ARI 18/2021
9 February 2021

The National Cyber Force: Directions and Implications for the UK

Danny Steed | Cyber Security & Intelligence Research Fellow, The Henry Jackson Society | @TheSteed86

Theme

The establishment of the National Cyber Force (NCF) raises significant questions about the directions that the cybersecurity of the United Kingdom will now take, and what the implications are.

Summary

The creation of the National Cyber Force (NCF) is a new watershed in British cyber capability. Signalling a clear intent to carry out offensive cyber operations, the NCF raises questions about the direction of British cyber strategy moving ahead. Examining the implications of the NCF, this ARI details some of the key legislative, doctrinal, and strategic challenges that need to be resolved by policymakers.

Analysis

The establishment of the UK's National Cyber Force (NCF) in November 2020 can easily be viewed from two perspectives: as a dramatic step change in UK cyber, an aggressive leap forward from previously more passive and reactionary strategies. Or, as a logical next step following the earlier standing up of the National Cyber Security Centre (NCSC) in 2016, simply 'the culmination of a process' and an inevitable progression of a maturing cyber security strategy evident since at least 2013.[1] Whatever perspective observers take, what is clear is that the NCF raises significant questions about the directions UK cyber security will now take, and what the implications are.

This article will address a series of broader questions about the NCF to identify some of the implications that UK policy must consider. First are the legislative concerns, particularly the balance between operating under legislation governing the intelligence services and concerns about international law. Second, the implications of cyber warfare increasingly being dominated by the intelligence services raises significant questions for the UK. Thirdly, how does UK cyber doctrine develop? Squaring the ever-closer operation of UK military forces with intelligence services marks a departure for doctrine. Finally, what does the establishment of the NCF say for the future of cyber security strategy and national policy?

[1] Conrad Prince, "On the Offensive: The UK's New Cyber Force", *RUSI*, November 23, 2020.

The lack of declared forward thinking in UK policy raises some concerns, in this author's opinion. The establishment of a major new component of UK intelligence/military capability with little political or public debate seems on face value to have left unresolved a large number of implications that will be faced in operational practice. UK cyber policy and strategy will need to find answers to many issues, lest it finds itself driven by cyber practice, rather than cyber practice being a subservient tool of policy.

The National Cyber Force

On Thursday 19th November 2020, Prime Minister Boris Johnson announced a large investment into UK defence capabilities, an injection of £16.5 billion over a four-year period. Included in the statement was the announcement of a new Space Command, and the National Cyber Force, who 'will disrupt terrorists, hostile state activity and criminals and transform the UK's cyber capabilities.' [2] Initial estimates are that the NCF has £250 millions of funds from the announced investment, with £76 million to be used in its first year of operations.[3] The strength of the NCF is hoped to reach 3,000 personnel within a decade, although it is not clear what balance of staffing will be drawn from GCHQ and the UK military.[4]

In their own release, the parent agency of the NCF –the Government Communications Headquarters (GCHQ)– issued several hypotheticals to illustrate the type of work the NCF can be expected to engage in. These include interfering with the mobile devices of terrorists; preventing the exploitation of the internet for use by serious crime, such as child exploitation and fraud; protecting UK military assets from cyber interference.[5] Given the noted increase in NCSC activity year on year –announcing it had dealt with 723 serious cyber incidents in its most recent annual report[6]– there is little doubt of the need for further UK capability in cyber to be developed.

The emphasis is clear, where the NCSC is tasked to provide and lead on domestic resilience to cyber incidents, the NCF is to engage on offensive cyber operations. This itself raises a curious dimension, as all things offensive cyber have been resolutely classified. The rule is reminiscent of the cult favourite movie *Fight Club*, where rule number one about offensive cyber is we do not talk about offensive cyber. The only such campaign to have been publicly acknowledged was by GCHQ in 2018, who took measures to actively disrupt and suppress the online propaganda effort by so-called Islamic State.[7]

[2] Ministry of Defence, "Defence secure largest investment since the Cold War", November 19, 2020.

[3] Toby Morbin, "UK Forms National Cyber Force", *Bank Info Security*, November 20, 2020.

[4] Matt Burgess, "The UK created a secretive, elite hacking force. Here's what it does", *Wired*, November 11, 2020.

[5] GCHQ, "National Cyber Force transforms country's cyber capabilities to protect the UK", November 19, 2020.

[6] National Cyber Security Center, "The NCSC Annual Review, 2020", November 3, 2020.

[7] Helen Warrell, "National Cyber Force will target UK adversaries online", *The Financial Times,* November 19, 2020.

With official releases offering little more information that the above, one must assume that further guidance will be provided in the imminent Integrated Defence Review, and the next generation of National Cyber Security Strategy, due later this year. But this is a big assumption to make, previous strategies and SDSR's in the UK have, at their worst, offered little more than a capital project shopping list for the UK military, and the blandest of policy direction at the strategic level.

Practical experience in the operational world has given UK cyber capability much to learn from in its various guides over the past decade. Instead of waiting (and hoping) for top level guidance, it is necessary to explore the implications that the NCF is sure to encounter in practice. These are implications that UK policy will have to find reconciliations and answers to, that is if policy wishes to establish a firm grip on the UK's future vision for cyberspace, rather than be led by the endless cycle of innovations in practice, whether benign or malevolent.

Implication 1: Legislative

While the NCF is said to operate strictly within legislative parameters, the statutes in question reveal much about the challenges that may be faced. Operating under the purview of the Intelligence Services Act (1994)[8] and Investigatory Powers Act (2017) provides the NCF with potentially sweeping powers both internationally and domestically.[9]

The ISA bill has historically been viewed as simply recognising the Secret Intelligence Service (SIS/MI6) and GCHQ on a legal basis for the first time and declaring ministerial oversight channels – though not direct Parliamentary ones – via the Intelligence and Security Committee (ISC). Akin to the criticisms levelled against the Security Services Act (1989),[10] such statute can be argued as being 'largely a cloak draped over an unchanged figure, not intended significantly to disturb existing working relationships.[11] Importantly in this context, however, is the line of ministerial responsibility this governing statute implies, for in theory the NCF should be answerable to the Foreign Secretary for its operations.

Should the NCF be operating in a domestic capacity – for example, to follow the hypothetical case offered of disrupting domestic terrorist activity or serious crime – it will follow the IP bill's procedure governing warranty. This split reveals the "wicked problem" faced by those operating in the cyber domain, that statutory provisions and ministerial oversight channels will be routinely difficult to follow in practice. With operations constantly criss-crossing domestic and foreign operations, utilising military personnel and capability as routine, there will be a need for UK policymakers to regularly review the legal challenges that NCF operations pose.

[8] The National Archives, Intelligence Service Act 1944*, Legislation.gov.uk*.

[9] The National Archives, Investigatory Powers Act 2016*, Legislation.gov.uk*.

[10] The National Archives, Security Services Act 1989*, Legislation.gov.uk*.

[11] Laurence Lustgarten and Iain Leigh, *In from the Cold: National Security and Parliamentary Democracy*, Oxford: Clarendon Press, 1994, p. 424.

David Omand warns that the production of intelligence 'involves overcoming constant friction in the system.'[12] This relates not only to the operational pressures of intelligence and military pursuits, but so too to the inherent dynamics of permitting secret operations in the name of security while balancing the appropriate level of intrusion on civil liberties. How policymakers review and debate the effects of the NCF in practice will go far in revealing how attuned the UK is shaping a safer cyberspace, but also how the ethics and proportionality of our own cyber operations evolve.

Implication 2: Intelligence-led warfare?

Debates about "way of war" are common on history and War Studies courses, with veritable mountains of literature assessing a national style or strategic culture that shapes its warfighting.[13] If cyber practice since 2015 is any guide, then the British way of cyber war will be led by its intelligence services. The establishment of the NCSC in 2016 under the parenthood of signals intelligence service GCHQ was ostensibly due to GCHQ's undisputed technical mastery standing them out for the role. This decision, however, carries larger questions about the British way in cyber warfare as it will no doubt be waged by NCF under the same organisational parenthood.

First, UK policymakers will need to understand that the mission of the intelligence services is growing, with a key issue to be tackled. Are our intelligence services meant to operate in their traditional guise, as passive gatherers of secret information on which to inform security decisions? Or are they now also expected to act and engage in our own "grey zone operations" in extremely fluid, fast moving situations?

This is a question worthy of public debate, for while it may appear merely semantic in nature, readers would be wise to note that many of the greatest intelligence controversies have stemmed from their movement into the realm of covert action, often with disastrous results. From the American perspective, the Church Committee hearings of the 1970s were held precisely to reign in reckless covert operations believed to have crossed legal and ethical boundaries.[14] In the UK, there is long history of successful and disastrous covert or special operations,[15] ranging from daring Special Operations Executive sabotage missions in the Second World War, to the disasters of SIS/MI6 attempted operations during the 1956 Suez Crisis.[16]

[12] David Omand, *Securing the State,* London: Hurst & Co., 2010, p. 262.

[13] That literature is far beyond the scope of this article, but a worthy yet brief introduction lies with Colin S. Gray, "Strategic culture as context: the first generation of theory strikes back", in Colin. S. Gray, *Strategy and History: Essays on theory and practice,* Abingdon: Routledge, 2006.

[14] U. S. Senate, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Services, 1975-1976.

[15] The best general history of which is the outstanding Rory Cormac, *Disrupt and Deny: Spies, Special Forces and the Secret Pursuit of British Foreign Policy,* Oxford: OUP, 2018.

[16] See this author's own extensive history of such operations, Danny Steed, *British Strategy and Intelligence in the Suez Crisis,* London: Palgrave Macmillan, 2016.

By placing GCHQ as the tip of the spear for offensive cyber operations, Britain has made a declaration that when cyber warfare is carried out it will be led by intelligence services, under intelligence statutes. There is not only the discussion to be held about the nation's long-term strategic culture in cyberspace, but also the consideration of how far we change the face of our intelligence services themselves. How far do we position our spies as agents of disruption – if not *agent provocateurs'* – to the expense of their traditional mission, to speak truth to power and provide secret information to help policy decisions?

The UK runs the very real risk of contributing to an ever-accelerating securitisation of cyberspace, hastening the fractures of the free and open internet we have long pledged to defend and uphold. As former NCSC CEO Ciaran Martin said in a recent speech, there is no separation between military cyberspace and civil cyberspace: 'It's the same domain.' And as Professor Martin concludes his speech, 'We militarise the Internet at our peril.'[17] Reconciling intelligence-led offensive cyber with our ambitions to ensure the free and open internet is a challenge that can only be addressed by elected representatives in Whitehall, not the spies housed at Cheltenham.

Implication 3: UK cyber doctrine

Closely linked to implication 2 above, the ever-closer synergy between military and intelligence capabilities raises questions about UK military doctrine, which has been trying to come to terms with all things cyber over the past decade. There is a specific dilemma to solve, does UK military doctrine lead the NCF, or will it be led entirely by GCHQ?

This is no trivial matter, for it shapes immensely the direction of UK military forces in cyberspace. If the answer lies with the latter, then UK military doctrine can focus on a purely defensive aspect to safeguard and ensure the integrity of its own information operations, leaving offensive operations purely to the NCF. For an analogy, it would place the UK military in the same place as the US Marine Corps regarding its airpower doctrine; as the US Air Force leads on aerial dominance or superiority operations, the US Marine Corps can focus its air assets very closely to its own force structure and intention.[18] The UK military would in this scenario cede authority to GCHQ on cyber warfighting, playing a support role to intelligence-led operations and campaigns.

If the former, then the Development, Concepts, and Doctrine Centre (DCDC) have much to do in building on publications like the Cyber Primer[19] and Information Advantage[20] respectively.

The direction the former would need to take would be an elaboration on how the UK military carries out warfighting cyber operations, exploring the interface with intelligence services, but also very clearly establishing lines of responsibility between the NCF and

[17] Ciaran Martin, "Cyber weapons are called viruses for a reason: Statecraft and security in the digital age", transcript of speech delivered at King's College London, November 10, 2020, pages 3 and 14 respectively.

[18] US Marine Corps, *MCWP 3-2 Aviation Operations*, May 9, 2000.

[19] MoD, *Cyber Primer*, 2nd Ed., July 26, 2016.

[20] MoD, *JCN 2/18 Information Advantage*, September 9, 2020.

UK military units. Given what is known about the NCF so far, this former scenario appears less likely. The UK military is not prepared conceptually or organisationally to become an effective force in this regard. Yet the lack of doctrinal clarity introduces this very uncertainty on where conceptual thought leadership will come from.

What is clear is that wherever concepts and doctrine for offensive cyber come from, the culture of over classification needs to be addressed. This is to ensure rigorous debate in practitioner and policymaking circles as well as, where possible, public debate. Former NSA Director Michael Hayden has expressed his concern that cyber capabilities are classified too far, preventing properly informed policy debate about their place in national strategy,[21] this is a problem in the UK as well.

The logic in this regard is simple, consider the UK's nuclear deterrent as a key example. It is well understood what aspects of the programme must remained classified, from details about warhead trigger technology, to performance data regarding the Trident missiles or *Trident* class submarines themselves. What is not classified is the need for open, public debate regarding the place of the nuclear deterrent in British defence in its own right. This is a debate that has been through numerous cycles without compromising the essentials aspects of secrecy where secrecy is needed.

The same needs to be established with offensive cyber operations. Clearly, details regarding exact NCF unit sizes, locations, and technological capabilities need to remain secret, as well as details of ongoing operations and target lists. What needs to be opened up for wider debate, mostly confidential but also in places publicly, is discussion around the capability itself. This is precisely to address some of the concerns already raised in this article, but also to ensure a well-informed policy audience on the role of the NCF itself. Ciaran Martin has reiterated his concern that 'there is still too often, very loose language reflecting a profound lack of understanding of the capabilities we are talking about.'[22] If offensive cyber remains perennially over classified, we can never expect our policymakers to engage in informed debate about its place in UK national security.

Implication 4: The NCF in national strategy

With the NCF being announced ahead of both the Integrated Defence Review and the National Cyber Security Strategy, it remains to be seen whether the place of the NCF will be further elaborated in either. This author would very much expect the NCF and the place of offensive cyber in broader UK strategy to be in both documents, should they not then it will be proof positive of a conceptual black hole in British cyber strategic thought.

The Integrated Review must seek to answer the place of UK military operations in line with the NCF and the interface with the intelligence services, establishing clear guidance on which doctrine can be developed. The National Cyber Security Strategy must answer a far bigger question, namely how does the UK ensure the delicate balance between its

[21] Michael Hayden has repeated this opinion in many outlets, but perhaps most memorably during his interview for movie documentary *Zero Days,* Dir. Alex Gibney, Jigsaw Productions, 2016, Film.

[22] Ciaran Martin (2020), p. 5.

ability to defend itself versus compromising the very shared domain in cyberspace we are striving to keep free and open?

Answering this will require a policy vision on which the operations of intelligence services and military units can usefully serve. Strategy is not to be seen as a corporate brochure exercise, producing near tautological phrases as is routinely witnessed across government; strategy must meaningfully connect the actions of our security actors to declared political intent. Without a policy vision, any strategy is inherently without a reference point to serve.

British policymakers must do better in this regard, being led by the technical expertise of GCHQ or the wisdom of the UK military cannot make up for a lack of vision for the type of cyberspace that the UK seeks to shape in the decades to come. It is policy vision that frames the mission that units like the NCF will face. National level strategy must not be seen as a mere budgetary exercise, but instead as a blueprint for the desired future the UK wishes to see in cyberspace. If our policymakers fail to do this, it will find itself in a reactionary state, shaped more by the escalating practices of the NCF engaging with its adversaries than it is by rational political guidance. This would be a dangerous position for the nation to find itself in.

Conclusions

To conclude, the establishment of the NCF is a new watershed moment in the development of UK cyber capability. It is a clear statement of intent from the UK that it will conduct offensive cyber operations, building on its main effort since 2016, the establishment of the NCSC and domestic resilience to cyber-attack. Yet, the NCF raises as many questions as it answers, especially regarding the implications legislatively, in our strategic culture for warfighting in cyberspace, our doctrinal expectations, and how it will be directed by national strategy.

The lack of public debate about offensive cyber in almost any capacity, and the launch of the NCF prior to the Integrated Review and next National Cyber Security Strategy, shows that major changes are taking place with very little debate. This must change, the full implications of the NCF have yet to be examined in detail. With the UK establishing long-term structures for warfighting in cyberspace, much greater effort in strategic direction, conceptual clarity, and political vision needs to be established to ensure that the NCF remains a tool in the service of British political aspirations, rather than British policy playing catch up to the tactical cat-and-mouse game being led increasingly by our spies.