THE POLICY INSTITUTE

CYBER SECURITY RESEARCH GROUP

KING'S College LONDON

UK Active Cyber Defence

A public good for the private sector

Tim Stevens, Kevin O'Brien, Richard Overill, Benedict Wilkinson, Tomass Pildegovičs, Steve Hill

January 2019

Key findings

The UK's Active Cyber Defence (ACD) programme has been a key aspect of the work of the National Cyber Security Centre (NCSC) in improving public-sector cybersecurity since late 2016. According to the NCSC, it has, through a range of ACD measures, objectively reduced the threat of cybercrime to government agencies and service users. On the basis of this success, NCSC has begun to promote ACD as a means of countering low-level cybercriminality and its effects on individuals, businesses, charities and other organisations beyond the public sector. It aims thereby to deliver on the core aspirations of the *National Cyber Security Strategy 2016-2021*, specifically its commitment to defending UK assets and interests in cyberspace.

This report explores the implications of scaling up ACD to the national level and expanding it beyond the public sector. Based on our analysis, we find the following:

1. Active Cyber Defence has significant potential in helping improve UK national cybersecurity.

Initial indications are that ACD has helped reduce the incidence and effects of low-level cybercrime on government agencies and service users. There are no significant technical obstacles to extending these protections beyond the public sector and no fundamental reasons why ACD tools and techniques should not be tested and deployed as appropriate. Indeed, individual firms and trade bodies are already engaged in developing capabilities and best practice frameworks that build on ACD knowledge and experience. We propose that firms and other stakeholders engage more actively with government through the NCSC in order to develop further how ACD might be deployed throughout UK networks as a means of countering cybercrime in the UK. These relationships are essential, as the NCSC's role is primarily advisory, helping organisations deploy ACD, rather than providing the technology itself.

> "... firms and other stakeholders [should] engage more actively with government through the NCSC in order to develop further how ACD might be deployed throughout UK networks as a means of countering cybercrime in the UK."

2. Active Cyber Defence can play a powerful role in shaping the cybersecurity marketplace and furthering the interests of UK internet users and consumers.

ACD looks to incentivise internet service providers and others by demonstrating its worth and utility to consumers. If ACD can be shown to protect end-users of government, commercial and other services from many of the negative impacts of cybercrime, consumers may in time seek out those organisations that provide ACD by default and move away from those that do not. If public trust in a firm or charity derives in part from good cybersecurity, organisations that adopt ACD as a way of improving cybersecurity will benefit; those that do not will suffer. There will need to be careful calibration of 'sticks and carrots' to encourage industry and others to adopt ACD where possible but the existing buy-in of major companies and industry bodies will assist greatly in this process. NCSC has no legal power to mandate ACD in any circumstance, nor does it seek it, so all progress in this area must be based on high standards of transparency, partnership and public reporting, particularly given NCSC's status as part of GCHQ.

3. Active Cyber Defence is a potentially useful model for export to like-minded countries.

The UK's understanding of active cyber defence differs from other countries' more offensive-minded interpretations of the term. ACD is purely defensive in the UK context and does not hint at 'hacking back' or other actions that risk escalation or retaliation. The UK has these capabilities but these are not part of ACD. In this respect, ACD may be promoted abroad as a suite of peaceable defensive measures that have appreciable effects on the impact and incidence of cybercrime. If the UK can show real gains in this area, it will help other countries to do similarly, thereby marginalising cybercrime in geographical terms and, in the long term, help to deter it. Moreover, UK expertise and technologies can be leveraged to promote UK national interests abroad, including by the development of industrial partnerships and networks of trust that bring about positive international cybersecurity outcomes.

4. Active Cyber Defence may constitute an emergent 'public good'.

Public goods are ordinarily provided by governments or civil authorities and refer to goods or services that are provided to all and the use of which by one person does not diminish its availability to another. A common example is national security. Public goods are rarely perfect – national security included – but can offer benefits at low direct cost to individuals and to as many people as possible within a given jurisdiction. If ACD can operate quietly, effectively and does not pass on significant costs to users, it may be understood as a possible public good. This is a provisional assessment and we recommend that government explores the wider potential of cybersecurity to be framed and developed as a public good, particularly as we enter the lead-in phase for the next national cybersecurity strategy, due in 2021. In this respect, ACD offers an interesting case study of how public goods might be developed in partnership between the public and private sectors.

> "ACD offers an interesting case study of how public goods might be developed in partnership between the public and private sectors."

5. Active Cyber Defence is not perfect, nor should we expect it to be.

ACD is not a finished product but a work in progress. Nor is it a single entity, amenable to simple, one-off deployment. It has many moving parts, some of which are more developed than others, and future developments will require adaptation, agility and responsiveness to changing sociopolitical and technological contexts. Its stakeholders will need patience, partnership and no small degree of self-reflection when expanding the ACD ecosystem. Like all forms of security it is unlikely ever to be perfect and we should be wary of attempting to make it so. However, we assess that ACD is a cost-effective and promising addition to UK national cybersecurity and merits further support and attention. If implemented carefully but robustly it should do much to tackle cybercrime and cyber threats to UK networks and help promote national prosperity and wellbeing.

1. Introduction: UK government and the cybersecurity challenge

In the quarter-century since the creation of the World Wide Web, the internet has become a primary means of global communication for half the world's inhabitants.[1] It underpins commerce, drives economic growth, fosters myriad communities of diverse identities and interests, and facilitates political activism of many stripes.

Yet, as is becoming increasingly apparent, the internet also allows for the expression of darker motives, associated with war, crime, subversion, terrorism and propaganda. In a few short years, cybersecurity – the pursuit of security in and through 'cyberspace' as the whole of today's digital environment – has risen to the top of national and international security agendas, as well as changing notions of public and personal safety. It is only a matter of time, asserts the chief executive officer of the National Cyber Security Centre (NCSC), before a cyber attack leads to significant disruption to essential services or national security, intersecting with the physical world and leading perhaps even to loss of life.[2]

While we often focus on these high-level incidents, which the UK has been fortunate so far to avoid and skilled enough to counter, arguably the greater everyday threat is cybercrime, which is rife and endemic. Organised crime groups and chancers alike are using the internet to generate profits by deceiving and defrauding individuals and companies. The harms generated by cybercrime are significant. It diverts funds from legitimate businesses and the government tax base. Cybercriminality causes personal distress to consumers and reputational harm to firms.

> "Official figures suggest that a UK resident is more likely to be a victim of cybercrime or fraud than any other offence."

In the UK, over four in 10 businesses and one-fifth of charities were subject to a cybersecurity breach or attack in 2017-18.[3] Official figures suggest that a UK resident is more likely to be a victim of cybercrime or fraud than any other offence.[4] Moreover, perhaps on account of the UK's relative wealth, its population is more than twice as likely to be targeted by cybercriminals compared to the global average, and each crime is more than twice as lucrative as the global average. One estimate suggests that £4.6 billion was stolen from 17 million UK internet users in 2017.[5]

Government has an obvious responsibility for protecting its own networks and people – the public sector – but a central problem persists in considering what its proper role should be in delivering cybersecurity to the private sector and civil society. In common with most countries, private companies own and operate the preponderance of infrastructure, all of which at some level relies on the internet. At the same time, citizens rely increasingly on internet platforms and services to manage their daily lives.

1 https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

2 E. MacAskill, 'Major cyber-attack on UK a matter of "when, not if" – security chief', *The Guardian*, 23 January 2018. https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin

3 Department for Digital, Culture, Media and Sport, Ipsos MORI Social Research Institute, and the University of Portsmouth, *Cyber Security Breaches Survey 2018*, 25 April 2018. https://www.ipsos.com/ipsos-mori/en-uk/cyber-security-breaches-survey-2018

4 Office for National Statistics, 'Crime in England and Wales: year ending June 2018'. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2018

5 A. Hern, 'Cybercrime: £130bn stolen from consumers in 2017, report says', *The Guardian*, 23 January 2018. https://www.theguardian.com/technology/2018/jan/23/cybercrime-130bn-stolen-consumers-2017-report-victims-phishing-ransomware-online-hacking

This report argues that the UK government has a crucial part to play in both public- and private-sector cybersecurity, not least as both sectors are so deeply interdependent. Our case study for illustrating aspects of this dynamic is the UK's government-funded Active Cyber Defence (ACD) programme, first deployed in 2016. Its principal goal has been to prevent cybercriminals from leveraging government networks and brands to defraud and deceive users of government services. Fortunately, most cybercriminality is relatively unsophisticated and careful use of available technologies can do much to reduce its volume and effect. ACD offers this suite of capabilities. Deployed and tested initially across the public sector, its tools and techniques are now being promoted for use beyond government networks to improve cybersecurity across the private sector and civil society. This raises questions about government intervention in the private sector and elsewhere, particularly as ACD was set up and is overseen by the NCSC, part of the UK's signals intelligence agency, GCHQ.

This report suggests that the ACD programme holds great potential to reduce the incidence and impact of cybercrime in the UK and, if adopted in other national contexts, can help counter the global proliferation of cybercrime. While broadly supportive of ACD, this report raises a range of considerations for the programme as it moves ahead. These include how to incentivise the private sector; resisting various forms of function and mission creep; issues around exporting ACD technologies; the possible negative externalities of ACD in adjacent fields of security and policing; and how ACD can deal with rapid technological change. We propose that ACD, if deployed carefully and sensitively, might be understood as an emergent 'public good', delivering significant socioeconomic benefits.

Background to the report

This report is based on a research project undertaken in 2018 by the King's College London Cyber Security Research Group (CSRG), affiliated with the King's Academic Centre of Excellence in Cyber Security Research (ACE-CSR). It is funded by the Economic and Social Research Council's Impact Acceleration Account, administered by the Policy Institute at King's College London. The aim is to produce an independent evaluation of the Active Cyber Defence programme, particularly in respect of its proposed expansion beyond the public sector. It addresses issues of technical feasibility, law, politics, policy, national strategy and industrial strategy, and is intended to help inform the UK government's continuing development of the ACD programme. We were assisted in this process by meetings with NCSC Technical Director Dr Ian Levy and colleagues at the NCSC in London.

Structure

The remainder of this report falls into six sections. Section 2 situates the Active Cyber Defence programme within the UK policy, institutional and legal context concerning cybersecurity. Section 3 looks in greater detail at the aims and components of the ACD ecosystem. Section 4 explores aspects of its proposed expansion and Section 5 presents a series of thematic issues for further consideration. In the final section, we propose that Active Cyber Defence can be framed as a public good and offer some reflections and recommendations based on our research and engagements.

2. Active Cyber Defence in context

In the United Kingdom, the threat of cyber attacks to social, economic and national wellbeing is a top-level concern for policy and strategy. The *National Security Strategy* (2015) recognises that the UK is 'vulnerable to attacks on parts of our networks that are essential for the day-to-day running of the country and our economy'.[6] The task of government and its partners, therefore, is to ensure sufficient levels of cybersecurity to defend and deter a range of high-level threats to these critical national infrastructures, and to reduce risks to them and to other systems that rely upon them. At the same time, cybersecurity must also deal with the nuisances of lower-level cybercrime, such as online fraud and deception leading to individual and corporate loss and distress.

The principal government guidance for UK cybersecurity is provided by the *National Cyber Security Strategy 2016-2021* (*NCSS 2016*), published in November 2016.[7] It sets out in some detail the government's approach to cybersecurity, aiming to ensure that by 2021, 'the UK is secure and resilient to cyber threats, prosperous and confident in the digital world'.[8] This ambition aligns with and articulates a specific element of the 2015 *National Security Strategy*, which announced the investment of £1.9 billion in the National Cyber Security Programme (NCSP) as a means to promote the development of UK cybersecurity skills, knowledge and capabilities.[9]

NCSS 2016 identified three organising principles – Defend, Deter and Develop – which, while mutually reinforcing, provide structure and coherence to the complex undertaking that is national cybersecurity. The 'Defend' strand promotes effective defence against an evolving panoply of cyber threats, robust incident response, and operational and individual resilience. 'Deter' aims to detect, understand and counter hostile cyber operations, including through the use of offensive cyber capabilities. The 'Develop' pillar supports cybersecurity research and development, business innovation, and educational and training programmes to meet public and private sector skills requirements. All three are supported by 'International Action', which is rather underdeveloped in its specifics, but outlines the UK's commitment to the peaceful pursuit of its national interests and to multilateral cooperation in the rules-based international order.

NCSS 2016 does not operate in isolation. It is augmented and supported by a growing number of policy papers, guidance notes, consultations and research reports, issued by the many government departments with sectoral cybersecurity responsibilities and risk ownership.[10] There has been a marked uptick in government policy and guidance

6 HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161, London, The Stationery Office, November 2015. https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

7 HM Government, *National Cyber Security Strategy 2016-2021*, London, Cabinet Office and HM Treasury, November 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. This supersedes earlier cybersecurity strategies, published in 2009 and 2011, neither of which referenced ACD and only spoke tangentially about developing more 'proactive means' to counter cyber-threats. See, for example, the 2011 Strategy at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

8 HM Government, *National Cyber Security Strategy*, p. 9.

9 HM Government, *National Security Strategy*, pp. 40-42.

10 Key departments include: Ministry of Defence; Foreign and Commonwealth Office; Home Office; Department for Digital, Culture, Media and Sport; Department for Business, Energy and Industrial Strategy.

since the release of the *NCSS* in late 2016, which aligns well with government's stated commitment to deepening and strengthening cybersecurity across the public and private sectors.

The Cabinet Office, through the Cyber and Government Security Directorate and the National Security Secretariat, has a formal coordinating function for cross-government cybersecurity and policy delivery.[11] Much of the everyday activity in this field, however, involves one of the key organisations formally established in *NCSS 2016*. The National Cyber Security Centre (NCSC) in London began operating in October 2016 and was formally opened in February 2017.[12] NCSC is part of Government Communications Headquarters (GCHQ), the UK's sovereign signals intelligence (SIGINT) and information assurance agency.[13] It also works closely with – in many ways overlaps with – the National Crime Agency (NCA), the UK's national law enforcement body, with its responsibility for countering and investigating online and digital crimes. The formation of the NCSC brought together under one roof the pre-existing Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT-UK), and the Communications-Electronics Security Group (CESG), a GCHQ body and national technical authority for information assurance (IA). It also took on responsibility for the cybersecurity of critical national infrastructures, previously the remit of the Centre for the Protection of National Infrastructure (CPNI), a process which is nearly complete.

This institutional reorganisation provides government agencies and departments, firms large and small, and citizens, with a single point of contact for cybersecurity expertise and guidance. NCSC works across multiple sectors and with international defence, intelligence and security partners to, in line with *NCSS 2016*, make 'the UK one of the safest places in the world to live and do business online'.[14] It has adopted a notably public-facing posture and a commitment to transparency whenever possible. This model has been described by its chief executive officer, Ciaran Martin, as essential to NCSC's intention 'to turn the secret into something useable in the open'.[15] Similar initiatives have been launched over the last several years in Australia, Canada, The Netherlands, and Estonia, and are being discussed in Sweden, Germany, and other countries as a more concerted effort to develop single national approaches to both cyber-defence and public-private cooperation on cybersecurity.

---

11 HM Government, *Intelligence and Security Committee Annual Report 2016-17: Further Government Response*, Cm. 9678, July 2018, p. 6. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727951/CCS001_CCS0718140448-001_ISC_supplementary_16-17_AR_response_Web_Accessi..._1_.pdf. At present, however, no single minister is responsible for cybersecurity; Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure*, Third report of session 2017-19, HL Paper 222 HC 1708, 19 November 2018, ss. 75-81. https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170802.htm

12 National Cyber Security Centre, *The Launch of the National Cyber Security Centre*, London, National Cyber Security Centre, February 2017. https://www.ncsc.gov.uk/news/launch-national-cyber-security-centre; see also, HM Government, *Prospectus: Introducing the National Cyber Security Centre*, London, Cabinet Office, GCHQ and CESG, May 2016. https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus

13 Signals intelligence (SIGINT) is conventionally understood as 'the interception of the communications of others (states, armies, companies, etc.)'; P. Gill and M. Phythian, *Intelligence in an Insecure World*, third edn., Cambridge, Polity Press, 2018, p. 53.

14 https://www.ncsc.gov.uk/information/about-ncsc

15 C. Martin, 'Ciaran Martin's cyber security summit speech', 23 October 2017. https://www.ncsc.gov.uk/news/ciaran-martins-cyber-security-summit-speech

In the same speech, Martin noted that NCSC's position as part of GCHQ, 'gives us reach into the sort of highly valuable and classified data and capabilities that only we, under a very strict and proportionate legal framework, can have.'[16] This is an important consideration. Historically, GCHQ and any subsidiary organisations have had two statutory functions. Under the *Intelligence Services Act 1994*, GCHQ may, for the purposes of national security, national economic wellbeing, and the prevention or detection of serious crime, monitor, interfere with, or obtain information from electronic equipment as part of its signals intelligence remit.[17] Under the same Act, GCHQ may also provide advice on information security and assurance to other government departments and agencies.[18]

These provisions were amended by the *Investigatory Powers Act 2016* to allow GCHQ to 'make use of' intercepted material and to advise a wider range of parties, including unspecified organisations and the general public.[19] This allows GCHQ to provide cybersecurity and other advice to business and individuals, principally through NCSC, and for this to be informed by secret intelligence if necessary. As NCSC notes, 'our guidance is advisory in nature and is underpinned by our unique insights into cyber threats.'[20] Neither GCHQ or NCSC has the power to mandate specific courses of action, which must instead come from the Cabinet Secretary. This situates political responsibility and liability for standards and policy with the government, not with GCHQ.

One the most eye-catching cybersecurity initiatives announced in *NCSS 2016* was Active Cyber Defence (ACD). Variously referred to as a 'principle', 'programme' or 'action plan', ACD draws on established practices across industry, which see 'cyber security analysts developing an understanding of the threats to their networks, and then devising and implementing measures *to proactively combat, or defend, against these threats*.'[21] In some contexts, this approach has been interpreted as allowing aggressive retaliation, including punitive countermeasures, by both governments and businesses against their perceived attacker.[22] The debate over the permissibility and utility of these forms of 'hack back' is much debated in the United States (and other Western countries) at present, and has been the subject of Congressional consideration.[23] It is generally advised against in the strongest terms due to, among other issues: difficulties in attributing cyber attacks and therefore reacting against the correct party; firms' lack of ability to control escalation if the situation worsened; uncertainty about the legal basis of these actions in most countries; and the weak,

16 Martin, 'Ciaran Martin's cyber security summit speech'.
17 *Intelligence Services Act 1994* (c13), ss. 3(1)(*a*) and 3(2).
18 *Intelligence Services Act 1994*, s. 3(1)(*b*).
19 *Investigatory Powers Act 2016* (c25), ss. 251(2)(*a*) and (*b*).
20 https://www.ncsc.gov.uk/guidance. See also JCNSS, fn. 108.
21 HM Government, *National Cyber Security Strategy*, p. 33, emphasis added.
22 See, for example, S. Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option*, Lanham, MD, Rowman and Littlefield, 2017, pp. 165-190; R.S. Dewar, 'The "triptych of cyber security": a classification of active cyber defence', in P. Brangetto, M. Maybaum and J. Stinissen (eds.), *2014 6th International Conference on Cyber Conflict: Proceedings*, Tallinn, NATO CCD COE Publications, 2014, pp. 7-21.
23 J. Thomsen, 'Pentagon cyber official warns US companies against "hacking back"', *The Hill*, 13 November 2018. https://thehill.com/policy/cybersecurity/416494-defense-cyber-official-warns-private-companies-against-hacking-back; *Active Cyber Defense Certainty (ACDC) Act of 2017*, HR 4036, 115th Congress (2017).

if any, co-ordination a business would have with its national government and law enforcement in undertaking such an action.

The official UK ACD posture, however, is framed as purely defensive, and 'is not intended to imply retaliation ("hack back") by victims or militarisation of the internet'.[24] The UK possesses, and has indicated its willingness to use, 'offensive' cyber capabilities, including through the joint GCHQ/Ministry of Defence National Offensive Cyber Programme (NOCP), which is developing 'a dedicated ability to counter-attack in cyberspace'.[25] This is justified in part as a means to bolster deterrence, but these activities are distinct from and form no part of the ACD programme.[26] The following section describes in more detail the precise aims and components of ACD.

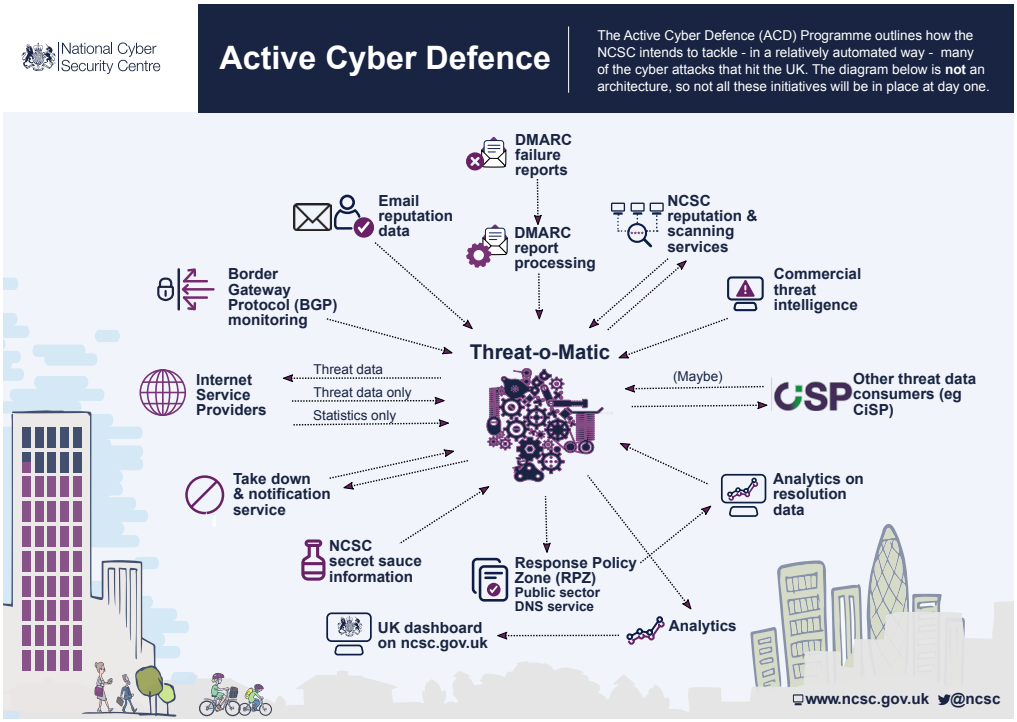
24 I. Levy, *Active Cyber Defence – One Year On*, London, National Cyber Security Centre, 5 February 2018. https://www.ncsc.gov.uk/information/active-cyber-defence-one-year

25 Intelligence and Security Committee of Parliament, *Annual Report 2016-2017*, HC 655, 20 December 2017, ss. 107-113; HM Government, *National Cyber Security Strategy*, p. 51;

26 The UK government recognises the role of cybersecurity in deterrence by punishment and by denial; HM Government, *National Security Strategy*, pp. 23-24; see also, House of Commons Defence Committee, *Deterrence in the Twenty-First Century*, Eleventh report of session 2013-14, vol. 1, HC 1066, 27 March 2014, ss. 20-21. https://publications.parliament.uk/pa/cm201314/cmselect/cmdfence/1066/106602.htm

3. Active Cyber Defence: aims and components

FIGURE 1: ACD ECOSYSTEM [CROWN COPYRIGHT]



The overall aim of the ACD programme is to help deliver the 'Defend' strand of *NCSS 2016*: 'to ensure that UK networks, data and systems in the public, commercial and private spheres are resilient to and protected from cyber attack.'[27] This approach correctly recognises that it is impossible to deter every malicious cyber actor, whether state, criminal, terrorist, or any other committed group or individual. The requirement therefore arises to improve cyber defences such that they 'will significantly reduce our exposure to cyber incidents, protect our most precious assets, and allow us all to operate successfully and prosperously in cyberspace.'[28] Defensive measures intend to increase the resilience of UK networks in order to make them less attractive targets for state-sponsored cyber actors and criminals.

> "Active Cyber Defence intends to protect the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time."

Active Cyber Defence is a key contribution to this endeavour. Its core motivation is 'to tackle, in a relatively automated way, a significant proportion of the cyber attacks that hit the UK.'[29] Its unique contribution is in taking a proactive approach to improving cybersecurity outcomes, using relatively automated processes that scale well in timely and efficient fashion to protect UK networks, users and interests. Active Cyber Defence intends, therefore, 'to protect the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time.'[30]

To do this, it tackles the problem of 'commodity attacks', understood as the high volume of relatively unsophisticated malicious software (malware) that afflicts

27 HM Government, *National Cyber Security Strategy*, p. 33.
28 HM Government, *National Cyber Security Strategy*, p. 33.
29 I. Levy, 'Active Cyber Defence – tackling cyber attacks on the UK', blog post, 1 November 2016. https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk
30 Levy, *Active Cyber Defence*, p. 1.

networks, systems and users on a daily basis, as well as multiple forms of credential theft, account hijacking, and so on.[31] It is not set up to deal with 'high-end' actors, political or criminal, that develop and deploy much more sophisticated and targeted operations against UK assets. This responsibility lies elsewhere in NCSC, which works with its intelligence, military and policing partners on tailored operations to counter these high-level threats.

This is an important distinction. Each major threat actor, such as foreign intelligence services and state-backed proxies, demands a specific and distinct response. These operations require bespoke operations and capabilities that command significant investments of time, labour and expense. In contrast, much of the business of countering commodity attacks is generic and can be automated, as indeed are many of the attacks themselves. This conceptual division allows for appropriate allocation of resources and in the long run, as NCSC hopes, it will 'reduce the noise enough to make the defenders' jobs easier when tackling those very targeted attacks.'[32]

Most commodity attacks are perpetrated using tools and techniques readily available online and well known to network defenders.[33] In addition, they are often not targeted at particular companies or individuals, but released 'into the wild' to hit as many potential targets as possible. For example, phishing, in which criminals try to obtain sensitive personal details via superficially trustworthy emails, works by sending email to as many people as possible. If even a small percentage of those who receive the email are duped, a substantial return on investment can be generated. Foreign governments also use phishing in a much more targeted manner in an attempt to gain access to specific individuals' information and assets.

ACD automates responses to many different types of commodity attacks, including phishing, but the ACD 'ecosystem' also includes a range of other operations (see Figure 1).[34] The following provides a snapshot of its four main activities, all of which have initially been deployed across the public sector only:

- **Takedown Service.** Asks hosting providers to remove websites and content impersonating the UK government and others, e.g. fake HMRC websites.

- **Mail Check.** Makes it harder for criminals to distribute emails that look like they come from a trusted source, such as a government agency.[35]

- **Web Check.** Helps government website owners check for common security issues.

---

31 Malware is software designed to disrupt, damage or gain unauthorised access to a computer system.

32 Levy, 'Active Cyber Defence – tackling cyber attacks'.

33 See National Cyber Security Centre, *Common Cyber Attacks: Reducing the Impact*, white paper, January 2016. https://www.ncsc.gov.uk/file/common-cyber-attacks-reducing-impact; National Cyber Security Centre, *Joint Report on Publicly Available Hacking Tools*, 11 October 2018. https://www.ncsc.gov.uk/joint-report

34 See, Levy, *Active Cyber Defence*; Levy, 'Active Cyber Defence – tackling cyber attacks'; C. Martin, 'Active cyber defence for the UK', *Civil Service Quarterly*, 30 January 2018. https://quarterly.blog.gov.uk/2018/01/30/active-cyber-defence-for-the-uk/; National Cyber Security Centre, *Annual Review 2018*, 16 October 2018, pp. 14-16. https://www.ncsc.gov.uk/news/annual-review-2018. The technical aspects of these ACD components are set out in Levy, *Active Cyber Defence*.

35 This project relies in part on implementation of the DMARC (Domain-based Message Authentication, Reporting and Conformance) protocol, https://dmarc.org/. DMARC enables tighter controls over the malicious abuse of email addresses.

- **Protective Domain Name System (DNS).** Blocks government users' access to bad websites, such as those known to distribute malware.

ACD includes a range of other initiatives, including protocol monitoring. This component aims to improve how internet and telecommunications protocols handle internet traffic, so as to make it more difficult to hijack UK assets and use them in, for example, distributed denial-of-service attacks.[36] This applies across the public and private sectors by dint of the common protocols used.

In its first annual report on ACD, published in February 2018, NCSC reported that 'people in the UK are objectively safer in cyberspace because of the ACD programme.'[37] In October 2018, further figures were released to bolster these claims.[38] For example, the Takedown Service more than halved the UK's share of global phishing attacks to 2.4 per cent, with nearly 140,000 UK-hosted phishing sites being removed, plus more than 14,000 impersonating the UK government. Protective DNS blocked an average of nearly 11,000 malicious domains every month, making these unavailable to government web users. Web Check identified over 2,300 urgent issues across the government's digital estate, allowing them to be fixed. The figures also showed that uptake of these services across government had increased significantly.[39]

Five interlocking principles underpin the ACD approach to UK cybersecurity.

> "... government will not ask anyone to implement cybersecurity solutions that it has not tested on itself."

The first is that ACD in its initial iteration has only been used to protect the public sector. NCSC has described this as an 'eat your own dog food' attitude, 'using government as a guinea pig'.[40] The presumption here is that government will not ask anyone to implement cybersecurity solutions that it has not tested on itself. Too often, governments are seen mainly as sources of cybersecurity regulation and guidance, without a complementary commitment to putting their own advice into action in the public sector. If the UK government can demonstrate that it is developing and implementing innovative technologies and best practice in this field, it is contributing visibly to the emergence of a powerful norm around the need for, and practicalities of, organisational cybersecurity. This may in time incentivise other actors to follow its lead.

The second principle is automation. NCSC and its partners are working towards automating as much of the day-to-day operation of ACD components as possible. This applies to the forms of technical monitoring and filtering required of ACD but also to the generation of threat intelligence and reporting mechanisms to government and other partners. While still in development, the central platform for collating and distributing relevant data around the ACD ecosystem – the 'Threat-o-Matic' – is

36 A protocol in this context is a set of rules governing how data is sent across the internet or a telecommunications network. The relevant protocols here are the Border Gateway Protocol (BGP) and Signaling System 7 (SS7). A distributed denial-of-service (DDoS) attack typically works by flooding a target system with connection requests from multiple hijacked sources, thereby overloading the target system or otherwise preventing legitimate requests from being answered.
37 I. Levy, 'Active Cyber Defence – one year on', blog post, 5 February 2018. https://www.ncsc.gov.uk/blog-post/active-cyber-defence-one-year
38 NCSC, *Annual Review 2018*, pp. 14-16.
39 For example, National Cyber Security Centre, 'Helping secure public sector email with Mail Check', 29 October 2018. https://www.ncsc.gov.uk/blog-post/helping-secure-public-sector-email-mail-check
40 Levy, *Active Cyber Defence*, p. 64.

designed to automate communications and technical decision-making among ACD elements.[41] This includes automating aspects of the public-sector DNS service, for example, in which internet service providers are alerted automatically to the presence of a bad domain and decide automatically to block it. This removes a layer of human interaction and potentially improves the ability to provide timely and effective protection from threats. It also shifts a certain amount of responsibility for cybersecurity from individual users to the owners and operators of internet infrastructure. All users continue to be encouraged to improve security behaviours but some decisions – for example, determining which email attachments are fake or which hyperlinks are genuine – no longer fall to them but to automated ACD processes instead. This represents an important move away from a 'blame the victim' mindset endemic to cybersecurity.[42]

ACD channels a third principle, set out in *NCSS 2016*. In an unusual act of self-reflection, the UK government recognised that its 2011 national cybersecurity strategy had not achieved as much as it had hoped to by looking principally to the market for cybersecurity solutions to achieve many of its goals.[43] Moreover, it outlined a specific intention 'to intervene more directly' in order to raise UK cybersecurity standards, particularly with respect to critical national infrastructures.[44] Paraphrased memorably by NCSC, the 'active' part of ACD 'means getting off our backside and doing something'.[45] ACD emphasises that cybersecurity cannot be left to the market alone and serves to remind business that the UK government is not averse to taking decisive action if the market cannot deliver adequate cybersecurity solutions.

The fourth principle concerns transparency in reporting. This is built into the ACD project and into the raison d'être of the NCSC itself. The Chancellor of the Exchequer's foreword to *NCSS 2016* called the strategy 'an unprecedented exercise in transparency', noting that '[w]e can no longer afford to have this discussion behind closed doors.'[46] The traditional secrecy of SIGINT organisations, which often have crucial roles in national cybersecurity, has sometimes hindered effective pursuit of cybersecurity. This has been most often in respect of the level and sensitivity of threat intelligence they have been able to share more widely among stakeholders in government and the private sector. The NCSC has committed to transparency from its inception, an orientation that reflects the revised legal framework in which it is embedded; that is, its public advice function demands transparency wherever possible, in order to drive up cybersecurity awareness and quality. With respect to ACD, NCSC published a full and unredacted annual report in February 2018 and is due to do so again in early 2019. As a new programme established for the first time under *NCSS 2016*, it has not yet been assessed by the National Audit Office (which

41 The Threat-o-Matic is described in more detail in Levy, *Active Cyber Defence*, pp. 61-63, which also notes that the 'cartoonish name is deliberate – it's part of demystifying cyber security and being honest about what we're doing' (p. 61).
42 See, B. Schneier, 'Stop trying to fix the user', *IEEE Security and Privacy*, 14, 5 (2016), p. 96.
43 HM Government, *National Cyber Security Strategy*, p. 13.
44 HM Government, *National Cyber Security Strategy*, pp. 13, 41. Critical national infrastructure (CNI) are those parts of infrastructure whose loss or compromise could cause significant impacts on essential services, perhaps leading to loss of life, and on national security or the functioning of the state. For a full formal definition, see https://www.cpni.gov.uk/critical-national-infrastructure-0
45 Levy, *Active Cyber Defence*, p. 8.
46 HM Government, *National Cyber Security Strategy*, p. 6.

has assessed other parts of the *National Cyber Security Strategy* back to 2011).[47] Coupled tightly with the need for pragmatic transparency is the stated principle of evidence-based decision-making. Again, this is consistent with *NCSS 2016*, which outlines an evidence-based approach to cyber policymaking and the importance of measuring progress in multiple fields of cybersecurity.[48] It also assists NCSC's internal learning processes by opening up ACD to 'scrutiny and challenge', particularly from internet service providers (ISPs) and critical infrastructure owner-operators.[49]

A fifth identifiable principle is that of partnership. Many of the ACD elements have been developed and implemented with organisations outside the public sector. The Takedown Service, for example, has benefited from the input of Netcraft, an internet services company based in the west of England. Protective DNS would not be possible without the cooperation of Nominet, which runs the UK's DNS service. Other aspects of ACD, such as protocol monitoring, have been developed in partnership with BT, which, in a world first for a telecommunications provider, has begun sharing threat intelligence with other ISPs.[50] NCSC provides data to a range of other partners, and also receives threat intelligence feeds from private vendors, each of which helps to improve threat awareness and remediation in the public and private sectors. The determination to work with entities outside government extends also to international partners. NCSC has, for instance, suggested that other governments might 'consider the effects of the initial ACD programme and whether they could implement similar services'.[51] The details of these interactions are classified but it is interesting to note that the US Department of Homeland Security is mandating federal agencies' use of the DMARC protocol, which commentators have noted is very similar to how the UK has implemented DMARC as part of the ACD Mail Check service.[52] NCSC has hosted delegates from 54 countries and we should assume that ACD has been discussed in many of these meetings.[53]

Our research indicates that the ACD programme is based on sound principles and has delivered genuine benefits to the UK public sector and its users. NCSC's willingness

47 See, for example, National Audit Office, *The UK Cyber Security Strategy: Landscape Review*, 12 February 2013. https://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/; National Audit Office, *Update on the National Cyber Security Programme*, 10 September 2014. https://www.nao.org.uk/report/update-on-the-national-cyber-security-programme/#

48 HM Government, National Cyber Security Strategy, pp. 61, 67-69. Formal auditing of government cybersecurity is the responsibility of the National Audit Office. See, for example, National Audit Office, *Cyber Security and Information Risk Guidance for Audit Committees*, September 2017. https://www.nao.org.uk/report/cyber-security-and-information-risk-guidance/

49 Levy, *Active Cyber Defence*, p. 1.

50 The Malware Information Sharing Platform (MISP) combines NCSC and other partners' data with BT's own to provide a comprehensive overview of the threat landscape to ISPs, NCSC and law enforcement agencies, including INTERPOL; BT, 'BT steps up battle against cyber-crime by sharing malware data with ISPs', press release, 6 February 2018. https://www.globalservices.bt.com/en/aboutus/news-press/bt-steps-up-battle-against-cyber-crime

51 Levy, *Active Cyber Defence*, p. 68.

52 For example, T. Seals, 'DHS mandates DMARC, HTTPS for all US federal agencies', *InfoSecurity*, 17 October 2017. https://www.infosecurity-magazine.com/news/dhs-mandates-dmarc-https/. By the same token, US observers might note superficial similarities between ACD and the US Department of Homeland Security's EINSTEIN system, https://www.dhs.gov/einstein

53 NCSC, *Annual Review 2018*, p. 17. This aspect of NCSC's activities should be better substantiated; see, JCNSS, *Cyber Security*, s. 21. See also, C. Franklin, Jr., 'Leaderboard shows adoption of DMARC email security protocol', *Dark Reading*, 20 November 2018. https://www.darkreading.com/application-security/leaderboard-shows-adoption-of-dmarc-email-security-protocol/d/d-id/1333311?_mc=NL_DR_EDT_DR_daily_20181121&cid=NL_DR_EDT_DR_daily_20181121&elq_mid=87901&elq_cid=27767302

to publish data and honest appraisals of ACD successes and failures is commendable and allows external parties to explore how the ACD ecosystem is being developed and deployed. Like the cyber threat itself, ACD is always evolving. In Section 4, we describe how NCSC is looking to expand ACD beyond the public sector. Section 5 sets out a series of considerations applicable to this expansion.

4. Active Cyber Defence: scaling up the ecosystem

Not all measures potentially involved in ACD are entirely novel. Governments have been engaged in similar efforts to minimise risks, vulnerabilities and threats to critical national information infrastructures for many years, both unilaterally and in close co-operation with the private sector. Indeed, what are now termed 'active cyber defence measures' have been deployed in the last several years as part of such public-private efforts to both reduce vulnerabilities and rebuff efforts by threat actors to exploit these. One of the most public of these was the October 2014 Operation SMN/'AXIOM' in which a coalition of private-sector and US government entities identified, shut down and cleansed a range of vulnerabilities in operating systems and computer network attack command-and-control capabilities allegedly being exploited by a Chinese state actor. The success of this action occurred mere weeks prior to a US-China summit in which China agreed to halt all offensive cyber operations aimed at intellectual property theft and related behaviours.[54]

The ACD programme has always, ultimately, been about protecting 'the entire UK cyberspace'.[55] The experiments thus far have been geared to demonstrating the value of ACD in improving the cybersecurity of the government digital estate, that is, the *.gov.uk* domain. Attention is now turning to how ACD can contribute to protecting the UK more widely, i.e. UK plc. This is an ambitious project that requires private-sector buy-in, as most of the UK's digital infrastructure, internet or otherwise, is owned and operated by private companies. It is one thing to convince government agencies and organisations to adopt particular technologies and best practices. It is quite another to incentivise firms to do the same, or indeed other organisations like charities, that may not see immediate value in doing so.

> "... research commissioned by the UK government suggests that even though most companies and charities reliant on, rather than operating, internet services have experienced adverse cyber incidents, there remains a dearth of cybersecurity policy, technology and training across multiple sectors"

There are competing dynamics in this environment. On the one hand, the Internet Services Providers' Association (ISPA), the UK's premier trade body representing the internet industry, has indicated its broad support for ACD.[56] While noting that there is no 'one-size-fits-all' solution emerging from ACD, 86 per cent of ISPA's members are implementing or planning to implement ACD measures.[57] On the other hand, research commissioned by the UK government suggests that even though most companies and charities reliant on, rather than operating, internet services have experienced adverse cyber incidents, there remains a dearth of cybersecurity policy, technology and training across multiple sectors.[58] Cybersecurity awareness continues to rise but this is often not matched by prioritisations in investment.[59] This will be a key consideration for ACD, as government will not provide 'ACD-in-a-

54 For SMN/'AXIOM' see https://www.novetta.com/2014/10/operation-smn-detailed-reporting-released/ and http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

55 HM Government, *National Cyber Security Strategy*, p. 33.

56 Internet Services Providers' Association UK, 'ISPA statement on Active Cyber Defence', 5 February 2018. https://www.ispa.org.uk/ispa-statement-active-cyber-defence/

57 Internet Services Providers' Association UK, 'ISPs say government must tackle convoluted regulatory system to safeguard UK cyber security', 16 October 2018. https://www.ispa.org.uk/isps-say-government-must-tackle-convoluted-regulatory-system-to-safeguard-uk-cyber-security/

58 Department for Digital, Culture, Media and Sport, Ipsos MORI Social Research Institute, and the University of Portsmouth, *Cyber Security Breaches Survey 2018*.

59 This applies in the public sector too. See, B. Heather, 'Exclusive: tighter cyber security deemed "not value for money"', *Health Service Journal*, 5 October 2018. https://www.hsj.co.uk/technology-and-innovation/exclusive-tighter-cyber-security-deemed-not-value-for-money/7023505.article

box' to interested parties. NCSC will provide advice, guidance and data but will not ordinarily supply the core technologies themselves.

This presents a practical challenge to any government hoping to promote better cybersecurity. It also raises questions about the appropriate levers available to an organisation like NCSC, which cannot itself mandate the adoption of ACD in whole or in part, especially without legislating it as a statutory requirement on businesses, which is not under discussion. It is significant that companies like Nominet and BT have been important partners in ACD, but they might be expected to be so as key operators of critical national infrastructure. The support of ISPA is also important, as its members represent most of the UK's ISPs, for whom improving cybersecurity is, or should be, a core requirement of their business model.

The main problem is in incentivising other organisations – especially across the critical national infrastructure (CNI), but also through small and medium-sized businesses and civil society organisations – to adopt better cybersecurity practices, which may not be understood as a key corollary to their dependence on internet technologies. Dependence creates vulnerabilities; vulnerabilities lead to risks. Cybersecurity is therefore a key factor in determining organisational risk and resilience postures. NCSC has hinted at the influence of 'cyber-Darwinism' at work.[60] Organisations that adopt better cybersecurity will survive and thrive; those that do not will fail or, at the least, risk their competitive advantage. This would also apply to ISPs that do not implement ACD or ACD-like provisions. If consumers cannot trust a company, they will withdraw their support and a company's bottom line will suffer. The appropriate lever here is public perception of a company's commitment to securing its consumers' data and activities, backed up with publicly available information that demonstrates what a particular company is or is not doing when it comes to ACD.

"Organisations that adopt better cybersecurity will survive and thrive; those that do not will fail or, at the least, risk their competitive advantage."

The hope with ACD is that it can help identify which companies are adhering to good practices and which are not. The 'carrot' is the recognition of one's commitment to cybersecurity; the 'stick' is the risk of going out of business. There will always be 'bulletproof hosts', which allow their (often criminal) clients great flexibility in the types of content hosted and activities undertaken, but these will be squeezed out of the UK, as they mostly have been already. As NCSC's Ian Levy observed, 'My job is not to beat cybercrime. It's to send it to France'.[61]

This may sound flippant but the central point is clear: if successive countries can clean up their national domains, it will push bad actors further out and away, corralling them in foreign jurisdictions where they are potentially susceptible to other forms of national power. ACD can help in this respect, by demonstrating, first, the UK's commitment to securing UK cyberspace from the majority of cybercriminal nuisance and effects and, second, the potential value of such an approach for other countries. No one expects wholesale adoption of 'the British model' abroad, nor

60 BT, 'BT Tower talk challenges cyber security perceptions', 7 July 2015. https://www.btplc.com/Innovation/Innovationnews/cybersecurity/index.htm

61 Stilgherrian, 'UK's NCSC to monitor internet routing to stop DDoS and hijacks', *ZDNet*, 12 October 2018. https://www.zdnet.com/article/uks-ncsc-to-monitor-internet-routing-to-stop-ddos-and-hijacks/

would this be politically appropriate, but elements of ACD may inspire others to implement similar initiatives, thereby contributing to the overall 'health' of the global internet. This includes work around various internet and telecommunications protocols and standards. NCSC is actively promoting changes in this field in international forums. If it can show improvements at home as a result of these revisions, it will be better positioned to incentivise their wider adoption.

Our research indicates that promoting the lessons and elements of the ACD ecosystem beyond the public sector is technically feasible and is already underway. As much of it is automated, it has an inherent scalability that facilitates further deployment while preserving efficacy. The primary ambition is to make it 'as unprofitable and risky as we can for cyber criminals to act in the UK'.[62] The ACD programme shows early promise in this respect but the following section outlines some considerations that should be taken into account as the project develops in scale and scope.

62 NCSC, *Annual Report 2018*, p. 16. See also, J. Saunders, 'Tackling cybercrime – the UK response', *Journal of Cyber Policy*, 2, 1 (2017), pp. 4-15.

5. Active Cyber Defence: considerations

> The social value of ACD lies in its self-restraint. It is set up as a suite of defensive and protective measures that deliver better cybersecurity, not perfect cybersecurity."

Keep ACD defensive

The social value of ACD lies in its self-restraint. It is set up as a suite of defensive and protective measures that deliver better cybersecurity, not perfect cybersecurity. It is therefore crucial that ACD continues to be perceived as limited to defence and does not stray into offence. The UK has an offensive cyber mission but this should not be confused with initiatives like ACD. At present, we detect no NCSC appetite for adopting a more aggressive ACD posture, as per US interpretations of the term.[63] This stance should be maintained, in order to build legitimacy and support for the programme, neither of which is a given. This will require internal government resistance to potential 'mission creep' but also public vigilance, including by the media and advocacy groups, many of whom are already actively engaged in monitoring UK government agencies.

The Intelligence and Security Committee (ISC) of Parliament should continue to examine the ACD programme to ensure it does not stray into problematic territory.[64] This includes avoiding the enrolment, accidentally or otherwise, of non-government entities into offensive or ambiguous cyber operations.[65] The Information Commissioner's Office (ICO) should additionally ensure that personally identifiable data is not finding their way back into the UK's SIGINT systems via NCSC. As NCSC is pushing responsibility for private-sector ACD deployment to the private sector itself, this should not happen anyway. For example, the public will not have access to the government DNS resolver, which might reveal personal data. NCSC only receives – and will only receive under normal circumstances – 'headline' statistics from the private sector, such as how many phishing clicks were stopped by a particular ISP in a given time period. NCSC will use these to build a comprehensive picture of national cyber threats and help determine ACD progress. ACD is not designed to gather more granular data about individual users but continued transparency on this issue will help ensure public trust and support.

Incentivising firms

There are hints in NCSC documentation that 'carrots' may not be enough to incentivise private firms to adopt ACD measures, or to take necessary remedial actions in good time. In the latter case, NCSC acknowledges that it is 'not clear what we should do about this, apart from calling out the companies who consistently fail to take fraud and security seriously.'[66] Elsewhere, the same report states that NCSC is 'willing to intervene if particular infrastructure owners are intransigent in fixing their networks.'[67] Neither statement constitutes formal policy but it is unclear what either process would look like in practice. It may be that government intervention is justified in the case of critical national infrastructure, if Operators of Essential Services (OES) fall foul of the EU's August 2016 Directive on the Security of Networks and Information Systems (the NIS Directive), which came into effect in the UK

63 But see, M. Sexton, 'UK cybersecurity strategy and active cyber defence – issues and risks', *Journal of Cyber Policy*, 1, 2 (2016), pp. 222-242.
64 Intelligence and Security Committee of Parliament, *Annual Report 2016-2017*, HC 655, December 2017, pp. 36-37.
65 F. Egloff, 'Cybersecurity and the age of privateering', in G. Perkovich and A.E. Levite (eds.), *Understanding Cyber Conflict: Fourteen Analogies*, Washington, DC, Georgetown University Press, 2017, pp. 231-247.
66 Levy, *Active Cyber Defence*, p. 19.
67 Levy, *Active Cyber Defence*, p. 38.

in August 2018. NCSC can act as a source of technical authority and guidance in such cases but has no regulatory role in the NIS Directive itself.[68] There may be some blurring of the lines between ACD and other instruments that requires further clarification but any form of intervention should be transparent, legal and outlined in advance, so companies know what to expect in specific circumstances. We do not currently recommend an accreditation system for 'ACD-compliant' organisations but this may form part of subsequent conversations around increased cybersecurity regulation and compliance. Similar debates have begun around using insurance stipulations as a market-driver for compliance, but this is bound up in wider, ongoing discussions about how specific and effective insurance can be used to modulate cybersecurity risk.

Technical feasibility

> "From a purely technical perspective, there appear to be no insurmountable technical problems in extending ACD from .gov.uk to the national level."

The overarching approach to the requirements, definition, specification, design and current implementation of ACD is based on the utilitarian approach of addressing initially those issues which can be practically achieved for the greatest benefit. Preliminary attempts to measure and quantify the outcomes of applying these remedies are encouraging. From a purely technical perspective, there appear to be no insurmountable technical problems in extending ACD from *.gov.uk* to the national level. There will be adoption and roll-out issues but these are not primarily technical in nature and can be managed with a sensible 'carrot-and-stick' approach.

We note that the hub-and-spoke architecture of the Threat-o-Matic facilitates the removal, addition and substitution of functional modules during the development and deployment of ACD. At the same time, the existence of a central hub represents a potential single point of failure that mandates the enforcement of additional security measures for this prime target. The issues of scaling-up and automation are inextricably linked and the problems associated with machine learning technologies constitute an active field of research.[69] NCSC is aware of unintentional selection biases in the machine learning training process.[70] It will be important to devise reliable methodologies for characterising the nature and magnitude of such biases as the programme evolves.

The transparency of machine learning outputs has recently become a topic of urgent research, as everyday applications increasingly rely on machine learning support. This is particularly relevant to ACD, where rational explanations for the classifications generated by machine learning algorithms will be necessary to justify the consequential courses of action adopted. The related issue of malicious poisoning of training data (as opposed to introducing inadvertent bias) is also non-trivial.[71] The security and validation of training data must therefore remain a significant consideration in ACD expansion. NCSC is presently working with external academic

68 National Cyber Security Centre, 'Introduction to the NIS Directive', January and October 2018. https://www.ncsc.gov.uk/guidance/introduction-nis-directive

69 See, for example, H. Reese, 'Bias in machine learning, and how to stop it', *TechRepublic*, 18 November 2016. https://www.techrepublic.com/article/bias-in-machine-learning-and-how-to-stop-it/

70 Levy, *Active Cyber Defence*, p. 9.

71 L. Muñoz-González and E.C. Lupu, 'The secret of machine learning', April 2018. https://www.bcs.org/content/conWebDoc/59383

and research partners to address these issues, including, of course, other undesirable behaviours that can emerge in data-heavy computational environments.

DNS filtering and takedowns

The Protective DNS service has demonstrated its value to the public sector, blocking attempts to access over 30 million malicious websites.[72] The Takedown Service has been similarly effective. Understandably, the question arises whether it would be possible or desirable to expand these services to the wider national domain. This would require extensive sharing of threat information across multiple sectors, some of the underlying technology for which is already operational or in development.[73] This is a voluntary scheme, and should remain so, and its success will be judged on whether it is effective, whether sector-specific strategies can be adopted, and if it remains apolitical. Suggestions that this might lead to a 'Great British Firewall', akin to China's national internet filtering project, are misleading but do capture legitimate concerns about an organ of government proscribing what people can view online.[74] NCSC has attempted to address these concerns by stating that it will limit types of shared intelligence narrowly to those directly concerned with cybersecurity, so that it cannot easily be 'used for something other than cyber security protection'.[75] This is not equivalent to saying it could not be used for filtering of content undesirable in some other sense, but NCSC should be pressed on what safeguards will be implemented to ensure compliance with human rights legislation.

Widening Web Check

There are suggestions that NCSC's Web Check tool might be used outside the public sector, in order to identify basic vulnerabilities in website design and deployment.[76] This is unproblematic in government contexts but takes on a different complexion outside them.[77] In essence, do organisations want their online assets to be scanned by an NCSC 'black box' that reports back to GCHQ?[78] We detect no desire on the part of NCSC to gather data in this fashion but NCSC has suggested that it might be sensible to devolve responsibility for Web Check to competent authorities in each sector, such as the Charity Commission in the third sector.[79] We endorse this suggestion, so as to create a buffer between the intelligence community and third parties, while acknowledging that NCSC will continue to provide technical guidance and advice on Web Check technologies. This will require adherence to a robust, and as yet undefined, framework of principles and responsibilities to be determined through further deliberation, as well as a clear set of responsibilities for leadership roles across multiple industry sectors.

72 NCSC, *Annual Review*, p. 14.

73 Levy, *Active Cyber Defence*, p. 66.

74 E. MacAskill, 'GCHQ's "Great British Firewall" raises serious concern – privacy groups', *The Guardian*, 14 September 2016. https://www.theguardian.com/uk-news/2016/sep/14/gchqs-great-british-firewall-raises-serious-concern-privacy-groups

75 Levy, *Active Cyber Defence*, p. 66. This would presumably imply not using ACD technologies to protect intellectual property, for example; see, *Cartier International and Others v BSkyB and Others* [2016] EWCA Civ 658.

76 Levy, *Active Cyber Defence*, p. 65.

77 See also, https://www.turing.ac.uk/research/research-projects/web-domain-discovery

78 The same applies should NCSC's proprietary host-based intrusion detection systems be rolled out beyond the public sector; NCSC, *Annual Review 2018*, p. 16.

79 Levy, *Active Cyber Defence*, p. 65.

Export controls

The adoption of ACD or ACD-like systems by foreign partners is central to the programme's broader aims. As previously noted, NCSC is in discussions with many third-party countries, some of which will pertain to ACD. If ACD is, in a sense, to be a British-branded export, how will UK government vet and select its foreign partners, so as to assure compliance with export controls on defence and security goods and services and, in particular, with human rights and democratic principles? The government has issued very brief guidance on the risk assessment and licensing process for cybersecurity exports, including that it consider possibilities for human rights abuses.[80] If ACD is to be part of the 'bespoke offers' advertised in the *Cyber Security Export Strategy*, what guarantees will be provided that ACD components will not be adapted for purposes unintended by their originators and which will be deleterious to citizens elsewhere? Amidst current concerns about British exports of surveillance technologies to human rights-abusing countries, clarity should be provided as to the conditions under which ACD technology trade or transfer will be conducted.[81] Similarly, the UK government will also be reluctant to share any practices which could reveal sources and methods of cyber-related intelligence collection that form part of the ACD threat, risk and vulnerability identification processes.

"Amidst current concerns about British exports of surveillance technologies to human rights-abusing countries, clarity should be provided as to the conditions under which ACD technology trade or transfer will be conducted."

Bureaucratic deconfliction

ACD is a specific component of *NCSS 2016* and an instrument largely of GCHQ via the NCSC – but it does not exist in isolation from other government activities in cyberspace. ACD aims to identify, halt and, wherever possible, terminate malicious online activities that impact the UK. Concurrently, the police and security agencies pursue investigations into cybercriminality and threats to national security in the same environment that ACD targets. These involve the identification of malicious activities, their attribution to real-world people or organisations and, often, covert operations to gather evidence or intelligence.[82] In pursuing these activities, the police and security agencies may come into contact with online elements ACD aims to remove, which could have knock-on effects on the success of a criminal or national security investigation. Similarly, statutory intelligence operations may need to leverage the same online entities, assets or resources ACD is looking to eliminate or remove. This also applies to the policing and intelligence operations of other countries, especially allies, a situation likely to intensify as more countries engage in such online efforts.

There is a risk that ACD could limit or damage the legitimate policing and intelligence operations of the UK and its allies.[83] Operational and strategic tensions

80 Department for International Trade, *Cyber Security Export Strategy*, 26 March 2018, p. 19. https://www.gov.uk/government/publications/cyber-security-export-strategy

81 J. Doward and E. Courea, 'Government urged to halt overseas sales of surveillance devices', *The Observer*, 6 October 2018. https://www.theguardian.com/world/2018/oct/06/government-halt-surveillance-kit-sales-authoritarian-countries

82 For example, the Digital Intelligence and Investigation (DII) capacity being developed through the Home Office, Office for Security and Counterterrorism (OSCT), and National Police Chiefs Council (NPCC); Association of Police and Crime Commissioners/National Police Chiefs Council, *Policing Vision 2025*, November 2016, p. 10. https://www.npcc.police.uk/documents/Policing%20Vision.pdf

83 Examples could include: severing links between UK-based entities and 'Dark Web' illegality while these are subject to investigation by UK or allied law enforcement; or, removing command-and-control elements or 'hop points' used by a foreign

could also emerge about what should take precedence in particular situations. Therefore, a co-ordination and deconfliction mechanism would seem to be in order. Complete co-ordination and deconfliction is rarely possible, especially when it comes to covert online operations; it is nevertheless essential that ACD takes account of and looks to co-ordinate its activities to the greatest degree possible with police and intelligence partners. This should be enabled by the existing involvement of the National Crime Agency in the NCSC and by NCSC's deep relationships with the rest of the UK intelligence community. It should also include the Digital Intelligence and Investigation (DII) lead in the National Police Chiefs Council (NPCC) to take into account the rest of UK policing. Operational deconfliction should be matched with policy deconfliction through the Cyber and Government Security Directorate (CGSD) and its links into the National Security Secretariat, which is responsible for the strategic and policy coordination of UK government cybersecurity. We assume these activities are occurring, but the complex and crowded technical and institutional cyber environment suggests that these issues are worth raising and are subject to ongoing monitoring and adjustment.

Risks and the national view

There has been little national debate about ACD specifically and *NCSS 2016* generally. This therefore makes it somewhat difficult to judge what level of online risk is acceptable to UK businesses and the public, or where the threshold should be for countering these risks. Indeed, even after each massive data leak or breach is made public, discussions about these incidents die down very quickly. In short, there is very little public debate – or possibly even real interest, let alone political pressure – surrounding cybersecurity in the UK today. Indeed, the real debate may only gather steam between the government and the private sector when ACD is extended beyond the public sector and the government takes a more proactive role in protecting the online footprint of UK plc. At the same time, the muted nature of this issue may also be down to a perception that the ACD programme is going in the right direction and, after two years, is a successful approach with which the private sector and civil society are comfortable. Nevertheless, continued close co-operation between the NCSC, the public, ISPs, firms and the UK critical infrastructure owner-operator community in determining the continued technical and political evolution of ACD is essential.

> "... continued close co-operation between the NCSC, the public, ISPs, firms and the UK critical infrastructure owner-operator community in determining the continued technical and political evolution of ACD is essential."

The role of the private sector in cyber defence

The role of the private sector in cyber defence is growing significantly. It is also coming under ever-increasing scrutiny and pressure to identify and remove malicious content from online platforms; to take more responsibility for, and play a stronger role in, evolving notions of personal and public safety online; and to demonstrate responsibility and accountability in their use of personal and commercial data. In co-operating with the private sector on the continued development of ACD, the NCSC should consider what these pressures may mean for future efforts to regulate commercial platforms and content providers and how it could seek to develop joint

government to engage in computer network operations against UK interests that are already entwined in an online UK intelligence operation.

initiatives with these companies to remove and restrict such content being made available on their platforms. For example, ACD aims to eliminate connections between UK entities and malicious cyber tools sold on the Dark Web, while at the same time companies such as Google, Facebook, Instagram, and so on, are doing the same. Cooperative ventures to achieve these joint goals would be worth considering by both government and private sector stakeholders, to their long-term mutual advantage.

Future-proofing

In examining ACD today, it is also worth considering what ACD may be able to achieve tomorrow. If there is one truism about threats, it is that those who propagate them will always seek to find – and often succeed in finding – a way to overcome defensive and protective measures put in place to counter them. For cyberspace and the ways in which malicious cyber activities have evolved over the last three decades, this has been an absolute. As security measures like firewalls, intrusion-detection/protection systems, anti-virus, counter-spam and counter-phishing programs have evolved to reduce or eliminate these threats, the capability and sophistication of these threat methodologies have similarly evolved to stay one step ahead of these countermeasures. For ACD, this will inevitably be the case.

“The internet has morphed considerably over the last three decades and will continue to do so. Therefore, ACD will need to change with it.”

ACD is similarly reliant to some degree today on the paradoxically globalised and nationally-bounded nature of the internet. It can seek to detect and identify threats virtually anywhere they originate, while similarly being able to focus on a specific geographic domain of the internet – i.e., the UK cyberspace as broadly construed – for its interventions. The internet has morphed considerably over the last three decades and will continue to do so. Therefore, ACD will need to change with it, for example, as internet traffic routes change, as the technologies that form the backbone of the internet evolve, and as the global regulatory environment which attempts to govern the internet shifts.

Without knowing, of course, what the future holds, it is nevertheless recommended that the NCSC and the technologists, scientists and policymakers who determine the future direction of ACD take stock of such potential future scenarios and plan for them today. For example, as both email spoofing and website spoofing continue to evolve – and potentially become far more capable of ‘hiding in plain sight’ from counter-measures – how will ACD continue to ensure the highest possible level of success in countering these? How will it tackle a gradual shift from network-level threats to those affecting the application layer? Or, once criminal gangs and foreign governments start using artificial intelligence (AI) and machine learning (ML) to enhance their efforts to overcome counter-measures and defences – as they inevitably will – how will ACD’s own AI/ML capabilities be able to counter this enhanced nefarious capability? This should not be understood as an AI ‘arms race’, or other such unhelpful framing, but as an ongoing effort to ‘design in’ ways of limiting and controlling undesirable effects of adversarial AI.

The experience that Western police and intelligence services have voiced publicly concerning their efforts to deal with the dramatic changes that the encryption of messages and devices have meant for their evidence and intelligence gathering is

instructive here. Without advocating a position in this contentious area, it is clear that this technological development presents significant challenges to the law enforcement and national security mission space. Making solid efforts today to anticipate, roadmap, and attempt to plan ahead for the continued evolution of the malicious online activities that ACD aims to halt is advisable. Doing so in close co-operation with the UK cybersecurity industry, researchers and critical infrastructure owner-operators is highly desirable and beneficial to the overall ACD effort. Our research indicates NCSC and its partners are fully apprised of these dynamics and intend to deliver widespread social benefits while recognising the risks inherent to all technologies.

6. Reflections and recommendations

It may seem an unusual step for an intelligence agency to seek to intervene so openly in the communications networks of a liberal, democratic state. For some, it may be a step too far. That being said, however, the issue of ACD has been remarkable for the almost complete lack of public debate and discussion around it since it was launched in 2016. This is in stark contrast to other issues surrounding the UK intelligence community and its use of publicly-available data in the last few years, e.g. the Investigatory Powers Act 2016, or the use of social media information and access to encrypted communications and devices to support national security or criminal investigations. This may be because the issue is too new or too technical, too 'uninteresting' to the greater public, or simply uncontroversial in its proposed approaches and intended outcomes.

We do not think it is a step too far. GCHQ has long had a role in protecting UK networks and its expertise has found new expression via the NCSC. This builds on the long-standing work of its predecessor organisations with the CNI such as CESG, the CPNI, the National Infrastructure Security Coordination Centre (NISCC), the National Security Advisory Centre (NSAC), and similar central bodies of recent decades. At the same time, this initiative to improve UK cybersecurity and to engage actively in its cyber defence reflects parallel efforts in countering terrorism and related physical threats to the UK. In some ways, ACD is a parallel to the UK Counter-Terrorism Strategy (CONTEST) PROTECT, PREVENT and PREPARE pillars as these have developed over the last two decades.[84] Similarly, the development of the UK's counter-cybercrime approach – enshrined initially in the *Computer Misuse Act* (1990) – also reflects active efforts to reduce the UK's vulnerability to cyber threats, a responsibility now led by the NCA and partially enshrined in the national DII programme of the Home Office and the National Police Chiefs Council (NPCC). It is sensible that NCSC should capitalise on all these institutional roots to promote better cybersecurity in the UK, including through the Active Cyber Defence programme, whose basic tenets and early promise we endorse.

This is a novel initiative that reflects broader shifts in national cybersecurity posture, not least of which is the backdrop of increased regulation to address issues the market has been unable to solve on its own. Based on the early results of public-sector ACD, it seems reasonable that it can help deliver cybersecurity improvement beyond government networks. How that happens will be partly a process of trial and error, not least in experimenting with the right mix of incentives to attract partners in business and the third sector.

"Based on the early results of public-sector ACD, it seems reasonable that it can help deliver cybersecurity improvement beyond government networks. How that happens will be partly a process of trial and error, not least in experimenting with the right mix of incentives to attract partners in business and the third sector."

Furthermore, during our research, we encountered the proposition that ACD might be framed as a 'public good'. Specifically, the outcomes of ACD – rather than the technologies themselves – can be portrayed in this fashion. A public good is something that one individual can consume without reducing its availability to another individual (non-rivalrous) and from which no one is *a priori* excluded (non-excludable). An example might be street-lighting, which is provided for the use of all

84 HM Government, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, June 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

and the consumption of which confers no disadvantage on anyone else also using it to walk home at night.

A personal computer meets neither of those criteria. One may be excluded from access to one by virtue of lack of funds or physical exclusion but, once purchased, others cannot access it either.[85] Computer security, when reliant on commercial products, extends to all users but only if they pay for it, and is also therefore not a public good.[86] A free computer security product muddies this categorisation a little but a user would still have to choose to download and install it; individuals tend not to have the choice whether to consume public goods or not.

Markets are usually very poor at providing public goods, as they seek value based on scarcity. Public goods are therefore usually supplied by governments or other collective bodies. Most states, for instance, appear to provide national security as a public good, in which all individuals are protected from external threats without needing to 'opt in', and the provision of security to one does not affect the provision of security to all. This does not mean that national security is always perfect, or can never be discriminatory on various grounds, but it is ideally set up as a public good. Could we view the cybersecurity provided by ACD in the same way?

One way of testing this proposition is to ask whether ACD meets the seven criteria of a public good set out in Table 1.[87]

TABLE 1: PUBLIC GOOD CRITERIA AND ACTIVE CYBER DEFENCE

Public good criterion	Does ACD meet criterion?	Comments
Not easy to measure quantity and quality	Partly	Metrics available but it is not possible to fully determine what would happen if ACD were not deployed.
Consumed jointly and simultaneously by many	Yes	ACD would operate equally and persistently for all users.
Difficult to exclude users who don't pay	Yes	ACD is free at the point of delivery. Exclusion only occurs as the result of user decisions.
Individual has limited choice whether to consume or not	Partly	It would be difficult to avoid if ACD was comprehensively adopted across the UK but users could opt out if they wished.
Individual has limited choice about kind or quality of goods	Partly	Choice could hypothetically be enacted at the ballot box, or when consumers choose between 'good' and 'bad' ACD deployments.
Payment for goods is not closely related to demand or consumption	Yes	ACD would require no direct payment, so payment and consumption mostly delinked. Minimal ACD costs might, however, be passed on to consumers.
Allocation decisions are primarily political	Partly	ACD deployment is voluntary but mandating it would require ministerial decision.

ACD appears to partially or wholly meet all of these criteria. There are very few 'pure' public goods, so ACD might qualify as 'good enough' to warrant labelling as a public good, particularly as one of the motivations for ACD was the market failures

85 It is a private good.

86 This is known as a 'toll good' or 'club good'.

87 These criteria are based on the classic work of V. Ostrom and E. Ostrom, 'Public goods and public choices', in Michael McGinnis (ed.), *Polycentricity and Local Public Economies*, Ann Arbor, MI, University of Michigan Press, 1999, pp. 75-105.

that accompanied the national cyber security strategy from 2011 to 2016. However, a confounding factor is that the private sector *is* being asked to invest in ACD. If the market tends to be averse to providing public goods, not least because of fear of free-riders, how can ACD as the product of both public and private entities be characterised as a public good?

A possible answer lies in asking what ACD is for. Many forms of security cannot be characterised as a public good; they exclude as much as they include, and one person's security is another's insecurity. However, when security adopts a preventive mode and is 'defined as the absence of a threat, it appears to meet the criteria of a collective [i.e. public] good.'[88] The stated aim of ACD is 'to protect the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time.'[89] This is a preventive mindset that intends to break the link between threat and end-user, so that the former is largely invisible to the latter. In this preventive register, ACD can indeed be considered a public good, regardless of who supplies it.

This points a way forward for ACD. As long as it remains non-discriminatory to end-users of UK internet services, it can claim legitimacy as a public good. This means that it must remain free at the point of delivery, so it does not discriminate on the ability to pay for services. It might, however, also imply that, to qualify as a public good, consumers should have very little choice but to access the internet via ACD-like systems. This apparent removal of public choice is not an ambition of ACD. In fact, ACD aims to give consumers *greater* choice over which services they select, based in part on whether providers can demonstrate their adherence to ACD principles and practices. That is, can an ISP, for instance, provide maximum ACD-style protection to a customer as part of its sales package? If so, it might attract customers on that basis and further incentivise ACD adoption in the marketplace. If not, consumers may look elsewhere for service provision. ACD is meant to promote these forms of competition and create a situation in which demand and supply dynamics shift the market towards ACD protections which are both free and secure by default.

> "In order to scale up ACD to the national level and to deliver on the promise of a genuine public good, we recommend that the government, GCHQ and NCSC aspire to the highest standards of probity, transparency and openness."

That said, it is the responsibility of NCSC and the government to demonstrate that ACD is effective, legal and ethical, rather than expecting businesses and charities to sign up solely on the basis of trust. The future of ACD is as much about being seen to be doing the right thing as doing that thing itself. In order to scale up ACD to the national level and to deliver on the promise of a genuine public good, we recommend that the government, GCHQ and NCSC aspire to the highest standards of probity, transparency and openness. This applies to their self-reporting and to their interactions with existing and potential partners. Obviously, this will be done with due respect for intelligence sources and methods but, post-Snowden, UK intelligence agencies have every incentive to be scrupulous in adherence to the spirit and letter of the law. This is particularly pertinent in an environment awash with personal data and subject to elevated concerns about digital surveillance and subversion. We recommend that NCSC continues to publish annual reports for the lifetime of ACD

88 E. Krahmann, 'Security: collective good or commodity?', *European Journal of International Relations*, 14, 3 (2008), p. 386.
89 Levy, *Active Cyber Defence*, p. 1.

and that these are subject to the scrutiny of the Intelligence and Security Committee of Parliament and other bodies like the Information Commissioner's Office (ICO), Investigatory Powers Commissioner's Office (IPCO), and others, including parliamentary select committees as appropriate.

We recommend that ACD be conceptualised provisionally as a public good to be delivered by both public and private partners. This may not be an easy pill to swallow for some private entities but, if NCSC is correct that ACD can help deliver a safer and more secure UK cyberspace, this will benefit companies as well as individual users. As noted earlier, private-sector entities have an increasing expectation of responsibility for the role that they play in the digital economy and information age, to actively reduce the risks to consumers from the information that the companies hold, handle, or propagate on others' behalf. This demands a more comprehensive public-private partnership for cybersecurity today than ever before. The indications are that many ACD provisions are relatively cheap to implement but can lead to significant and tangible gains in cybersecurity.[90] Moreover, some are deployed at the network level, so the buy-in of a few major companies – including ones already involved – will bring about major positive effects nationally. We recommend that the government conducts or commissions a deeper study of cybersecurity as a public good in order to inform the next phase of the *National Cyber Security Strategy* in 2021.

We also support the continued development of a more multilateral, global effort to increase cyber defences in the manner indicated by ACD. Government should work through multiple channels to expand awareness and uptake of relevant approaches, through diplomacy and foreign policy, intelligence and police liaison, and international business relationships. This should also include standards organisations, like the International Organization for Standardization (ISO) or the US National Institute for Science and Technology (NIST) and its benchmark Cybersecurity Framework. Efforts should also extend to civil society partnerships at home and abroad.

> "... 'exporting' ACD to as many countries as possible will, like an effective 'neighbourhood watch programme' or public immunisation, help to reduce the number of opportunities and targets available to cybercriminals and malicious foreign actors throughout the world.."

One country cannot force others to adopt such measures. Equally, one country cannot simply aim to deflect threats and risks to other countries: in today's highly interconnected, globalised world, those problems will inevitably blow back at some point, often very rapidly. Conversely, pursuing ACD and similar efforts in isolation from a multilateral framework may end up being counterproductive and ultimately diminish the success of such an initiative. Similar recent and ongoing multilateral initiatives – such as the EU's General Data Protection Regulation (GDPR), or global co-ordination to counter online child exploitation – have shown how much greater the potential of such efforts is when pursued multilaterally and with adherence to commonly accepted norms. Therefore, 'exporting' ACD to as many countries as possible will, like an effective 'neighbourhood watch programme' or public immunisation, help to reduce the number of opportunities and targets available to cybercriminals and malicious foreign actors throughout the world.

90 Like other elements of the National Cyber Security Programme, the cost of ACD is not publicly reported. We are confident that ACD provides significant return on investment congruent with the public interest and may also free up funds for countering other forms of cyber threat. We recognise that this reporting situation does 'hinder external scrutiny of the effectiveness and value for money' of ACD and other initiatives. See, JCNSS, *Cyber Security*, ss. 30-36.

It is also expected that the ACD will be audited by the NAO, as well as reviewed by the Intelligence and Security Committee and the Investigatory Powers Commissioner's Office (IPCO). Such reviews can only serve to enhance the transparency and public accountability of an initiative that is rather different from conventional intelligence community operations, albeit for legitimate purposes and the public good. The NCSC should encourage such reviews and advertise their results once completed. As a highly beneficial part of the evolution of ACD – alongside the close collaboration recommended with both the private sector and research community – the feedback received from audits and reviews can only help to strengthen ACD capabilities and objectives. This will be especially the case as the global internet infrastructure continues to evolve, and global regulatory norms emerge to guide how businesses and individuals engage with the online world.

Finally, we recommend that the UK government persists in its current interventionist cybersecurity posture. It should be remembered that the levels of intervention now are relative to a very weak baseline of even five years ago. The present levels of government involvement are therefore neither dramatic nor overbearing. Moreover, if ACD data are representative of wider trends, there are signs of improvement in UK cybersecurity. This is partly a function of the intensification of government cybersecurity efforts, most notably via the NCSC, but also of increased investment and awareness across the private sector and civil society. Many challenges, particularly countering state-sponsored cyber operations and critical infrastructure protection, are beyond the scope of this report, but ACD is indicative of what can be done with relatively few resources and some innovative thinking. We recommend that industrial, academic and other partners engage with NCSC on ACD and related initiatives, in order to further conceptual and practical cybersecurity knowledge in the UK.

> "... ACD is indicative of what can be done with relatively few resources and some innovative thinking."

In conclusion, we assess that the Active Cyber Defence programme is a promising addition to UK cybersecurity and merits further support and attention. If implemented carefully but robustly it should do much to tackle cybercrime and cyber threats to UK networks and users and help promote national prosperity and wellbeing.

7. Abbreviations

ACD	Active Cyber Defence
AI	Artificial intelligence
BGP	Border Gateway Protocol
CCA	Centre for Cyber Assessment
CERT-UK	Computer Emergency Response Team UK
CESG	Communications-Electronics Security Group
CGSD	Cyber and Government Security Directorate
CONTEST	UK Counter-Terrorism Strategy
CNI	Critical national infrastructure
CPNI	Centre for the Protection of National Infrastructure
DDoS	Distributed denial-of-service
DII	Digital Intelligence and Investigation
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
GDPR	General Data Protection Regulation
GCHQ	Government Communications Headquarters
EU	European Union
HMRC	Her Majesty's Revenue and Customs
IA	Information assurance
ICO	Information Commissioner's Office
IPCO	Investigatory Powers Commissioner's Office
ISC	Intelligence and Security Committee of Parliament
ISO	International Organization for Standardization
ISP	Internet service provider
ISPA	Internet Services Providers' Association

JCNSS	Joint Committee on the National Security Strategy
MISP	Malware Information Sharing Platform
ML	Machine learning
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NCSP	National Cyber Security Programme
NCSS	National Cyber Security Strategy
NISCC	National Infrastructure Security Coordination Centre
NIS Directive	European Union Directive on the Security of Networks and Information Systems
NIST	US National Institute for Science and Technology
NOCP	National Offensive Cyber Programme
NPCC	National Police Chiefs Council
NSAC	National Security Advisory Centre
NSS	National Security Strategy, National Security Secretariat
OES	Operators of Essential Services
OSCT	Office of Security and Counterterrorism
SIGINT	Signals intelligence
SS7	Signaling System 7

Authorship, acknowledgements and bibliography

About the authors

Dr Tim Stevens is Lecturer in Global Security in the Department of War Studies, King's College London and head of the KCL Cyber Security Research Group. He has published widely on cybersecurity and related issues in academic journals and is a frequent contributor to online, print and broadcast media. He is the author of *Cyber Security and the Politics of Time* (Cambridge University Press, 2016) and co-author of *Cyberspace and the State* (Routledge, 2011).

Dr Kevin O'Brien is a Senior Visiting Research Fellow in Cyber Security and Digital Intelligence in the Department of War Studies, King's College London. He currently serves as one of Accenture's Security Leads in Canada, and was previously a senior manager in the Canadian government intelligence community. He has served as a senior advisor to the UK, US, Canadian, Australian, New Zealand, and several European governments on contemporary security and intelligence challenges, including cybersecurity and critical infrastructure protection, protective and preventive security in both the digital and physical worlds, and counterterrorism and violent extremism.

Dr Richard Overill is Senior Lecturer in Computer Science in the Department of Informatics, King's College London. Since 1996 his principal research interests have centred on cybersecurity and digital forensics, resulting in over sixty interdisciplinary publications in these areas. He is a Chartered Mathematician, a Chartered Scientist and a Chartered Engineer.

Dr Benedict Wilkinson is Senior Research Fellow in the Policy Institute, King's College London. He has specialist interests in UK defence and security policy, publishing numerous policy reports and journal articles in these fields. He is the co-editor of *The Art of Creating Power: Freedman on Strategy* (Oxford University Press, 2017) and author of *Scripts of Terror: The Stories Terrorists Tell Themselves* (Oxford University Press, 2019).

Tomass Pildegovičs is an MPhil candidate in Politics and International Relations at the University of Cambridge. He holds a BA in International Relations with First Class Honours (2018) from the Department of War Studies, King's College London. His research interests include EU-Russia relations, NATO-EU cooperation, and Baltic foreign and security policy.

Steve Hill is a Senior Visiting Research Fellow in the Department of War Studies, King's College London. He currently manages technology operational risk for a leading global bank and previously served for over 30 years in the British government, including as a Deputy Director in the National Security Secretariat of the Cabinet Office with cybersecurity responsibilities.

Acknowledgements

We are very grateful to the staff of the National Cyber Security Centre for their generosity of time and spirit in preparing this report, in particular their technical director, Dr Ian Levy. We also thank Professor Sir David Omand for his invaluable input and advice.

Bibliography

Active Cyber Defense Certainty (ACDC) Act of 2017, HR 4036, 115th Congress (2017).

Association of Police and Crime Commissioners/National Police Chiefs Council, *Policing Vision 2025*, November 2016. https://www.npcc.police.uk/documents/Policing%20Vision.pdf

BT, 'BT Tower talk challenges cyber security perceptions', *7 July 2015*. https://www.btplc.com/Innovation/Innovationnews/cybersecurity/index.htm

BT, 'BT steps up battle against cyber-crime by sharing malware data with ISPs', press release, 6 February 2018. https://www.globalservices.bt.com/en/aboutus/news-press/bt-steps-up-battle-against-cyber-crime

Department for Digital, Culture, Media and Sport, Ipsos MORI Social Research Institute, and the University of Portsmouth, *Cyber Security Breaches Survey 2018*, 25 April 2018. https://www.ipsos.com/ipsos-mori/en-uk/cyber-security-breaches-survey-2018

Department for International Trade, *Cyber Security Export Strategy*, 26 March 2018. https://www.gov.uk/government/publications/cyber-security-export-strategy

Dewar, R.S., 'The "triptych of cyber security": a classification of active cyber defence', in P. Brangetto, M. Maybaum and J. Stinissen (eds.), *2014 6th International Conference on Cyber Conflict: Proceedings*, Tallinn, NATO CCD COE Publications, 2014, pp. 7-21.

Doward, J. and E. Courea, 'Government urged to halt overseas sales of surveillance devices', *The Observer*, 6 October 2018. https://www.theguardian.com/world/2018/oct/06/government-halt-surveillance-kit-sales-authoritarian-countries

Egloff, F., 'Cybersecurity and the age of privateering', in G. Perkovich and A.E. Levite (eds.), *Understanding Cyber Conflict: Fourteen Analogies*, Washington, DC, Georgetown University Press, 2017, pp. 231-247.

Franklin, C., Jr., 'Leaderboard shows adoption of DMARC email security protocol', *Dark Reading*, 20 November 2018. https://www.darkreading.com/application-security/leaderboard-shows-adoption-of-dmarc-email-security-protocol/d/d-id/1333311?_mc=NL_DR_EDT_DR_daily_20181121&cid=NL_DR_EDT_DR_daily_20181121&elq_mid=87901&elq_cid=27767302

Gill, P. and M. Phythian, *Intelligence in an Insecure World*, third edn., Cambridge, Polity Press, 2018.

Heather, B., 'Exclusive: tighter cyber security deemed "not value for money"', *Health Service Journal*, 5 October 2018. https://www.hsj.co.uk/technology-and-innovation/exclusive-tighter-cyber-security-deemed-not-value-for-money/7023505.article

Hern, A., 'Cybercrime: £130bn stolen from consumers in 2017, report says', *The Guardian*, 23 January 2018. https://www.theguardian.com/technology/2018/jan/23/cybercrime-130bn-stolen-consumers-2017-report-victims-phishing-ransomware-online-hacking

HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161, London, The Stationery Office, November 2015. https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

HM Government, *Prospectus: Introducing the National Cyber Security Centre*, London, Cabinet Office, GCHQ and CESG, May 2016. https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus

HM Government, *National Cyber Security Strategy 2016-2021*, London, Cabinet Office and HM Treasury, November 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

HM Government, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, June 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

HM Government, *Intelligence and Security Committee Annual Report 2016-17: Further Government Response*, Cm. 9678, July 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727951/CCS001_CCS0718140448-001_ISC_supplementary_16-17_AR_response_Web_Accessi..__1_.pdf

House of Commons Defence Committee, *Deterrence in the Twenty-First Century*, Eleventh report of session 2013-14, vol. 1, HC 1066, 27 March 2014. https://publications.parliament.uk/pa/cm201314/cmselect/cmdfence/1066/106602.htm

Intelligence and Security Committee of Parliament, *Annual Report 2016-2017*, HC 655, December 2017.

Intelligence Services Act 1994 (c13).

Internet Services Providers' Association UK, 'ISPA statement on Active Cyber Defence', 5 February 2018. https://www.ispa.org.uk/ispa-statement-active-cyber-defence/

Internet Services Providers' Association UK, 'ISPs say government must tackle convoluted regulatory system to safeguard UK cyber security', 16 October 2018. https://www.ispa.org.uk/isps-say-government-must-tackle-convoluted-regulatory-system-to-safeguard-uk-cyber-security/

Investigatory Powers Act 2016 (c25).

Jasper, S., Strategic Cyber Deterrence: *The Active Cyber Defense Option*, Lanham, MD, Rowman and Littlefield, 2017.

Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure*, Third report of session 2017-19, HL Paper 222 HC 1708, 19 November 2018. https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170802.htm

Krahmann, E., 'Security: collective good or commodity?', *European Journal of International Relations*, 14, 3 (2008), pp. 379-404.

Levy, I., 'Active Cyber Defence – tackling cyber attacks on the UK', blog post, 1 November 2016. https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

Levy, I., *Active Cyber Defence – One Year On*, London, National Cyber Security Centre, 5 February 2018. https://www.ncsc.gov.uk/information/active-cyber-defence-one-year

MacAskill, E., 'GCHQ's "Great British Firewall" raises serious concern – privacy groups', *The Guardian*, 14 September 2016. https://www.theguardian.com/uk-news/2016/sep/14/gchqs-great-british-firewall-raises-serious-concern-privacy-groups

MacAskill, E., 'Major cyber-attack on UK a matter of "when, not if" – security chief', *The Guardian*, 23 January 2018. https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin

Martin, C., 'Ciaran Martin's cyber security summit speech', 23 October 2017. https://www.ncsc.gov.uk/news/ciaran-martins-cyber-security-summit-speech

Martin, C., 'Active cyber defence for the UK', Civil Service Quarterly, 30 January 2018. https://quarterly.blog.gov.uk/2018/01/30/active-cyber-defence-for-the-uk/

Muñoz-González, L. and E.C. Lupu, 'The secret of machine learning', April 2018. https://www.bcs.org/content/conWebDoc/59383

National Audit Office, *The UK Cyber Security Strategy: Landscape Review*, 12 February 2013. https://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

National Audit Office, *Update on the National Cyber Security Programme*, 10 September 2014. https://www.nao.org.uk/report/update-on-the-national-cyber-security-programme/#

National Audit Office, *Cyber Security and Information Risk Guidance for Audit Committees*, September 2017. https://www.nao.org.uk/report/cyber-security-and-information-risk-guidance/

National Cyber Security Centre, *Common Cyber Attacks: Reducing the Impact*, white paper, January 2016. https://www.ncsc.gov.uk/file/common-cyber-attacks-reducing-impact

National Cyber Security Centre, *The Launch of the National Cyber Security Centre*, London, National Cyber Security Centre, February 2017. https://www.ncsc.gov.uk/news/launch-national-cyber-security-centre

National Cyber Security Centre, 'Introduction to the NIS Directive', January and October 2018. https://www.ncsc.gov.uk/guidance/introduction-nis-directive

National Cyber Security Centre, *Joint Report on Publicly Available Hacking Tools*, 11 October 2018. https://www.ncsc.gov.uk/joint-report

National Cyber Security Centre, *Annual Review 2018*, 16 October 2018. https://www.ncsc.gov.uk/news/annual-review-2018

National Cyber Security Centre, 'Helping secure public sector email with Mail Check', 29 October 2018. https://www.ncsc.gov.uk/blog-post/helping-secure-public-sector-email-mail-check

Office for National Statistics, 'Crime in England and Wales: year ending June 2018'. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2018

Ostrom, V. and E. Ostrom, 'Public goods and public choices', in Michael McGinnis (ed.), *Polycentricity and Local Public Economies*, Ann Arbor, MI, University of Michigan Press, 1999, pp. 75-105.

Reese, H., 'Bias in machine learning, and how to stop it', *TechRepublic*, 18 November 2016. https://www.techrepublic.com/article/bias-in-machine-learning-and-how-to-stop-it/

Saunders, J., 'Tackling cybercrime – the UK response', *Journal of Cyber Policy*, 2, 1 (2017), pp. 4-15.

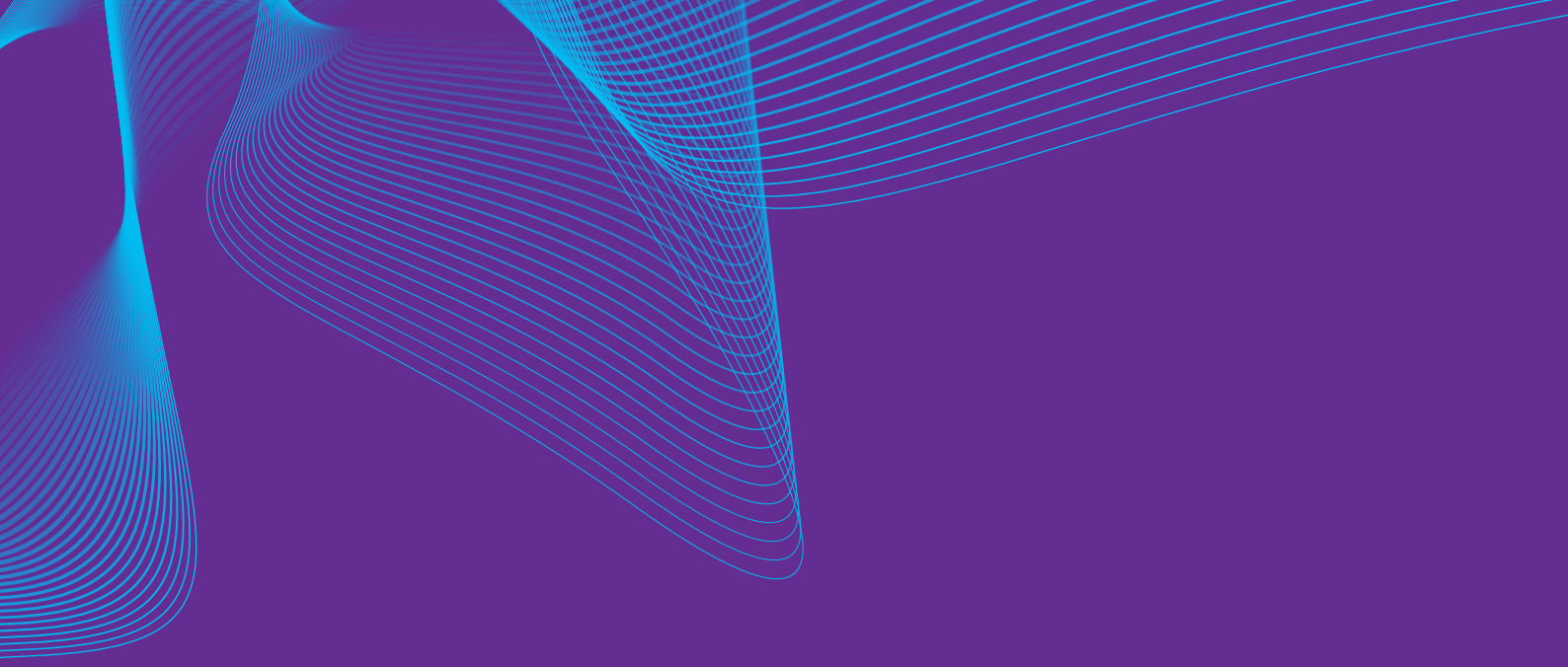
Schneier, B., 'Stop trying to fix the user', *IEEE Security and Privacy*, 14, 5 (2016), p. 96.

Sexton, M., 'UK cybersecurity strategy and active cyber defence – issues and risks', *Journal of Cyber Policy*, 1, 2 (2016), pp. 222-242.

Stilgherrian, 'UK's NCSC to monitor internet routing to stop DDoS and hijacks', *ZDNet*, 12 October 2018. https://www.zdnet.com/article/uks-ncsc-to-monitor-internet-routing-to-stop-ddos-and-hijacks/

Seals, T., 'DHS mandates DMARC, HTTPS for all US federal agencies', *InfoSecurity*, 17 October 2017. https://www.infosecurity-magazine.com/news/dhs-mandates-dmarc-https/

Thomsen, J., 'Pentagon cyber official warns US companies against "hacking back"', *The Hill*, 13 November 2018. https://thehill.com/policy/cybersecurity/416494-defense-cyber-official-warns-private-companies-against-hacking-back



Connect with us

@policyatkings kcl.ac.uk/sspp/policy-institute