Committee, which he chaired in 2011–12. He came to London from Belfast, where he was Tony Blair's senior official on the Northern Ireland peace process, responsible for negotiations with political parties, paramilitaries and with the Irish and US governments.

Robert caused international controversy as director GCHQ in 2014 by criticising Silicon Valley companies in the *Financial Times*, but he has also spoken at MIT in defence of strong encryption and US technology leadership. He has a particular interest in Bletchley Park, where he is a Trustee, and in the history of technology, computing and cryptology. He was a member of the UK government's Defence Innovation Advisory Panel.

He is a Senior Fellow at Harvard University's Belfer Center, a Fellow of the Institute of Engineering and Technology, and Honorary Fellow of Wadham College, Oxford. He is one of the few non-US nationals to have been awarded the US Intelligence Distinguished Public Service Medal.