From Cyber Security to Cyber Power: Appraising the Emergence of ‘Responsible, Democratic Cyber Power’ in UK Strategy

**Joe Devanny**

Lecturer

Department of War Studies

King’s College London

London, United Kingdom

joseph.devanny@kcl.ac.uk

**Andrew C. Dwyer**

Lecturer in Information Security

Information Security Group

Royal Holloway, University of London

London, United Kingdom

andrew.dwyer@rhul.ac.uk

**Abstract:** Across three successive strategies (2009, 2011 and 2016) ‘cyber security’ was the umbrella concept for United Kingdom (UK) cyber strategy. Conceptual continuity belied changes in substance, as the state played an increasingly active role, particularly domestically. Cyber security remains a top priority in the UK’s most recent (2022) strategy, but it was superseded as the umbrella concept by ‘cyber power’. We argue that this was a deliberate decision, global in outlook, and with complex and contestable strategic implications. The UK’s concept of ‘responsible, democratic cyber power’ (RDCP) responds to significant changes between 2016 and 2022 in the geopolitics and threat environment affecting (but not confined to) cyberspace. The UK’s new cyber strategy promises to align domestic and international actors under an integrated approach, addressing perceived strategic vulnerabilities and exploiting opportunities to pursue national interests. We investigate RDCP’s conceptual coherence and strategic utility, tracking its emergence as UK strategic discourse shifted from one of cyber security to cyber power. RDCP offers one avenue for states to coordinate cyber strategy, integrating the various components branded under ‘cyber’ as an instrument of national strategy – pursuing security, prosperity, and projection of national values and influence. However, there are different potential interpretations of RDCP and an even greater number of potential ways to implement it. In the UK, as elsewhere, effective cyber power requires prioritization about what a state values, whether in developing a resilient and competitive cyber ecosystem or in meeting the challenges and threats posed by systemic competitors. We conclude by reflecting on what it means to be a ‘medium-sized, responsible and democratic cyber power’ in an era of increasing inter-state competition in cyberspace.

**Keywords:** *cyber power, inter-state competition, national cyber strategy, United Kingdom*

# Introduction

Cyber security is central to state strategy amidst the return of overt geopolitical competition, recent avowals of cyber forces by several states, and recognition that cyberspace supports both economic prosperity and the projection of national values. Many states have published national strategies addressing (in)security in cyberspace and exploiting its perceived opportunities. Scholarship on cyber strategy reflects the mainstreaming of cyber security within wider national strategy (Fischerkeller, Goldman, and Harknett 2022), alongside debates about the broader concept of ‘cyber power’ (Kramer, Starr, and Wentz 2009; Betz and Stevens 2011; Smeets 2022). Meanwhile, the focus of research is increasingly broader than the state as researchers are mindful of the private sector and civil society as actors and targets in cyberspace (Maschmeyer, Deibert, and Lindsay 2021). Analysis of published cyber strategies offers an important method to investigate how states perceive and intend to address the strategic implications of threats and opportunities in cyberspace, what audiences they seek to influence, and to what end.

In recent years, as cyber strategies have expanded in scope, they have presented ‘whole-of-government’ approaches as insufficient, instead advocating for greater inclusion of industry and civil society with formulations such as ‘whole-of-system’, ‘whole-of-society’ and ‘whole-of-cyber’ (Devanny 2021). This has occurred alongside growing public acknowledgement over the past 20 years of the role of cyber operations in national strategy (Healey 2013).[[1]](#footnote-2) Corresponding institutional arrangements, in intelligence agencies and military cyber commands, should therefore be explored as part of an integrated national strategy. This challenges institutions more accustomed to secrecy – the ‘Ronan Keating doctrine’ of ‘saying it best when saying nothing at all’ (Dwyer and Martin 2022) – and now increasingly expected to strike a delicate balance between saying too much (and risking compromising equities) and saying too little to satisfy the imperatives of strategic communications (Buchan and Devanny 2022).

The United States looms large in the literature about cyber strategy and its institutional arrangements. This is understandable, given the power and influence of the US and the comparatively greater public availability of information about its activities and doctrine. But cyber strategy is relevant globally. More states are publishing cyber strategies and establishing cyber security centres. This surface similarity masks significant national variation in the experience of devising and implementing cyber strategy. Partly, variation stems from inevitable asymmetries of states’ capabilities. However difficult it is to define ‘cyber power,’ some states clearly have greater capabilities than others (Willett 2019; Voo, Hemani, and Cassidy 2022). Variation also stems from the difficulty of achieving strategic objectives in and through cyberspace, including the challenge (in any government) of navigating the inter-institutional and bureaucratic politics of cyber strategy (Harknett and Smeets 2022; Valeriano, Jensen, and Maness 2018; Lindsay 2021).

The United Kingdom (UK) is one ‘medium-sized’ state that has tried to develop and implement a distinctive cyber strategy for over a decade against the same backdrop of geopolitical competition facing other states. This article examines UK cyber strategy since 2009, contributing to the growing literature aimed at understanding how different states experience and address challenges in cyberspace. This turn in scholarship mirrors the increasing participation of more states (and non-state stakeholders) in global diplomacy about the future of the Internet and norms of responsible state behaviour in cyberspace (Kavanagh 2017). Published UK cyber strategies, alongside public interventions by senior officials, comprise the national perspective of one capable state actor on contemporary developments in cyberspace. The UK government plays an active role in global cyber diplomacy and has recently portrayed itself as a ‘cyber power’. In proposing and accepting the challenge of developing a narrative of ‘responsible, democratic cyber power’ (RDCP), the UK highlighted many of the issues facing states in formulating, communicating (domestically and internationally), and implementing cyber strategy.

This article argues that the UK’s adoption of ‘cyber power’ as a strategic umbrella concept was a deliberate decision, global in outlook, with complex and contestable strategic implications. In the first section, we track the development of the UK’s four national cyber (security) strategies (2009, 2011, 2016 and 2022). We note how RDCP responded to significant geopolitical and cyber security changes between 2016 and 2022. The UK’s 2022 strategy promised to better integrate domestic and international efforts, address perceived strategic vulnerabilities, and exploit opportunities to pursue national interests. The second section of the article investigates RDCP’s conceptual coherence and strategic utility. RDCP – construed broadly as the impact of democratic values and accountability arrangements on the responsible exercise of power in cyberspace – offers a framework for national cyber strategy. It integrates the various components branded under ‘cyber’ as instruments of national strategy pursuing security and prosperity, and projecting national values and influence. RDCP is, however, open to several different interpretations and methods of implementation. In the UK, as elsewhere, effective application of cyber power requires decisions about what is valued and prioritized, whether in developing resilient and competitive cyber ecosystems or meeting the challenges and threats posed by geopolitical competitors. We conclude by reflecting on what it means to be a ‘medium-sized, responsible and democratic cyber power’ in this era of increasing inter-state competition in cyberspace.

# A Brief History of UK Cyber Strategy

In the first three successive UK strategies (2009, 2011 and 2016), ‘cyber security’ was the framing concept, only replaced by ‘cyber power’ in 2022. This section addresses the principal similarities and differences between these four iterations, situating them in the context of wider national security strategy and politically across six successive UK premierships. We identify key themes in the UK’s emerging approach, including the rising prominence of cyber operations, and the increasing size and ambition of each published strategy.

*The 2009 Strategy*

The UK government published its first National Cyber Security Strategy (NCSS) in 2009 (HM Government 2009a). This followed a wider trend, towards the end of a long period of Labour government (1997–2010), in which several national security documents and initiatives were created, including the first National Security Strategy (2008). Before the 2010 general election there was cross-party recognition that national security coordination needed to improve. The Brown government’s cyber security strategy is an example of that trend, which drew some inspiration from contemporary US practice (Devanny and Harris 2014). The UK’s first strategy was several years behind the US National Strategy to Secure Cyberspace (2003), and unsurprisingly behind the UK’s first counter-terrorism strategy (2003 – published in 2006). Cyber security has lagged counter-terrorism – and, indeed, other ‘cyber’ priorities such as intelligence collection – as a national security priority (Hannigan 2019, 10), and the UK often historically lags the US in national security transparency. In retrospect, 2009 was the start of a period in which cyber security was steadily elevated as a UK government priority, *vis a vis* both other cyber priorities and non-cyber priorities.

The 2009 strategy was relatively short (32 pages). It was much shorter than the government’s contemporaneous ‘Digital Britain’ report (HM Government 2009b) on the economic impact of digital technology that did not mention cyber security. The 2009 strategy’s subtitle indicated its priorities: ‘Safety, Security and Resilience’. It was co-published by two then relatively new institutions: the Cabinet Office’s Office for Cyber Security; and the Cyber Security Operations Centre, led by the cyber, signals intelligence and security agency, Government Communications Headquarters (GCHQ). One former top UK cyber official described the 2009 strategy, not unfairly, as a ‘scoping’ phase (Hannigan 2019, 3). This scoping phase had enduring impact, establishing the analytical foundations for subsequent strategies. Not all its reforms lasted, and its basic approach acknowledged – and left unchallenged – GCHQ’s primacy as the UK’s most cyber-capable institution. This remains true today, but GCHQ’s primacy is offset by the progress made by other institutions. Digital policy and regulatory responsibilities grew in other departments, such as the Department of Digital, Culture, Media, and Sport (and by 2023 the new Department for Science, Innovation and Technology). Successive strategies highlighted the Foreign, Commonwealth and Development Office’s (FCDO) growing role in cyber diplomacy, providing evidence that UK strategy is not monolithic, but is produced through institutional plurality.

The 2009 NCSS frames the problem of cyber security in high-level brushstrokes. It coined three priorities: reducing risk from the UK’s use of cyberspace; exploiting opportunities in cyberspace; and improving the underlying knowledge, capabilities, and decision-making necessary for successful strategy (HM Government 2009a, 3). The strategy obliquely mentioned the need to ‘intervene against adversaries… to exploit cyber space to combat threats from criminals, terrorists and competent state actors’ (HM Government 2009a, 4, 19). It, therefore, started to address the problems of governmental cyber security coordination. It identified the need to improve governance, capability, and doctrine as well as to facilitate the growth of an increasingly digital, secure, and resilient economy and society. Notwithstanding its enduring logic and analysis, the strategy’s impact was inevitably affected by the impending general election. In May 2010, the Brown premiership was replaced by a Conservative-led coalition government.

*The 2011 Strategy*

The Conservative-Liberal Democrat coalition government entered office determined to handle national security issues differently from its Labour predecessors in the context of controversy regarding the ‘war on terror’ and military operations in Afghanistan and Iraq. Under the coalition, cyber security became more prominent. This reflected the increasing salience of cyber operations in international security, e.g., with the first public reporting about Stuxnet (2010), Shamoon (2012), and Edward Snowden’s allegations about US and wider Five Eyes digital intelligence (2013). The UK government prominently featured cyber security in speeches, strategies, and initiatives. It was presented as an example, domestically, of the new government’s security credentials and investment and, internationally, of UK leadership in multilateral cyber diplomacy (e.g., the 2011 London Conference on Cyberspace). At a time of significantly reduced public expenditure under ‘austerity’ fiscal consolidation, cyber security benefited from a growing budget, innovations in coordination, and institutional reform.

The coalition’s 2011 NCSS should be interpreted within a wider, five-yearly framework of National Security Strategies (NSSs) and Strategic Defence and Security Reviews (SDSRs). Both the 2011 and 2016 Cyber Security Strategies followed the top-level priorities of this NSS/SDSR process. The coalition’s 2010 NSS identified cyber security as one of four top-tier risks, noting the UK’s ‘comparative advantage’ to achieve ‘economic and security opportunities’ in and through cyberspace (HM Government 2010a, 30). The SDSR highlighted the negotiation of a UK-US Memorandum of Understanding (MoU) to facilitate information-sharing and joint military cyber operations (HM Government 2010b, 48). The NSS/SDSR process overall committed to investing £650m over four years (eventually uplifted to £860m) in a new National Cyber Security Programme (NCSP). Almost two-thirds of this investment went to the intelligence agencies, primarily GCHQ (HM Government 2010b, 47; HM Government 2011, 25). Reform placed the Office for Cyber Security and Information Assurance, as well as (from 2013) the UK’s national Computer Emergency Response Team (CERT UK), under a Deputy National Security Adviser for Intelligence, Security and Resilience. The coalition further reshaped the cyber security institutional landscape, creating: a Joint Forces Cyber Group in the new Joint Forces Command (2012); a Joint Forces Cyber Reserve (2013); a Centre for Cyber Assessment (CCA) (2013); and a national CERT based in the Cabinet Office (2013–14).

The 2011 NCSS, we argue, should be understood as an effort to reshape – and to reshape the public narrative about – the governmental cyber agenda. It was slightly longer than its 2009 precursor and re-framed the UK’s top priorities as: tackling cyber-crime and being one of the most secure places in the world to do business online; improving resilience to cyber-attacks; helping shape an open, vibrant, and stable cyberspace to support open societies; and building UK cyber security knowledge, skills, and capability (HM Government 2011, 8). Its subtitle, ‘Protecting and promoting the UK in a digital world’ highlighted the strategy’s broad remit and multiple audiences. It was an exercise in explaining and promoting the UK’s agenda domestically and internationally. In continuity with the previous strategy, the 2011 NCSS: emphasized the need to collaborate with business and civil society to improve cyber security awareness and best practice; recognized the continuing need to build domestic cyber security capacity; and discreetly mentioned the requirement to develop sovereign capability ‘to detect and defeat high-end threats’ (HM Government 2011, 9). It also prominently embraced international engagement and the emerging field of cyber diplomacy, noting the London Conference to develop multilateral and multistakeholder ‘rules of the road’ for cyberspace.

Overall, the coalition government’s cyber strategy did not break fundamentally with the 2009 strategy. It continued the UK’s growing recognition of the need to improve national and international coordination to address cyber threats. It also demonstrated that senior figures in government perceived cyber security as a key component of a wider public narrative about security. In former GCHQ Director Robert Hannigan’s later assessment, the 2011–16 period highlighted the limits of what could be achieved with the existing approach. Its limitations showed the need for a more active, shaping role for government in cyber security (Hannigan 2019). This was an incremental shift, subsequently embedded in the 2016 NCSS.

*The 2016 Strategy*

At the 2015 general election, the Conservative party won an outright majority, ending the coalition and establishing the Conservatives as the sole party of government. In this context, the UK produced a new NSS/SDSR in 2015, providing a new framework for the next NCSS in 2016. However, the NCSS was published in November 2016, four months into Theresa May’s premiership, five months after the Brexit referendum that had led to Cameron’s resignation. Beyond the period’s unsettled domestic politics, there were likewise geopolitical changes, including continuing repercussions for European security of the 2014 Russian invasion of Ukraine. This was accompanied by the increasing salience of great power competition as an international security theme, especially in changing attitudes about how the UK and other states should address China’s rising power and influence. Each of these factors was bigger than cyber security, but each affected the way that the UK made and implemented cyber strategy.

The 2016 NCSS emerged in this new context. The government adopted a more active role, shaping the national effort to improve cyber security. It devoted more resources to cyber security, increasing the NCSP to £1.9bn. The 2016 creation of the National Cyber Security Centre (NCSC) was the new approach’s most prominent institutional manifestation. It provided more clarity, visibility, and leadership to the government’s cyber security agenda (Hannigan 2019). The strategy re-phrased the top national cyber priorities as defend, deter, and develop (HM Government 2016, 9). More streamlined than the four 2011 priorities, they closely followed earlier approaches, including the emphasis on cyber diplomacy (described as ‘international action’).

The NCSC amalgamated several precursor bodies, most prominently GCHQ’s information assurance arm (CESG), and the cyber aspects of the Centre for the Protection of National Infrastructure (CPNI), and absorbed newer entities, such as CERT UK and the CCA, created during the previous implementation period. Still formally part of GCHQ, the NCSC adopted a more public-facing profile. Its first Chief Executive, Ciaran Martin, was an articulate and visible cyber-security leader. This was an important part of the new approach, improving cyber security coordination across government, engaging with the private sector, and offering an internationally leading approach to cyber security organization.

This was a period of incremental progress towards what became (in 2020) the National Cyber Force (NCF). Its precursor entity, Defence-GCHQ collaboration under the National Offensive Cyber Programme (NOCP), progressed slowly through inter-institutional deliberations about how best to proceed (Devanny et al. 2021, 11–12; Blessing and Austin 2022, 30). The 2016 NCSS referred to cyber operations in a guarded manner, emphasizing that: ‘The principles of deterrence are as applicable in cyberspace as they are in the physical sphere... the full spectrum of our capabilities will be used to deter adversaries and to deny them opportunities to attack us’ (HM Government 2016, 47). Shortly before the NCSS’s publication, in September 2016 the UK and US finally signed the MoU first mooted in 2010. Shortly after that, both the UK and US commenced cyber operations against the so-called Islamic State group (Devanny et al. 2021, 11).

Despite the domestic political context (Brexit) and the wider geopolitical currents since the 2011 strategy, the 2016–21 implementation period saw a settled effort to build on previous strategies, creating new institutions like the NCSC and increasing funding of the NCSP. There were also increasingly public statements by government officials and ministers about the role of offensive capabilities in UK cyber strategy, and a commitment (in 2018, realized in 2020) to create the NCF (Devanny et al. 2021, 10–12). Indications of the shift towards ‘cyber power’ as a framing concept for UK strategy could be seen in these increasingly public mentions of cyber operations, as well as in the UK’s increasing ambition about the size of the NCF (from a proposed size of c. 500 in 2015 to a target of 2,000 personnel in 2018 and a 3,000 target in 2020). This was, arguably, reflective of growing global unease about cyber security threats, not least in the form of the wave of ransomware crime, and a need to demonstrate a capacity to respond more effectively than before.

*The 2022 Strategy*

The 2022 National Cyber Strategy (NCS) was published in December 2021, two years after Boris Johnson’s emphatic general election victory of December 2019 – and just six months before the end of Johnson’s turbulent premiership. Politically and geopolitically, Brexit, COVID-19, and the Russian invasion of Ukraine set the context in which this iteration of UK cyber strategy was developed and implemented. The NCS was also launched alongside growing public awareness of state hacking of IT supply chains following the SolarWinds (2020) and Microsoft Exchange (2021) incidents. The NCS likewise followed the Johnson premiership’s flagship national security strategy, the Integrated Review of Security, Defence, Development and Foreign Policy (UKIR) (HM Government 2021a).

The UKIR re-framed cyber strategy under five pillars: strengthening the UK cyber ecosystem; building a resilient and prosperous digital UK; taking the lead in the technologies vital to cyber power; advancing UK global leadership and influence; and detecting, disrupting, and deterring adversaries in and through cyberspace, ‘making more integrated, creative and routine use of the UK’s full spectrum of levers’ (HM Government 2021a, 41; HM Government 2021b, 11–13). Whilst the list is re-ordered and additional aspects are elevated compared to the 2016 NCSS, the top-level prioritization remains remarkably consistent with previous strategies. The NCS is more explicit than its precursors about the role of cyber operations in wider strategy, but with an important caveat that, to date, the UK had not achieved its intended deterrent outcomes with its adversaries (HM Government 2021b, 25). What is, however, less clear from reading the NCS and other UK statements is whether this implies that the UK thinks that more successful deterrence will come from new approaches to cyber operations, or from intensifying existing efforts.

The most notable change in the NCS was its replacement of cyber security – removed from the strategy’s title – with the new framing concept of cyber power. This was not a surprise development (Devanny 2021, 64). Cyber power had already appeared in speeches by senior UK officials, notably in a 2019 speech by GCHQ Director Jeremy Fleming (Fleming 2019). It then featured prominently in the UKIR. Even prior to the UKIR’s publication, Johnson had pre-announced that the NCF had attained operational capacity. The notional rationale for the NCS’s title change was to highlight that a national cyber strategy needed to encompass more than cyber security. As one commentator explained: ‘[the NCS] elevates the cyber domain from a security concern for technology specialists to a wide-ranging theme of grand strategy—one that will no longer be a “whole-of-government” initiative but will expand into a “whole-of-society” effort’ (Beecroft 2021).

The NCS describes cyber power as ‘an ever more vital lever of national power and a source of strategic advantage... [It] is the ability to protect and promote national interests in and through cyberspace’ (HM Government 2021b, 11). Evident in the UK’s understanding of cyber power is its capacity to be more than the deployment of cyber capabilities, extending to cyber diplomacy and capacity-building, as well as the contribution of digital technologies to national prosperity. This expanded view in the UKIR unfolds in a more complex, somewhat under-developed concept: ‘Responsible, Democratic Cyber Power’ (RDCP) (HM Government 2021a, 40). Regrettably, the UKIR did not precisely define RDCP. It interchangeably referred to RDCP and ‘responsible cyber power’ (the latter reminiscent of a common phrase in multilateral cyber diplomacy, ‘responsible state behaviour in cyberspace’). The precise definition of the ‘democratic’ element of RDCP is elusive throughout the UKIR (Devanny 2021). The short passage devoted to RDCP (HM Government 2021a, 40–42) implies that it is conceived principally as an operational concept. It states that the UK conducts responsible, targeted, and proportionate operations in cyberspace, in explicit contrast with its adversaries’ less responsible behaviour (HM Government 2021a, 42).

The NCS expands on the UKIR’s development of RDCP, developing its diplomatic aspects, combining the promotion of international stability, upholding the rules-based international order, and championing values such as ‘human rights, diversity, and gender equality’ (HM Government 2021b, 95). It likewise emphasizes collaboration ‘with like-minded nations to promote our shared values of openness and democracy’ (HM Government 2022b, 33). The NCS clarifies that cyber diplomacy, aimed at opposing ‘digital authoritarianism’ and defending citizens’ rights in cyberspace, including advocating ‘democratic values’ in international technology standards, is an important addition to RDCP’s emphasis on responsible operations (HM Government 2022b, 34, 88). RDCP’s expansion to include a wider range of foreign-policy objectives reflects the FCDO’s growing contribution to UK cyber strategy – evident in the significantly-increased size of its Cyber Policy Department (Center for Strategic and International Studies 2022).

Much of the Strategy’s first year of implementation was dominated by the Russian invasion of Ukraine, continuing efforts to address the ransomware crisis, and domestic turbulence across three successive premierships (Johnson, Liz Truss, and Rishi Sunak). This was not the ideal political context for stable stewardship of national strategy, but the mechanics of cyber strategy appeared (publicly, at least) to proceed largely unaffected. The UK’s rhetoric about RDCP was by now well-established, but there was still an open question about its longevity. It is reasonable to speculate about whether RDCP will long survive the mid-2023 retirement of Jeremy Fleming as GCHQ Director (Nicholls 2023) and how it would translate into a coordinated programme of action across government (e.g., cyber diplomacy led by the FCDO, cyber operations by the NCF). There was clear evidence of ongoing engagement and outreach to academia, industry, and other states, for example, in a Wilton Park conference sponsored by FCDO in November 2022 (Buchan 2022). This engagement fed into wider UK government efforts to develop a vision of RDCP in practice. But questions remained about how best to implement this vision and persuade other states of its merits. This is the subject of the final section.

# Translating Responsible, Democratic Cyber Power

The longevity of RDCP as a framing concept for UK cyber strategy will depend on whether it continues to be championed by advocates within government and whether it can achieve the (primarily international) objectives of UK strategic communications regarding its cyber strategy. The concept of RDCP is very broad and can serve multiple objectives. It entails the use of hard and soft power in pursuit of the ‘national interest’ (security, prosperity, values), manifesting both a ‘power-based’ and ‘rules-based’ approach to international security (Libicki 2021). Specifically, we suggest that the UK’s vision of RDCP can be summarized across four elements:

1. Integration of the UK’s cyber ecosystem, including sovereign assets, in the pursuit of the national interest.
2. Diplomatic efforts to shape the future of cyberspace in accord with national interests and democratic values, including through efforts to support cyber capacity-building.
3. ‘Operating responsibly’ through practising restraint, proportionality, and upholding applicable international law, rules, and norms.
4. Emphasizing liberal democratic processes of accountability and oversight (involving the executive, legislature, judiciary, and wider stakeholders), and including (a degree of) transparency about how these activities are enacted.

There are potential benefits, both domestic and international, from adopting a strategic narrative about RCDP. A recent example of shaping the public narrative domestically was GCHQ’s director, Jeremy Fleming, accepting (not without controversy) an invitation to be a guest editor of the BBC’s flagship current affairs programme, *Today* (Targett 2023). This suggests a calculation that the more visible and transparent the UK’s cyber actors become – by emphasizing their responsible and democratic attributes – the more public confidence and support there will be for their activities. Another example of this approach was the NCF’s publication in April 2023 of a document articulating the UK’s approach to offensive cyber operations and identifying three guiding principles of responsible cyber operations – accountability, precision and calibration (HM Government 2023, 14).

In this respect, the RDCP strategic communication campaign can be seen as a kind of insurance policy against the impact of possible future adverse headlines, e.g., of the Snowden variety. It is an example of pre-emptively, pro-actively shaping the conversation, rather than simply waiting to react in a crisis. For liberal democratic states, effective public communication is not just prudent but essential to accountability and oversight. RDCP also directly intersects with key government actors outside the realm of cyber security, whether in the setting of international technical standards, elaborating legal safeguards over foreign investment, or developing exports that promote interoperable standards embedding strong security and privacy.

However, it is the broader concept of cyber power – rather than its elaboration in RDCP – that underpins the coherence of this diverse range of UK government actors beyond cyber security. The success of RDCP will therefore depend on how effectively the different institutions within the UK government are coordinated internally – both through strategic narrative and policy development – to exert an active leadership role in driving the ‘whole-of-system’ agenda. Correctly calibrating RDCP’s bureaucratic politics will be crucial. It will require a clear sense of leadership and purpose. This is, of course, true of any cyber strategy, whether pursued under the umbrella of RDCP or another organizing principle.

RDCP’s prudential logic scales up internationally through cyber diplomacy. Developing a strong narrative about responsible and democratic behaviour could serve UK foreign policy by influencing ‘middle ground’ states beyond the like-minded group in multilateral cyber negotiations (HM Government 2021b, 94). Here, the ‘R’ and ‘D’ in RDCP clearly situate the UK against the behaviour in cyberspace of less responsible, less democratic adversaries. We argue that this was the original intention of departing from the more concise notion of ‘responsible state behaviour’ that is commonly associated with multilateral cyber diplomacy. In adding ‘democratic’, the UK implicitly criticizes the behaviour of those states that use cyber power in ways that undermine democracy and democratic values. It also enables the UK to develop a distinctive space between the few most powerful cyber actors and the many states with less capability. However, several commentators have noted that this is not an easy task, given concerns amongst other states over the potential impact and implications of, for example, the US strategy of persistent engagement (Shires and Smeets 2021). Likewise, some have noticed a latent tension between ‘cyber power’ and ‘cyber security’ as UK strategic priorities (Dwyer and Martin 2022).

RCDP faces challenges in how it can be effectively promoted as a model for other states to emulate. This is not a problem unique to RDCP. It reflects a context in which progress in cyber diplomacy is difficult, and states like the UK try to play an active, constructive role (Buchan and Devanny 2022). Put simply, the RDCP concept is only likely to succeed if the core concept of ‘cyber power’ is received favourably by the states it is intended to influence. If there is confusion about the UK’s references to ‘democratic’ uses of cyber capabilities, or allergic reaction to the language of ‘power’ in the rhetoric of persuasion, then RDCP might need to be reconsidered. Ultimately, the objectives of UK strategy could be pursued under the more traditional rubric of cyber diplomacy – ‘responsible state behaviour in cyberspace’. Why would other states, seeking to promote the norms-based order in cyberspace, embrace RDCP?

The answer implicit in RDCP is that states could find in it a foundation to engage internationally and to allay any fears that the avowal (by the UK and other states) of offensive cyber capabilities is tantamount to militarizing cyberspace. Yet, the translation of RDCP for other states to embrace raises at least three issues. First, RDCP, like the broader concept of cyber power, is contested and difficult to quantify (Voo, Hemani, and Cassidy 2022). States possess diverse interpretations of what ‘responsibility’ and ‘democracy’ mean in the context of international security. This would make assessing RDCP across states – if it were widely adopted – exceptionally difficult. Second, given that the political independence of states is a fundamental precept of international relations, it is not obvious that the ‘democratic’ element of RDCP improves upon the more concise, more established, and less domestically prescriptive UN concept of ‘responsible state behaviour in cyberspace’. As Johanna Weaver has noted, in cyber diplomacy most states are more preoccupied with international stability than with liberal democratic values. Consequently, it arguably makes more diplomatic sense to carefully calibrate the extent to which UK diplomacy prioritizes concentration on the impact of state behaviour on international stability, rather than on the promotion of democratic values (Weaver 2022). The interchangeable language of the UKIR regarding RDCP and ‘responsible cyber power’ perhaps suggests that the UK recognizes this nuance. Notably, perhaps, the NCF’s recent publication follows this approach, referring to RDCP in the body of the document but to ‘Responsible Cyber Power’ in its title. This could suggest an on-going refinement of the UK’s strategic communications and use of the RDCP concept. Finally, third, there is some real doubt about whether ‘power’ is a useful trope of cyber diplomacy, in that it could potentially alienate some states which might perceive their own lack of power or powerlessness (Buchan 2022). Might the rhetoric of cyber power be counterproductive for UK policy? It is possible that UK strategy would be better articulated by placing greater emphasis on the UK’s cooperative, collaborative role as a partner to many states in global cyber diplomacy, pursuing the incremental gains of quiet leadership in cyber diplomacy and capacity building. This approach might be more attractive and successful diplomatically because it is softer – selling the benefits of what the UK has to offer as a partner, rather than emphasizing the image of its strength as a ‘power’. Such a critique echoes in some ways the debates about and reception of the ‘responsibility to protect’ (R2P) (Crossley 2018). RDCP could even be interpreted – although this interpretation moves beyond the UK’s explanation of the concept – to suggest that states have an obligation to use cyber operations to protect populations, or to pursue collective countermeasures. Such implications are likely to appeal to some states more than others (Buchan and Devanny 2022).

Whatever its rhetoric and choice of framing concept for strategic communications, the UK is committed to an active, international cyber strategy: engaging in multilateral (and promoting multistakeholder) efforts to shape global norms of responsible behaviour in cyberspace; providing, funding and sharing best practice regarding cyber capacity building; and working to ensure that regulations and standards for next-generation technologies work for democracies and do not benefit illiberal, authoritarian states. It cannot match the scale of US cyber operations – and it will continue to work as closely as possible to align its operations with those of the US and other allies. Nonetheless, the UK is making a significant investment in offensive cyber operations, offering its growing capability to NATO under Article V and via the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism (Devanny et al. 2021, 16). Cumulatively, you might say that this classifies the UK as an ‘upper-middle power’ in the arena of global cyber cooperation, competition, and conflict. The case study of RDCP demonstrates that the UK is self-aware about the potential latent in its national combination of active diplomacy, convening power, and thought leadership, alongside the hard power of its cyber capabilities. Its advocacy of RDCP could be seen as one interpretation – amongst many – of how the UK should play these cards on behalf of the rules-based international order, the promotion of stability, democratic values, and, of course, its national interest. It offers one – to date under-elaborated – model for other ‘middle power’ states to follow.

# Conclusion

Published national cyber strategies serve an important function in strategic communication and public diplomacy. They are an opportunity to demonstrate transparency, persuade diverse audiences, and shape opinion. They can also be a ‘fudge’ – a compromise between different institutional actors, reflecting their respective equities and viewpoints. Four iterations of UK cyber strategy have effectively elevated the priority of cyber security in public debate and have explained for multiple audiences the key points of UK strategy. Since 2009, the UK has maintained a broadly consistent focus on developing its national cyber ecosystem, improving cyber security, and developing its resilience. The rise of (responsible, democratic) cyber power as the framing concept of UK cyber strategy embraced two developments in particular – the rising salience of cyber operations as a publicly-avowed aspect of state strategy, and recognition of the relevance and role of other stakeholders (and increasingly inter-state geopolitical competition).

This article has provided an overview of RDCP’s emergence as the UK’s new umbrella concept for cyber strategy. It identifies the major challenges facing RDCP, particularly in terms of its international appeal. This is consequential, as RDCP is best interpreted as a framework for translating cyber power for cyber diplomacy, not as a structuring concept for the domestic elements of UK cyber strategy. The language of ‘power’ poses difficult questions for medium-sized states engaging in cyber operations whilst upholding the increasingly challenged rules-based international order. The evolving interpretation of RDCP indicates that it is still a fluid concept. Its next steps are still to be determined three years after UK officials first publicly invoked ‘cyber power’. The reception of the NCF’s recent document on Responsible Cyber Power will likely help to shape the next phase of this process. The durability of the ‘democratic’ element may be limited. It presents challenges and perhaps restricts RDCP’s appeal in international engagement. The focus on ‘responsibility’ may better serve UK objectives and align more closely with wider international discourse about responsible state behaviour in cyberspace. The longevity of the RDCP phrase is therefore much less significant than the effectiveness of the underlying diplomacy, policy, and operations encompassed by it.

Acknowledgements

We thank our colleagues – and fellow researchers in other institutions – from whom we have benefited in discussing UK cyber strategy. We are immensely grateful for the constructive feedback provided by the CyCon reviewers, and also to those practitioners who have engaged with us and other academics in discussing UK strategy. Joe Devanny is also grateful to the British Academy for the Innovation Fellowship during which he was able to undertake this research.

References

Beecroft, Nick. 2021. ‘The UK’s Cyber Strategy Is No Longer Just About Security’. Carnegie Endowment for International Peace. 17 December 2021. https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security-pub-86037.

Betz, David and Tim Stevens. 2011. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge for the International Institute for Strategic Studies.

Blessing, Jason and Greg Austin. 2022. *Assessing military cyber maturity: strategy, institutions and capability*. London: International Institute of Strategic Studies.

Buchan, Russell and Joe Devanny. 2022. ‘Clarifying Responsible Cyber Power: Developing Views in the U.K. Regarding Non-intervention and Peacetime Cyber Operations’. *Lawfare Blog*, 13 October 2022. https://www.lawfareblog.com/clarifying-responsible-cyber-power-developing-views-uk-regarding-non-intervention-and-peacetime.

Buchan, Russell. 2022. ‘Summary Report: Acting responsibly in cyberspace WP3146’. FCDO/Wilton Park. 14–16 November 2022. [https://www.wiltonpark.org.uk/app/uploads/2023/01/WP3146-Summary-Report-Acting-Responsibly-in-Cyberspace-Nov-2022-1.pdf](https://www.wiltonpark.org.uk/wp-content/uploads/2022/11/WP3146-Summary-Report-Acting-Responsibly-in-Cyberspace-Nov-2022.pdf).

Center for Strategic and International Studies. 2022. ‘Placing Cyber Diplomacy at the Top of the Agenda’. *Inside Cyber Diplomacy*, 15 August 2022. <https://www.csis.org/node/66558>.

Crossley, Noele. 2018. ‘Is R2P Still Controversial? Continuity and Change in the Debate on “Humanitarian Intervention”’. *Cambridge Review of International Affairs* 31(5): 415–36. https://doi.org/10.1080/09557571.2018.1516196.

Devanny, Joe and Josh Harris. 2014*. The National Security Council: National Security at the Centre of Government*. London: Institute for Government.

Devanny, Joe, Andrew Dwyer, Amy Ertan, and Tim Stevens. 2021. *The National Cyber Force that Britain Needs?* London: King’s Policy Institute, Cyber Security Research Group and UK Offensive Cyber Working Group.

Devanny, Joe. 2021. ‘The Review and Responsible, Democratic Cyber Power’. In *The Integrated Review in Context: Defence and Security in Focus*, edited by Devanny, Joe and John Gearson, 62–64, London: Centre for Defence Studies.

Dwyer, Andrew and Ciaran Martin. 2022. ‘A Frontier Without Direction? The U.K.’s Latest Position on Responsible Cyber Power’. *Lawfare Blog*, 1 August 2022. https://www.lawfareblog.com/frontier-without-direction-uks-latest-position-responsible-cyber-power.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford: Oxford University Press.

Fleming, Jeremy. 2019. ‘Director’s Speech on Cyber Power – As Delivered’. GCHQ. 25 February 2019. <https://www.gchq.gov.uk/speech/jeremy-fleming-fullerton-speech-singapore-2019>.

Hannigan, Robert. 2019. *Organising a Government for Cyber: The Creation of the UK’s National Cyber Security Centre*. London: Royal United Services Institute (RUSI).

Harknett, Richard J. and Max Smeets. 2022. ‘Cyber Campaigns and Strategic Outcomes’. *Journal of Strategic Studies* 45(4): 534–67.

Healey, Jason, ed. 2013. *A Fierce Domain: Conflict in Cyberspace 1986–2012*. Arlington, VA: Cyber Conflict Studies Association (CCSA).

HM Government. 2009a. *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space (Cm 7642)*.

HM Government. 2009b. *Digital Britain: Final Report (Cm 7650)*.

HM Government. 2010a. *A Strong Britain in an Age of Uncertainty: The National Security Strategy (Cm 7953)*.

HM Government. 2010b. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review (Cm 7948)*.

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

HM Government. 2016. *National Cyber Security Strategy 2016–21.*

HM Government. 2021a*. Global Britain in a Competitive Age: The Review of Security, Defence, Development and Foreign Policy (CP 403).*

HM Government. 2021b*. National Cyber Strategy.*

HM Government. 2023. *The National Cyber Force: Responsible Cyber Power in Practice*.

Kavanagh, Camino. 2017. *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*. Geneva: United Nations Institute for Disarmament Research.

Kramer, Franklin D., Stuart Starr, and Larry K. Wentz, eds. 2009. *Cyberpower and National Security*. Washington, DC: National Defense University Press.

Libicki, Martin. C. 2021. Obnoxious Deterrence. *14th International Conflict on Cyber Conflict: Keep Moving*. Tallinn: NATO CCD COE, 65–77.

Lindsay, Jon R. 2021. ‘Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem’. *Intelligence and National Security* 36(2): 260–78.

Maschmeyer, Lennart, Ronald J. Deibert, and Jon R. Lindsay. 2021. ‘A Tale of Two Cybers – How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society’. *Journal of Information Technology & Politics* 18(1): 1–20.

Nicholls, Dominic. 2023. ‘Spy Chief Sir Jeremy Fleming to Step Down as Director of GCHQ’. *Telegraph*, 26 January 2023. https://www.telegraph.co.uk/news/2023/01/26/sir-jeremy-fleming-step-director-gchq/
Nye, Joseph S. 2010. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs.

Shires, James and Max Smeets. 2021. ‘The U.K. as a Responsible Cyber Power: Brilliant Branding or Empty Bluster?’ *Lawfare Blog*, 23 November 2021. https://www.lawfareblog.com/uk-responsible-cyber-power-brilliant-branding-or-empty-bluster.

Smeets, Max. 2022. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. London: Hurst.

Targett, Ed. 2023. ‘Opinion: GCHQs’ Director Should not Be Playing Guest Editor on the BBC’. *Stack*, 3 January 2023. <https://thestack.technology/gchq-director-sir-jeremy-fleming-bbc-today-programme/>.

Valeriano, Brandon, Brian Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion.* Oxford: Oxford University Press.

Voo, Julia, Irfan Hemani, and Daniel Cassidy. 2022. *National Cyber Power Index 2022*. Cambridge, MA: Belfer Center for Science and International Affairs.

Weaver, Johanna. 2022. ‘The Rules-Based International Order: Some Hard Truths’. Keynote presented at the 14th International Conference on Cyber Conflict: Keep Moving (CyCon 2022), Tallinn, Estonia. https://www.youtube.com/watch?v=O8eFiJaNzRU&ab\_channel=natoccdcoe

Willett, Marcus. 2019. ‘Assessing Cyber Power’. *Survival* 61(1): 85–90.

1. We use cyber operations to encompass a range of activities that are sometimes referred to as ‘offensive’ but may not be exclusively characterized as such. [↑](#footnote-ref-2)