CENTRE FOR TECHNOLOGY & GLOBAL AFFAIRS

ctga.ox.ac.uk

UNIVERSITY OF OXFORD

POLICY BRIEF – No. 2 April 2019

The UK's Alphabet Soup: The Organization of Cybersecurity Actors Protecting Critical National Infrastructure

Jamie Collier
Research Affiliate, Centre for Technology and Global Affairs, University of Oxford
jamie.collier@cybersecurity.ox.ac.uk

INTRODUCTION

A number of different actors are involved in protecting critical national infrastructure (CNI) systems within the United Kingdom. The breadth of expertise across varied sectors and industries means that UK CNI is ultimately protected by a loose network rather than a single empowered actor. Although the necessity of such an assemblage is inevitable, the roles and responsibilities of the participants remain ill-defined.

The UK government sits at an inflection point. It must decide on the extent of its own role in protecting CNI, as well as formalizing its relationship with other relevant security actors. This policy brief seeks to clarify this issue by outlining three sets of decisions that the UK government must address in the coming years: first, the balance of roles and responsibilities between the public and private sector; second, the arrangements for the internal delegation of the cybersecurity remit within government; and third, the opportunities for international cooperation that the United Kingdom should engage in and prioritize.

THE PUBLIC–PRIVATE NEXUS

In ensuring the cybersecurity of CNI, the UK government faces a difficult balancing act in determining the appropriate balance of responsibilities between the public and private sector. The private sector has understandably taken the lead in the cybersecurity of CNI, with approximately eighty percent of CNI privately owned and managed.[1] In its 2011 Cyber Security Strategy, the government assumed that the private sector would be appropriately incentivized to protect its own systems – an issue of particular importance for CNI. Therefore, the government has largely played

1 Warwick Ashford, "Is UK Critical National Infrastructure Properly Protected?" *Computer Weekly*, March 3, 2011, http://www.computerweekly.com/news/1280097313/Is-UK-critical-national-infrastructure-properly-protected.

a hands-off role in the cybersecurity of private firms, regulating with a light touch and minimal governmental involvement. Where the government has become involved, this has typically been through public-private partnerships, including information-sharing arrangements, simulation exercises, and high-level auditing. The government has also developed an accreditation programme called "Cyber Essentials," which requires a certain level of cybersecurity competence and is now stipulated for suppliers bidding for sensitive government contracts, including those that are related to CNI.

Because many private owners of CNI are monopolies, and because cybersecurity often clashes with other business objectives (such as keeping costs low), a hands-off approach from the government may result in a sub-optimal level of CNI cybersecurity. There is an emerging consensus that a cybersecurity market failure exists, including in portions of CNI.[2] In the event of a serious cyber attack on CNI (where, for example, key portions of the power grid are disabled), most of the costs of a security failure would fall on citizens rather than the relevant private owners of CNI. The government has recently signalled a tougher approach than it initially described in the 2011 Cyber Security Strategy, claiming in its 2016 Cyber Security Strategy that a market-based approach "has not produced the required pace and scale of change."[3] Going forward, the document asserts, "Government has to lead the way and intervene more directly by bringing its influence and resources to bear to address cyber threats."[4]

Yet, just as there are dangers that the government's approach is too "hands-off," increased intervention comes with its own set of risks. As the government intervenes more directly, it risks losing the cooperative tone and goodwill that exists between the public sector and private owners of CNI. Furthermore, with several MPs having recently revealed publicly that they share their passwords with colleagues, and with the recent WannaCry ransomware outbreak leading to serious disruption of out-of-date NHS systems, the government has some work to do before it can establish itself as an authority on issues of CNI protection.[5]

Regulation represents a blunt instrument for changing cybersecurity behaviour. CNI exists in a variety of industries, each of which should be managed and regulated differently given the specific challenges faced in each sector. Certain sectors might be faced with challenges related to specific types of legacy systems for example. Various notions of security are also more or less relevant depending on the CNI sector in question (availability is more crucial for the power grid when compared to the healthcare sector where issues of confidentiality become increasingly important for example). While the government could theoretically intervene in the market in numerous ways (such as regulations, mandatory security spending requirements, minimum security standards, shifting legal liabilities, etc.), many of these options offer imperfect solutions. Government intervention could prove to be ineffective. While mandating rudimentary minimum security standards is a useful first step for organizations, they do little to prevent against sophisticated threat actors such as other nation-states. Encouraging CNI firms to spend more on cybersecurity – either through tax credits or mandatory spending requirements – would be unlikely to result in substantially greater security. Instead, it is more likely that existing staff would be nominally reclassified as security personnel and organizations could adjust their accounting to include broader spending on IT equipment as security spending.[6] Fines and shifting liabilities may impact behaviour, although their precise impact and potential to affect change are not well understood.

The EU's General Data Protection Regulation, which came into force in May 2018, will provide useful education on these matters. This regulation exposes firms to fines of up to €20 million or 4 percent of annual turnover when they suffer from a data breach and have failed to implement basic cybersecurity measures (such as regularly auditing and testing networks).[7] Government intervention may also have unintended consequences. Regulation and mandatory security requirements raise costs that could be passed onto customers.[8] Regulation is also likely to disproportionately harm small businesses and start-ups that lack the resources to easily interpret and implement changes. Regulation may therefore have the unintended effect of further increasing the barriers to entry, thereby discouraging start-ups and smaller firms from entering the market in the first place. Therefore, while government measures might lead to improvements in security, the process could be markedly inefficient with disproportionately high costs relative to the potentially small improvements in cybersecurity.

2 Several government officials have confirmed a cybersecurity market failure, including former Director of GCHQ Robert Hannigan. See Sam Jones, "GCHQ Chief to Say Free Market Failing on Cyber Security," *Financial Times*, November 9, 2015, https://www.ft.com/content/4ec3e438-8708-11e5-90de-f44762bf9896.

3 "National Cyber Security Strategy 2016–2021," HM Government October 26, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

4 Ibid.

5 "Privacy Regulator Warns MPs Over Shared Passwords," *BBC News*, December 4, 2017, http://www.bbc.co.uk/news/technology-42225214.

6 Eli Dourado, "Is There a Cyber Security Market Failure?" *Mercatus Center Working Paper*, Vol. 12, No. 5 (January 23, 2012), pp. 1–34.

7 The UK government has confirmed that it will closely mirror the European Union's GDPR after Brexit. See Warwick Ashford, "UK Legislation Will Mirror EU's GDPR, Says Matt Hancock," *Computer Weekly*, February 1, 2017, http://www.computerweekly.com/news/450412141/UK-legislation-will-mirror-EUs-GDPR-says-Matt-Hancock.

8 Dourado, "Is There a Cyber Security Market Failure?"

The private sector is a more dominant and better-resourced security actor than government. It is therefore appropriate for private firms to take the lead in the cybersecurity of CNI, with the government playing a supportive function. Here, partnership arrangements can provide a useful way forward. While an increase in regulations is arguably necessary, the United Kingdom should be hesitant to further legislate cybersecurity without first developing a better understanding of the extent to which a market failure actually exists, the reasons why such a market failure exists, and the potential policy instruments that could be used to correct these failings. Academia and think tanks can be helpful in exploring these issues directly, as well as exploring best practices from across the world and in learning from analogous areas of market failures beyond the cybersecurity of CNI.

THE INTRAGOVERNMENTAL CYBERSECURITY RESPONSE

The government must also further examine its internal management and delegation of cybersecurity responsibilities. The government has a decentralized model, with each department largely responsible for the cybersecurity of its own CNI; the Department of Health, for example, is responsible for cyber incidents that affect the NHS, while the cybersecurity of the power grid is a matter for the Department of Energy and Climate Change.[9] This approach ensures that those responsible for CNI understand the broader context and specific challenges that exist within the relevant sector, but decentralized roles and responsibilities also increase the potential for inefficiencies. Furthermore, with an allocation of £1.9 billion for cybersecurity from 2016 to 2021, different departments will inevitably compete for budgets, whether or not they have capabilities to deliver. With multiple government departments working on cybersecurity simultaneously and in an uncoordinated manner, there is likely to be an inefficient allocation of resources and needless duplication of capability, offering poor value for taxpayers.

Government departments are not immune from market failure, given that cybersecurity can clash with other governmental priorities. The May 2017 WannaCry ransomware attack provides a case in point. Running up-to-date software features is a routine security measure, but in a resource-constrained environment, the impact of failing to follow that advice may not be foreseen (especially when the security aspects of such a decision are not fully considered). For an organization such as the NHS, there is a clear opportunity cost to investments in IT and cybersecurity – whether that be recruiting more nurses, increasing junior doctors' salaries, or investing in new hospital wards. The government should further investigate incentive structures that discourage or prevent prioritization of and optimal investment in cybersecurity. While low prioritization might be caused by limited resources and other pressing objectives, in the case of CNI, the consequences of insecure systems are potentially catastrophic. New thinking is required for situations where the incentive structures of a government department fail to encourage sufficient investment in cybersecurity. This might involve further investment in education on the urgency of cybersecurity at the ministerial level, or even more fundamental changes in policy and budget allocation to suitably alter departmental incentives.

While government departments are still responsible for CNI cybersecurity within the sectors that they cover, the government has centralized its specialized cybersecurity organizations, with the United Kingdom's computer emergency response team, the Centre for Cyber Assessment, and the previous cybersecurity arm of the Government Communications Headquarters (GCHQ) all now falling within the National Cyber Security Centre (NCSC). The NCSC is part of GCHQ but is also a distinct entity and, crucially, one that is far more public-facing given that communication with businesses and the public is crucial for cybersecurity.[10] The NCSC deserves credit for its clear messaging strategy in the aftermath of serious cyber incidents and data breaches. The WannaCry ransomware outbreak provides a case in point, with the NCSC issuing statements and advice to the press, the private sector, and the public both during and after the incident. This bodes well for the protection of CNI in the future, with the government now having an authoritative entity that is able to steer incident response. The NCSC's initial performance has been promising, and the government should support its continued development. The challenge for the NCSC now is to further establish itself as the go-to source for governmental cybersecurity advice in the eyes of the public.

INTERNATIONAL ENGAGEMENT

International organizations also regard the emergence of cybersecurity as an opportunity to expand their remits and budgets. NATO, the European Union, and the United Nations are all now pitching themselves as cybersecurity organizations and competing with one another to capture the issue with a limited resource of political and economic capital available. Cybersecurity can be presented through

9 Jamie Collier, "Cyber Crisis Management: A Critical Comparison Between the UK and Estonia," in Mariarosaria Taddeo and Ludovica Glorioso, eds., *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Initiative*, (Cham: Springer, 2016), pp. 187–212.

10 Jamie Collier, "Getting Intelligence Agencies to Adapt to Life Out of the Shadows," Council on Foreign Relations, April 5, 2017, https://www.cfr.org/blog/getting-intelligence-agencies-adapt-life-out-shadows.

various prisms, and organizations naturally frame cybersecurity issues in ways that suit them. NATO has framed cybersecurity in militaristic terms, labelling cyberspace as the "fifth domain of warfare,"[11] while the European Union has proposed cybersecurity cooperation initiatives in the context of the European project (such as the "Digital Single Market").

With various international organizations developing their presences in the cybersecurity realm, the United Kingdom faces choices regarding the sort of partnerships in which it might wish to invest resources and energy. Different multilateral organizations can offer similar cooperation arrangements (for example, NATO and the European Union host similar cyber crisis simulation exercises), and the government should be wary of duplication that is unlikely to bring value for taxpayers. Some established multilateral organizations have only recently begun looking at cybersecurity, and have a mixed track record of success.[12] Engaging in such international efforts might, at times, be more reflective of political symbolism than substantive international cooperation on the issues at hand (although this could change as multilateral bodies further develop).

More established cybersecurity cooperation mechanisms offer more promising short-term prospects. Both public and private computer emergency response teams have worked together effectively through the global Forum of Incident Response and Security Teams (FIRST) organization. The United Kingdom also has a track record of working closely with the United States and the Five Eyes community (an intelligence agency alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States) over issues of signals intelligence and cybersecurity.

Given the sensitivity of the topic, substantive and close cooperation on CNI security can likely occur only with a small number of the government's most trusted allies. Larger international fora, by contrast, are perhaps better suited for examining higher-level issues. Moving forward, the government would benefit from a more formal and thorough cost-benefit analysis of the added value that various international organizations and networks offer the United Kingdom in the context of cybersecurity and the protection of CNI when compared to previous initiatives that have touched on the issue.

POLICY RECOMMENDATIONS

It is clear that a variety of actors – including the government, the private sector, and international organizations – must work together to secure CNI against cyber threats. The precise roles and responsibilities of all of these actors, however, are not yet fully established. Going forward, the UK Government can facilitate further exploration on this open question. This will involve an audit of current cybersecurity initiatives within the government, private sector and international community. Where cybersecurity providers (including government entities) are currently failing to deliver the required response, academic research can help policymakers to determine if such sub-optimal outcomes can be rectified (through, for example, further government intervention or transferring ownership and responsibilities related to the issue to other entities.

Regulation remains a potentially blunt instrument: further government intervention offers some prospects for correcting current inefficiencies yet also comes with significant risks that can result in unforeseen negative outcomes. Again, academic research and partnerships between the UK Government and academic centres can help to both test policy proposals as well as formulate policy that has a better chance of improving cybersecurity provision.

There remains a high risk of processes being duplicated given the number of stakeholders involved in cybersecurity provision. This is likely to result in inefficiencies that impose increased costs on both organizations and individuals. The risk of needless duplication is perhaps most high amongst international organizations, given the breadth of different organizations currently seeking to capture a cybersecurity remit. The UK Government should play a role in both establishing where duplication exists and exploring how it can be reduced.

Ensuring the cybersecurity of CNI represents a significant undertaking. The challenge will increase as the United Kingdom's digital dependence grows. While the government might be just one player in a larger group, it plays a decisive role in the development of this assemblage. Moving forward, the UK government needs to develop a clear strategy for how it envisions its future role for cybersecurity and CNI, and formulate plans on how such a vision can be implemented.

11 Pierluigi Paganini, "NATO Officially Recognizes Cyberspace a Warfare Domain," June 18, 2016, http://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html.

12 For example, the United Nations Group of Governmental Experts on Information Security failed to arrive at a consensus in the 2016/2017 outcome report. See Alex Grigsby, "The End of Cyber Norms," *Survival*, Vol. 59, No. 6 (November 19, 2017), pp. 109–122; and Arun Mohan Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?" *Lawfare*, July 4, 2017, https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

CENTRE FOR
TECHNOLOGY &
GLOBAL AFFAIRS

UNIVERSITY OF
OXFORD

POLICY BRIEF – No. 2

ABOUT THE CENTRE FOR TECHNOLOGY AND GLOBAL AFFAIRS

The Centre for Technology and Global Affairs at Oxford University is a global research and policy-building initiative focusing on the impact of technology on international relations, government, and society. The Centre's experts use their research findings to develop policy and regulatory recommendations addressing the transformative power of technological change.

The Centre serves as a bridge between researchers and the worlds of technology and policymaking to impact policy in the resolution of pressing problems across six technological dimensions: Artificial Intelligence, Robotics, Cyber Issues, Blockchain, Outer Space, and Nuclear Issues.

The Centre's mission is (a) to provide leadership in creating new knowledge on practical problems affecting the security and welfare of governments, citizens, and private enterprises; (b) to influence major policy decisions and opinions in these arenas; and (c) to guide the work of leading technology developers and policymakers.

The Centre is based in the Department of Politics and International Relations at Oxford University. It is supported by core funding from Kluz Ventures.

Kluz Ventures

Centre for Technology and Global Affairs
Department of Politics and International Relations
University of Oxford
Manor Road
Oxford OX1 3UQ
United Kingdom

UNIVERSITY OF
OXFORD

DPIR
DEPARTMENT OF POLITICS & INTERNATIONAL RELATIONS