CYBER SECURITY RESEARCH GROUP

OFFENSIVE CYBER WORKING GROUP

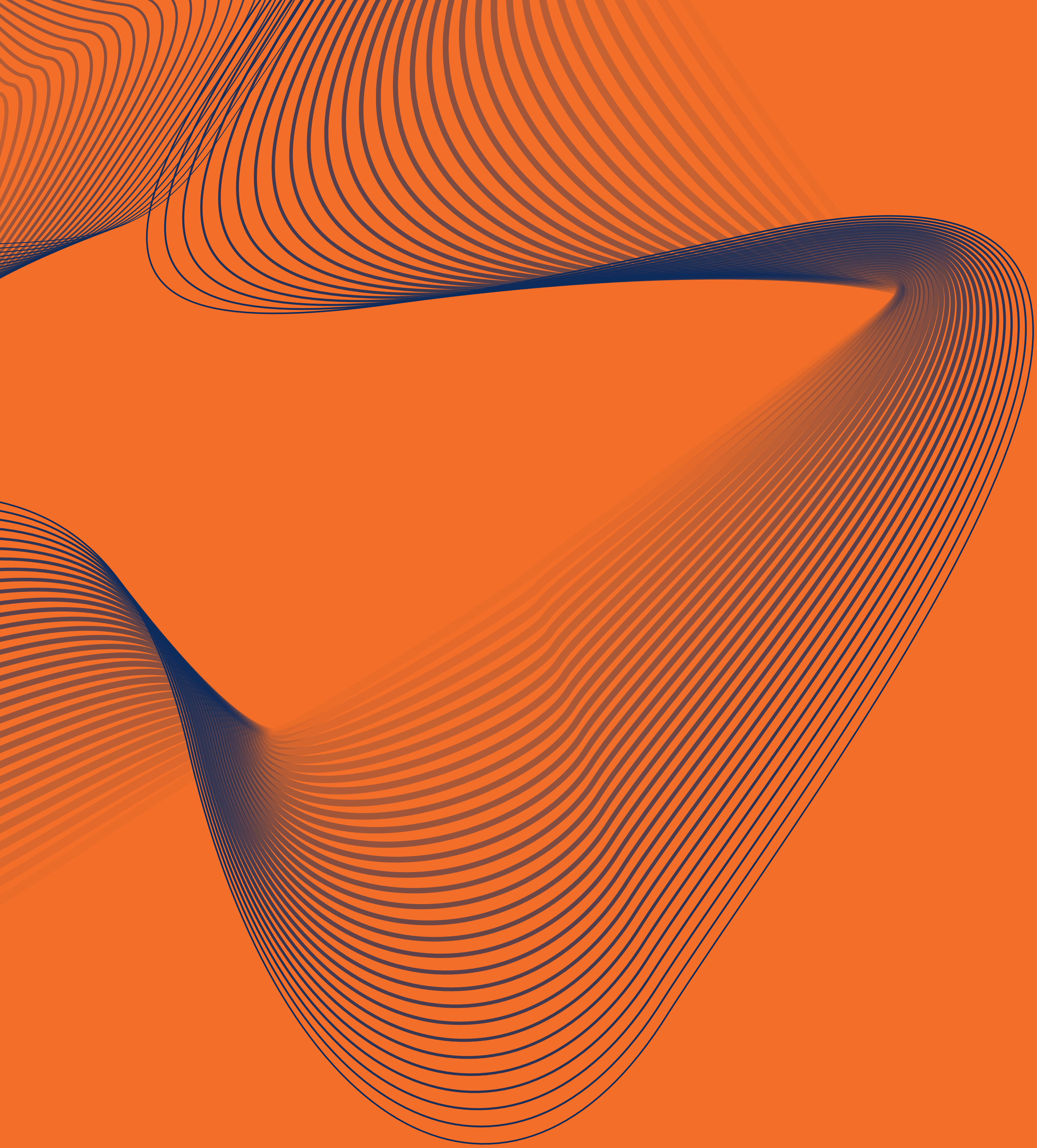
THE POLICY INSTITUTE

KING'S College LONDON

The National Cyber Force that Britain Needs?

Joe Devanny, Andrew Dwyer,
Amy Ertan and Tim Stevens

April 2021



Foreword

By **Ciaran Martin**
Professor of Practice in the Management of Public Organizations, University of Oxford and founder of the UK's National Cyber Security Centre, part of the intelligence agency GCHQ

The development of offensive cyber capabilities and organisations to deploy them is one of the most strategically significant issues facing governments as they come to terms with the technological revolution.

Offensive cyber raises profound challenges and choices of statecraft for governments everywhere in at least three different ways.

First is what it says about a nation's strategic posture towards the internet. In what circumstances, and for what purposes, should governments exploit the online weaknesses of others? When should online information gathering – digital espionage – give way to active disruption? In a networked world, what impact does this activity have on our own cyber security and is there a trade-off between exploiting vulnerabilities in others and protecting your own citizens?

Second, how is such sensitive, risky and contentious activity governed? What does being a "democratic, responsible cyber power", as the UK government asserts it is, mean, and who decides that? How do governments ensure their activities are responsible, and don't promote instability and accidental harm on the internet? How does a lawful, democratic state gain informed public consent for what will often invariably be secretive operations?

Finally, how is offensive cyber organised and run? Who is responsible for ensuring a realistic and deliverable set of capabilities in an area prone to hype? What should be the respective roles of intelligence, military and law enforcement? How do the long-standing Five Eyes intelligence partnerships, and newer partnerships with other countries, adapt to these new capabilities? How does political oversight work, and who is at the table to speak for cyber security and internet safety when offensive cyber is being discussed? And how does a nation ensure it has the right human capital – the leadership and skills – to deliver the objective?

The UK's recent emphasis on offensive cyber in its Integrated Review of Defence, Security, Foreign and Development Policy, as well as the establishment of the National Cyber Force, means that it is imperative that Britain debates these issues. But the topic has received far too little public attention. That's partly because the necessary operational secrecy around offensive cyber has afforded some protection from the normal mechanisms of scrutiny as policy has developed. But there is no good reason why the operating environment, the policies, the oversight, and in particular the strategic posture, cannot be openly debated. That is why this report from four outstanding scholars of cyberspace is so welcome.

Ultimately, the UK will have to account for its actions as an actor in cyberspace in all of these areas, and this excellent paper provides a crucial framework for how that should be done. It correctly concludes that the security of domestic cyberspace should retain primacy, and sets out a clear, hard-headed account of how the many challenges facing those tasked with building the National Cyber Force might be addressed. It is essential reading for anyone interested in the UK's activities in cyberspace.

Executive summary

Cyber operations are increasingly important to state power projection in the contested and competitive defence and security environments of the globalised 21st century. The United Kingdom has created a National Cyber Force (NCF) to assist in its ambitions to conduct offensive operations against hostile state actors, terrorists and serious organised criminals. This joint military-intelligence organisation will replace and streamline existing arrangements and will help the UK achieve full-spectrum effects in pursuit of detecting, disrupting and deterring its adversaries. The NCF is intended to be a key contributor to the UK's desire to be an effective, responsible and democratic "cyber power" in global affairs. The broad remit of the NCF was outlined by the UK government in March 2021, but questions remain about the NCF's role, responsibility, organisation and mission. This report identifies a set of core themes for the UK government to consider as the NCF begins its work as the spearhead of a revised and more proactive UK approach to adversaries in cyberspace.

> "Cyber operations are increasingly important to state power projection in the contested and competitive defence and security environments of the globalised 21st century"

Key findings

- Despite the significant emphasis on offensive cyber in recent UK government publications and statements, ambitions for the NCF should be realistic. Plans should recognise that offensive cyber is but one of several components of cyber strategy. The starting point for national "cyber power" should be cyber security. Offensive cyber capability occupies an important but subordinate place in national cyber strategy.

- The NCF has a wide variety of possible missions, countering state threats, terrorism and serious and organised crime. It cannot pursue all these missions equally well. Priorities will need to be determined. A balance of counter-cyber operations and support to military operations is arguably the best (and least controversial) use of the NCF.

- The NCF is the latest iteration of a slow and sometimes difficult process of inter-departmental development of UK offensive cyber organisation. As it grows, the NCF will need to be mindful of its historical development, diverse cultures and their contribution to the whole organisation. This should inform any future direction of travel, such as on continued joint status (predominantly between the Ministry of Defence (MoD) and Government Communications Headquarters (GCHQ)), or the NCF becoming principally a defence entity.

- The joint nature of the NCF raises the question of how its priorities are agreed. There is a compelling argument for active coordination from the centre of government, both from senior officials and ministers. The future of UK offensive cyber should not be decided by competition between the NCF's constituent departments but holistically by ministers.

- Like other areas of UK defence and intelligence, offensive cyber is international by design. The NCF will continue to collaborate closely with allies such as US Cyber Command and the UK government has repeatedly emphasised its commitment to contribute cyber capabilities within the NATO alliance. There remains a balance to be struck between what can be done with allies and what will continue to require sovereign capabilities. The UK has committed to discussions on international norms development and the application of international law relevant to responsible state behaviour in cyberspace, including offensive cyber operations.

Recommendations

With limited resources the NCF must be well-equipped, both in terms of informed strategic decision-making and in operational terms. The structure, scope and capability development undertaken by the NCF must strike the right balance in contributing to the UK’s “more integrated, creative and routine”[1] use of tools including offensive cyber capabilities. Our recommendations are made in four categories: **government and accountability**, **organisational configuration**, **international cooperation**, and **mission focus.**

Governance and accountability

Effective ministerial and senior official leadership will be crucial for informed decision-making around offensive cyber operations (OCOs). We recommend the UK government:

- Ensures that its ministerial small group for cyber delivers the leadership required to provide top-level accountability and strategic direction.
- Conducts a review of ministerial portfolios containing cyber responsibilities across government.
- Appoints a deputy National Security Adviser for Cyber, enabling central strategic thinking.

Organisational configuration

To enable a clear organisational configuration relating to mission focus and institutional structure, we recommend the UK government:

- Establishes clarity about NCF mission priorities for offensive cyber operations, including the process for allocating effort according to strategic priorities.
- Carefully plansthe proposed relocation of the NCF HQ to effectively mitigate short-medium term impact on its workforce and operations.
- Conducts a Cabinet Office-led cross-government audit across defence, security and intelligence agencies and departments.

International cooperation

Within a contested global landscape, we recommend the UK government does the following to strengthen international cooperation relating to OCOs:

- Continues existing strategic cooperation (with the Five Eyes and NATO) for example) and identify new cyber expertise-based partnerships with like-minded nations.

- Be proactive and transparent about the purpose and functions of the NCF in relevant international diplomacy.

- Demonstrates through operational practice and diplomacy its commitment to reducing cyber conflict by adherence to international law.

Mission focus

The NCF will need a clear and well-scoped mission focus to be effective. We recommend:

- A proportionate NCF mission focus, not exacerbating the militarisation of cyberspace, and operating within clear legal and ethical frameworks.

- The majority of NCF operations should consist of persistent, low-level counter-cyber operations, rather than the more controversial practice of targeting adversaries' critical infrastructure

- The UK government should continually review and assess the NCF's effectiveness and adjust mission focus if necessary, including to meet its legal and ethical obligations.

1. Introduction: UK government and the offensive cyber challenge

The UK is undergoing a period of reflection relating to its desired role in the current global security context. The domestic challenges of Brexit, the coronavirus pandemic and constraints on public expenditure are set against a global backdrop of increased uncertainty and potentially significant threats to national and international security. Amidst multiple corrosive challenges to the international order that has served the UK well, one remains peculiarly difficult to address and resolve: the cyber threat posed by state and non-state entities determined to undermine national security and prosperity through the malicious use of digital technologies. Whether compromising critical national infrastructure such as energy and transport, or distortion of public debate and opinion, hostile actors seek to profit – strategically and financially – from exploiting our ubiquitous dependence on computation, much linked to the Internet.

> “The domestic challenges of Brexit, the coronavirus pandemic and constraints on public expenditure are set against a global backdrop of increased uncertainty”

The quandary for policymakers is this: if the UK accepts that every country has the right to develop and deploy a variety of means – diplomatic, informational, military, economic, and beyond – to counter and combat threats to its security, where in this complex mix of competences should an offensive cyber capability lie? Such a capability would give the UK the ability to proactively deny and degrade the cyber capabilities of hostile actors, disrupt their cyber operations, pursue fully integrated multi-domain operations, and, ultimately, offer the potential to deter threats to a hyper-connected digital economy in the 21st century.

This report outlines the UK’s existing offensive cyber capacity and provides recommendations to situate the National Cyber Force (NCF) in an evolving environment. Although operational details are scarce, the UK has been open about its strategic intent with respect to offensive cyber capabilities, as reasserted in the recent *Integrated Review of Security, Defence, Development and Foreign Policy* (*Integrated Review*). [2] The UK has reorganised its arrangements for offensive cyber over the last decade, building on the skills and expertise of various bodies including the military, police and intelligence communities. It has deployed offensive capabilities against criminal entities and in integrated military operations with some success, particularly in partnership with allies. The UK has indicated repeatedly that it will retaliate, including with punitive cyber means, against adversaries that transgress acceptable bounds of behaviour in cyberspace.

To these ends, in 2020 the UK created a new force, the NCF, building principally on the dual operational and oorganisational experience of GCHQ and the MoD, the historical lead agencies of the UK’s offensive cyber mission. It also includes specialism from the Secret Intelligence Service (SIS/MI6) as well as the Defence and Science Technology Laboratory (Dstl), reflecting the breadth of skills and capabilities in human intelligence, applied science and covert technology required to execute offensive cyber operations. In almost all government communications, the NCF is presented as a joint military-intelligence partnership. As many informed commentators assert, this was a sensible and predictable next step in UK cyber organisation, though there are residual, yet important, questions about precisely what the NCF is for. “Global Britain”, asserts the UK government in the *Integrated Review*, is “best defined by actions rather than words”. [3] If this is true, what should the NCF do and where does offensive cyber fit in the strategic toolbox of the UK as a “responsible, democratic cyber power” in the 21st century? How too will the NCF feed into and promote the “whole-of-nation effort” in cyber security promoted in the *Integrated Review*?[4]

This report recommends concrete actions that the UK government can take with respect to the NCF. These are arrayed across four core themes: governance and accountability, organisational configuration, international cooperation, and mission focus, all of which additionally work towards the improved cyber security of the whole UK. The report recommends: a thorough assessment of who is responsible for strategic cyber security engagement across government; that the role and responsibilities of the NCF are articulated clearly in principle and in relation to other actors; that fostering international cooperation is key to both the potential success of the NCF and to developing norms of responsible state behaviour in respect to offensive cyber operations; and that regular assessments of NCF activities are undertaken to ensure efficacy over time. Moreover, offensive cyber operations should not be regarded as a technological “fix” to problems that are resistant to resolution by these capabilities.

Background to the report

This report is based on a research project undertaken in 2020-21 by the King’s College London (KCL) Cyber Security Research Group (CSRG) and the UK Offensive Cyber Working Group (OCWG). CSRG is affiliated with the KCL Cybersecurity Centre Academic Centre of Excellence in Cyber Security Research (ACE-CSR) and the KCL School of Security Studies.[5] The OCWG is a UK-based academia-led initiative examining the conceptual, policy and practical implications of offensive cyber activity in the UK.[6] The project was funded by the Economic and Social Research Council’s Impact Acceleration Account, administered by the Policy Institute at King’s College London. The project aimed to produce an independent evaluation of the National Cyber Force structure and role as currently understood, and to propose a set of recommendations for the UK government as it develops the National Cyber Force against the backdrop of the *Integrated Review* of Security, Defence, Development and Foreign Policy (*Integrated Review*).

Structure

The remainder of this report consists of four main sections. Section 2 explores the operational landscape that suggests the need for a sovereign offensive cyber capability; it traces the development of this capability through to the establishment of the joint military-intelligence National Cyber Force. Section 3 looks at how international law, ethical and normative frameworks, and the UK’s alliance relationships, help shape the UK’s offensive cyber posture. Section 4 outlines four considerations as the NCF enters its operational phase and further integration into the national cyber mission: governance and accountability; organisational configuration; international cooperation; and mission focus. Section 5 concludes this report with a final set of reflections and recommendations.

2. The UK case for cyber

The historical development of cyber security in the UK indicates that the British government sees operational and strategic utility in strengthening national offensive cyber capacity. This section first establishes the operational landscape in which a sovereign offensive capability is deemed necessary. It then outlines how this capability has emerged since 2010, rooted as it is in long-term military-intelligence cooperation. The third subsection details the establishment of the NCF and points towards questions about its identity, size and mission.

> “All cyber threat actors operate across a complex landscape that maps poorly to sovereign borders or discrete legal jurisdiction”

Operational landscape

Since the 2010 National Security Risk Assessment, the UK government has consistently regarded cyber threats as top (Tier 1) national security priorities. In addition to national security strategies (2010, 2015), the UK has implemented two iterations of national cyber security strategy (2011, 2016), with a third expected in 2021. These and other UK government statements identify three primary types of hostile actor that pose cyber threats to the UK: adversary foreign states, serious organised criminals, and terrorist organisations.[7] Each category presents a different range of resources, capabilities and objectives:

- **Adversary foreign states:** State actors and state-sponsored groups are politically motivated to access or disrupt government and critical infrastructure. States conduct military, espionage, subversion and influence operations through cyber means, as well as connecting with cybercriminals and proxies for diverse strategic and operational purposes, especially if this permits states to claim “plausible deniability” if their involvement is suspected.

- **Serious organised criminals:** Whilst cybercrime can be low-level and opportunistic, serious cyber fraud, theft and extortion are carried out by organised crime groups from such regions as Eastern Europe (including Russia), South Asia and West Africa. Cybercriminals are motivated by profit and use cyber means to effect traditional crimes (cyber-enabled crime) and to develop new forms of criminality in which information technologies are the platforms and targets of crime (cyber-dependent crime).

- **Terrorist organisations:** Terrorists have yet to leverage computer networks for destructive purposes (cyberterrorism) but are adept at using the internet for radicalisation, recruitment, fundraising and command-and-control (internet terrorism). The current absence of cyberterrorism is a poor guide to the future and terrorists will continue to seek impactful cyber capabilities.

This typology is not exhaustive. For instance, the “insider threat” posed to organisations by employees and contractors with a combination of internal knowledge and the motivation to harm is also considered important, as is the general risk of everyday users’ poor cyber security practices through ineffective design.[8] Systemically, the recent SolarWinds and Microsoft Exchange compromises highlight the risks posed by the reliance of public and private sector entities on enterprise infrastructure that is not only subject to persistent malicious activity but also undermined by poor alignment between market incentives and the need for good cyber security.[9]

All cyber threat actors operate across a complex landscape that maps poorly to sovereign borders or discrete legal jurisdictions. When defensive countermeasures are deployed by the UK, these are readily restricted to UK-based networks, within a "permissive" environment where government can expect assistance in achieving its goals. One such example is the Active Cyber Defence programme that aims to reduce, through largely automated means, the harm to the UK from high-volume, low-impact "commodity cyber attacks", which typically address low-level cybercrime.[10] More proactive operations, whether pursuing or disrupting cybercrime, conducting digital counterintelligence, or military cyber operations – any of which can be considered "offensive" – frequently occur outside UK networks. Like international espionage, forays into allies' networks may be permitted by custom or by formal diplomatic mechanisms, but offensive cyber operations of necessity occur in whole or in part in foreign or hostile "non-permissive" environments. They intervene in a range of problematic sites and situations, each with distinct jurisdictional, legal, diplomatic and ethical implications.

UK national strategy reserves the right to conduct these operations, subject to operational necessity and international law. The development of an offensive cyber capability to pursue and punish adversaries is an overt strand of the "Deter" pillar of the 2016 national cyber security strategy, ensuring that the UK has "the means to take offensive action in cyberspace, should we choose to do so".[11] Furthermore, "Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere".[12] The presence of such "systemic competition" between multiple actors complicates distinctions between war and peace and manifests as competition short of "open confrontation or conflict".[13] As in other similarly capable countries, the UK sees offensive cyber as an essential component of its operational and strategic toolbox.

Organisational development

UK offensive cyber operations emerged collaboratively between multiple actors, principally GCHQ and MoD. Differing organisational priorities have shaped operational roles and responsibilities, including institutional perspectives on how and when offensive cyber capabilities should be used. GCHQ is primarily an intelligence agency, developing capabilities to collect information; its "effects" mission, to use its capabilities to achieve other objectives, was always secondary. In contrast, the primary mission of MoD – although it has significant intelligence capabilities – is to defend the UK, by force where necessary. Cyber capabilities were developed earlier by GCHQ, given its longer experience of computer network operations, but it also continues to discharge its support mission to MoD.[14] The "prehistory" of UK offensive cyber operations remains untold, although inevitably pre-dates their avowal by the UK in September 2013, the first country to do so.[15] The 2010 *Strategic Defence and Security Review (SDSR)*, for instance, announced improved coordination of military cyber developments, including the use of reservists. It made no overt reference to "offensive" cyber, although this was arguably implicit in references to integrating new cyber capabilities with conventional non-cyber capabilities.[16]

By 2015, the *SDSR/National Security Strategy* was referring to a joint GCHQ/MoD cyber collaboration as the National Offensive Cyber Programme (NOCP).[17] Reportedly created in 2014, the NOCP was to be funded in part by the £1.9 billion allocated for the second iteration of the National Cyber Security Programme (NCSP).[18] The Chancellor of the Exchequer described the NOCP as "a dedicated ability to counter-attack in cyberspace"; he warned "individual hackers, criminal gangs, terrorist groups and hostile powers" that the UK would "defend ourselves" and "take the fight to you too."[19] The rhetoric of deterrence and reaction was a persistent theme in senior ministerial speeches about the development of a national offensive cyber capability. The Defence Secretary in 2016 stated: "It is important that our adversaries know there is a price to pay if they use cyber weapons against us, and that we have the capability to project power in cyberspace as in other domains."[20] He would only say then that the UK had "begun to integrate offensive cyber into our military planning alongside the full range of military effects."[21] In 2017, however, he announced that the UK was now "using offensive cyber routinely in the war against Daesh" in Iraq and Syria.[22]

It is unclear to what extent NOCP operations were coordinated with those of US Cyber Command (USCYBERCOM), although the two countries in September 2016 signed a memorandum of understanding on defensive and offensive cyber capability development.[23] As part of Operation Glowing Symphony from November 2016, USCYBERCOM reportedly conducted "a rolling series of propaganda takedowns and account lockouts" against Daesh/Islamic State.[24] USCYBERCOM has subsequently acted against Russian disinformation operations prior to and during the US 2018 midterm elections.[25] From 2018, the UK would also declare that Russia was a legitimate target of offensive cyber operations, not least on account of Russia's own information and cyber operations.[26]

Establishing a National Cyber Force

In September 2018, the government pledged £250 million to move beyond the NOCP and create the NCF, with ambitious plans to increase its size from an initial operating capacity of 500 to 2000 personnel.[27] This followed the March 2018 Salisbury attack and a revitalised government focus on countering and deterring hostile state actors, particularly Russia, an approach formalised in the *Integrated Review*. Government sources increasingly presented cyber capabilities as an important element in the UK's response to Russia.[28] A senior Whitehall official later appeared to suggest that offensive cyber operations were indeed used in response to the Russian threat.[29] Yet, the NCF was more than a reaction to the perceived increase in the threat from Russia and other hostile state actors. Former senior intelligence and cyber officials suggested that the NCF was a logical attempt to optimise effectiveness and efficiency through an integrated civilian-military organisation tailored to the resources available in the UK system.[30] Since 2010, successive governments have attempted to protect cyber from the impact of reduced public expenditure, whether the fallout from the global financial crisis then, or the coronavirus pandemic now. In each case, the government has committed to increasing offensive cyber capacity but has had to keep the size of the NOCP/NCF small and augment it with reservists.[31]

£250 million
pledged to establish a National Cyber Force

This opens the questions of what the revamped NCF is for and how large it will need to be to meet its mission requirements. In 2019, the National Audit Office reported that the UK had “routinely used offensive cyber to counter the threat from terrorism. This has had a significant effect on degrading Daesh capabilities.” [32] It is unclear whether the emphasis on counterterrorism operations reflects the operational prioritisation of NOCP/NCF missions, or if the sensitivity of avowing operations against state actors prevents a wider discussion of targeting and mission success. Whatever the situation, when the Prime Minister announced on 19 November 2020 that the NCF was operational, he stated it would target not only terrorists, but serious organised criminals and hostile state actors. This wider mission set would be accompanied by an increase in NCF personnel to 3000 by 2030.[33] This seems to imply a larger number of NCF operations, the ability to conduct more sophisticated operations, or longer offensive cyber campaigns. To a large extent, this will be determined by the capacity to grow the NCF in terms of personnel and the competition across other strategic national missions at GCHQ or MoD, plus the broader cyber security environment in the private sector.

3. UK offensive cyber in a global context

The UK views offensive cyber as an integral part of its sovereign capability. It capitalises upon the experience of joint military-intelligence organisation and operations, as well as creating opportunities for future synergies and operational vigour. In considering the precise disposition and tasking of the National Cyber Force – what the UK wants the NCF to achieve and how – we examine what the NCF can realistically do, given the constraints and opportunities of the international structures in which the UK is embedded. The following section looks at how international law, ethical and normative frameworks and the UK's alliance obligations shape the choices facing the UK as it develops its offensive cyber posture.

International law

The UK has argued consistently that its national cyber security objectives will be pursued through adherence to domestic and international law, a standard it also expects of others.[34] This includes offensive cyber capabilities, which "can be deployed at a time and place of our choosing, for both deterrence and operational purposes, in accordance with national and international law."[35] As the Attorney General stated in a widely reported speech in May 2018, states have the right to develop sovereign offensive capabilities, and to defend themselves against hostile cyber actions, but they must be "governed by law just like activities in any other domain."[36] The 2016 *National Cyber Security Strategy* notes that other states, by way of contrast, have deployed offensive cyber capabilities and may do so "in contravention of international law in the belief that they can do so with relative impunity, encouraging others to follow suit."[37] UK efforts in respect of international law as pertaining to offensive cyber consists of two main fields: convincing others of the applicability of international law to cyber operations; and determining precisely how international law applies to those activities.

Ostensibly, the first of these workstreams is already well developed. In 2013, the UN Group of Governmental Experts (GGE) on information security agreed that customary international law applied in its entirety to state cyber operations. Two years later, it affirmed that the UN Charter and the tenets of international humanitarian law (IHL) that govern warfare – necessity, proportionality, humanity, distinction – apply in cyberspace.[38] The NATO-sponsored Tallinn Manual Process also confirmed that all international law always applies to state cyber operations.[39] A host of multilateral and multistakeholder groups and organisations support this position. However, three GGE members – US, China, Russia – refused to sign the 2018 "Paris Call for Trust and Security in Cyberspace" that reaffirms the GGE position.[40] Whilst the US stance might have been a function of the Trump administration's antipathy to multilateralism, it also suggests that the US position on international law, whilst affirmed in most contexts, is not settled entirely. These developments are demonstrably more a question of "how" rather than "if" international law applies, where recent US debates have centred around how differing interpretations of "sovereignty" in international law enable or forbid digital interventions in non-permissive environments.[41]

The UK position is clearer and, in addition to IHL justifications for offensive cyber operations in armed conflict, the Attorney General drew specific attention to UN Charter provisions prohibiting under normal (non-war) circumstances the interference by one state in the domestic affairs of another, including through cyber

“The international governance of counter-cybercrime is uneven and lacks global harmonisation”

means; the right to respond to states undertaking such activities in UK territory; and the right to self-defence should a cyber operation “result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack”.[42] Offensive cyber operations offer flexibility of response to a wide range of threats of differing severity, including electoral manipulation by a foreign power, threats to “critical infrastructure”, or indeed any illegal act prosecuted through conventional means. The UK does not believe that any such countermeasures – which cannot amount to a use of force – require prior notification to the targeted state party. Although this applies only to situations involving states, customary international law – and treaty mechanisms – would also regulate the use of cross-border offensive cyber operations to thwart cybercrime, although the international governance of counter-cybercrime is uneven and lacks global harmonisation.[43]

Ethics and norms

The UK supports the development and deployment of offensive cyber capabilities in times of war and peace subject to international law. It also promotes adherence to international law as a norm of responsible state behaviour in cyberspace, including the legal use of offensive cyber capabilities. However, the UK’s position expresses clearly that offensive cyber capabilities can be used if certain conditions are met but says rather less about if they should be. The consensus position of the 2015 GGE, for instance, articulates five “limiting norms”, including that states should not conduct or support activity that impairs or “intentionally damages critical infrastructure”, as well as preventing “the use of harmful hidden functions”.[44] These would seem to disbar offensive cyber operations of various kinds except, of course, when national interests demand otherwise. UK discussion – at least in public – tends to assume the probity of the latter without concerning itself too much with the former. In this sense, the “strategic promise” of offensive cyber is running ahead of the more granular ethical debate.[45]

The UK has committed to the NCF carrying out cyber operations in a “legal, ethical and proportionate way”.[46] The language of ethical cyber operations does not surface in the *Integrated Review*, however, and the UK’s commitment to developing and socialising norms of responsible state behaviour would be well-served by clear articulation of its ethical position concerning where and when offensive cyber operations will be considered operational possibilities. Publicly and explicitly highlighting ethical considerations beyond traditional military concepts – just war theory, for instance – and international law, would encourage deeper domestic engagement on these issues, as well as signalling to other states the importance of ethical frameworks for the planning and execution of offensive cyber operations. This could encourage virtuous feedback loops in which ethics and norms co-evolve, such as to incorporate “kill-switches” in operational computer code, that in turn help shape national cyber postures and operations.[47] It would also indicate that the ethics of offensive cyber operations are just as important as international legal deliberations: ethical challenges are not necessarily soluble through law. Offensive cyber operations may be legally permitted in certain circumstances and environments, but this does not mean they are always the ethical course of action.[48] The UK’s strategic posture sensibly allows for flexibility in its choice of response mechanisms, including to hostile cyber operations, but ethical flexibility is a more problematic proposition.

Military cyber operations arguably pose the fewest ethical puzzles, as they are already subject to IHL. Offensive cyber actions, for instance, may be "more ethical" than conventional means in certain military contexts, if they can achieve their desired effects whilst causing less harm than kinetic capabilities, or even prevent harm; this may make their use obligatory.[49] Equally, if military effects cannot be achieved by an offensive cyber action without risking harm to non-combatants, should it go ahead? The picture is rather more nuanced in the non-war situations in which the NCF will predominantly operate.[50] In response to demonstrable hostile acts, the case is relatively easy to make for targeting adversaries' operational infrastructures ("counterforce", in nuclear jargon), but if offensive cyber is to be used as a form of signalling or coercion, this may require holding at risk "countervalue" targets like civilian infrastructure. What are the material consequences of such actions, and the second-order emotional or cognitive effects on civilians? Importantly, would such actions be in tension, or possibly undermine, the UK's normative commitments and its general support for a rules-based approach to international behaviour? There are many other issues deserving of an ethico-political analysis, including the approach taken to vulnerabilities discovered by UK government operators.[51] This all points to the need in policy and practice to ensure that all NCF personnel are situated within an ethical and moral practice. They should regard a general level of "ethical literacy" as a recurring requirement of their roles.

Alliances

The NCF will not operate in a vacuum. It is deeply enmeshed in an enduring network of alliances and partnerships, most notably with European neighbours and the US, and as a member of NATO and the Five Eyes (FVEY) Anglophone intelligence alliance (comprising the UK, US, Australia, Canada and New Zealand). By necessity, the NCF must be attentive to, and often integrate with, the offensive cyber capabilities, doctrines and postures of its allies, whilst developing its own stance that reflects UK national interests, ambitions and obligations. In some situations, such as FVEY, this is primarily an intelligence-sharing arrangement characterised by a significant degree of trust between allies. Whilst this has delivered significant operational benefits for over 70 years, it has also been challenged by allegations of shared impropriety (Edward Snowden) and by disagreements over specific issues, most recently over Huawei and 5G. The arrangement is unusually robust, though, and will persist, perhaps even developing common strategic positions around offensive cyber, as well as enhanced operational relationships.

One potential challenge to operational coherence in cyber operations – as opposed to alliance cohesion – concerns the US' doctrinal shift to "persistent engagement".[52] This requires US Cyber Command and others to engage constantly with adversaries in order to inflict costs on potential and actual attackers. An inherent aspect of this is the need to "defend forward" that implies – although interpretations are not settled in the US – operating outside domestic US networks in non-permissive environments to deny, distract and frustrate adversaries' operating capabilities.[53] This is not an inherently offensive posture, but the apparent normalisation of extra-jurisdictional operations hints at the tension between perceived operational necessity and international normative and legal obligations. The question for the UK is how far to align itself with US posture, including as that posture develops under the Biden administration.[54] Indications in UK strategy suggest an unproblematic application of "persistent engagement" across defence, although the cyber component of this effort is referred to only as "contesting the cyber domain to protect our networks".[55]

It remains unclear how this more proactive approach will be welcomed by other important allies, or indeed how it might be emulated by adversaries.[56] France makes a clear distinction between offensive and defensive cyber, for instance, that is blurred significantly by persistent engagement.[57] Germany has historically been reluctant to relax its constitutional restraints on military cyber operations and articulates a cautious approach to offensive cyber.[58] Close allies like Norway and the Netherlands also differ in their approaches to military offensive cyber.[59] Whilst these perspectives do not affect offensive cyber equally across all its likely manifestations, it may affect offensive cyber in support of military operations in a formal alliance like NATO, of which all these countries are members. NATO aims to have a fully operational Cyber Operations Centre (CyOC) by 2023, which will provide defensive and offensive cyber mission support.[60] This will rely on integrating "national cyber effects or offensive cyber into Alliance operations and missions".[61] The UK has committed to declare its offensive cyber capabilities to NATO under its Article V commitment to the Alliance.[62] Any issues with divergent doctrinal, legal or constitutional barriers to capability-sharing and interoperability are addressed in joint doctrine and a formal mechanism called Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA).[63] However, NATO is under civilian control and the politics of offensive cyber deployment, including by NCF, will not always defer to military doctrine.

4. A distinct UK approach

The foregoing discussion suggests multiple opportunities to develop a distinct role for the National Cyber Force in delivering operational and strategic effects consistent with UK national aims and objectives. To do so, it must consider: the nature of the operational environment; the idiosyncrasies of the UK defence and security landscape, including resource constraints; its international legal and alliance obligations; and the importance of maintaining and promoting behavioural norms and ethics. This section outlines four specific considerations for UK decision-makers as the NCF enters its operational phase and further integration into the national cyber mission: governance and accountability; organisational configuration; international cooperation; and mission focus. None of these factors is a wholly discrete category and all should be viewed as mutually supporting in multiple ways.

Governance and accountability

As with other aspects of UK cyber strategy, offensive cyber would benefit from reviewing existing arrangements for ministerial accountability and coordination by senior officials at the centre of government. The last two iterations of the National Cyber Security Strategy were developed under the National Security Council (NSC) process established in 2010. The NSC process remains in place, but its significance has fluctuated under successive prime ministers, each of whom has used it differently. For several years, a ministerial sub-committee of the NSC, chaired by a senior minister, oversaw cyber strategy. This sub-committee appears not to have met since Boris Johnson became prime minister in July 2019.

The *Integrated Review* announced that a ministerial small group has subsequently been formed "to cohere cyber decision-making across government."[64] This reversal is welcome, but the government should clarify the group's membership and remit and review its supporting structures to ensure it provides the necessary strategic direction for cyber decision-making. If not already the case, it should again be chaired by a senior minister – perhaps either the Prime Minister or Chancellor of the Exchequer – to avoid or resolve conflicts between MoD and the Foreign Office over who should have precedence in offensive cyber operations. The joint capability has historically suffered from a "long and difficult battle between GCHQ and the Ministry of Defence over authority" for specific operations, reflecting the military-intelligence mix of offensive cyber.[65] The confirmation that MoD will be the biggest contributor to the NCF perhaps indicates a shift in bureaucratic influence away from GCHQ and must be actively managed from the centre of government.[66]

Improvement to ministerial leadership in cyber should extend below the strategic NSC level to everyday ministerial oversight. Cyber security is currently allocated across a wide range of ministerial portfolios. Greater focus and coherence could be achieved with a network of dual- or even triple-hatted cyber ministers responsible for coordinating the multiple agencies and departments closely involved with offensive cyber (and broader cyber security) strategy. This cross-departmental mode might help reduce the risk of competition over resource allocation and policy direction.
In addition to streamlining ministerial responsibilities, the UK could benefit from attention to senior official appointments and coordinating secretariats at the heart of government.

Amidst several reorganisations of senior national security roles in the last decade – often to reflect the priorities of a new National Security Adviser (NSA) – the number of deputy NSAs has fluctuated. Several have included cyber within their wider portfolios, but there has not yet been a Director General-level official in the Cabinet Office with a sole mandate for cyber strategy and coordination. The new NSA (March 2021) should appoint a deputy NSA for Cyber, equivalent to the White House creation of a similar role in January 2021.[67] A senior cyber official at the heart of government, appropriately supported, could improve long-term cyber coordination. This would help to formalise the process for addressing areas of policy in which competing priorities, the balance of UK security, or departmental interests collide, including around offensive cyber operations.[68]

Organisational configuration

The NCF comprises organisations with different resources, expertise, legal authorisations, organisational cultures, and operational backgrounds. The NCF commander is from GCHQ, reflecting the weight of capability and experience in conducting cyber operations that GCHQ brings to the collaboration.[69] However, the NCF is not part of GCHQ – unlike NCSC – and GCHQ is not, formally at least, first among equals. It is difficult to forecast confidently how organisational differences will shape the working relationship and mission priorities (see below) of the NCF, particularly as MoD will contribute more of the funding for the NCF.[70]

Dedicated senior cyber officials at the centre of government will help to arbitrate disputes and act as honest brokers if protracted disagreements require elevation and ministerial resolution. The NCF presently operates under a range of different legal authorities, depending on whether the Foreign Secretary or the Defence Secretary is required to authorise particular operations. At this stage, the implications of divided departmental equities are unclear. Ultimately, the decision about NCF utility and identity must be political judgements and the responsibility of senior ministers. Nevertheless, the views of officials from NCF constituent parties – those most steeped in the practicalities of offensive cyber operations – will shape the options put to ministers and the briefings that shape their understanding and decision-making.

3,000
National Cyber Force Personnel to be recruited by 2030

Given the ambition to increase NCF personnel to 3000 by 2030, there must be clear understanding of why this is necessary and how such growth will be achieved. Different workforce strategies will produce different cohorts whatever the total number. Is the priority to increase the number of high-end operators and developers, or to accelerate growth by rapid hiring of less-skilled operators? Each implies different outcomes in terms of the number and sophistication of possible NCF operations.[71] The UK has, despite some progress, struggled to overcome barriers to the development of career cyber professionals in the services.[72] The Chief of Defence Staff announced in 2019 that the MoD would pursue “unified career management” to create “blended career fields” for uniformed and civilian personnel, including in cyber. [73] In addition, the MoD has tried to better integrate reservists’ skills and experiences in its cyber force.[74] This has offset some of the adverse effects of shedding labour during the period of austerity.[75] The Joint Cyber Reserve created in 2013 helped address this and will presumably play an important role in the NCF.[76]

NCF recruitment and retention decisions may affect GCHQ and MoD's cyber intelligence and cyber security missions. These should be explored in a cross-government audit of cyber workforce strategy, aligned with the Whole Force concept that includes civilians, armed personnel, reservists and contractors. This is a problem that transcends the national defence and intelligence community. The government recognises the need to nurture the development of a national pipeline of cyber talent, for example in its recent creation of the independent UK Cyber Security Council.[77] There is a clear requirement, here as elsewhere, for government to integrate its offensive cyber priorities with its wider cyber priorities – an intention at least that some commentators have inferred from the language of the *Integrated Review*.[78]

The *Integrated Review* committed to establishing a new NCF headquarters in the North of England, as part of a broader policy to increase technology-related employment across the UK regions.[79] This is consistent with existing decisions to move central government officials out of London, such as the 750 staff from HM Treasury due to relocate to Darlington.[80] Whilst this suggests other factors have contributed to the decision, it is important to consider the possible impact of the move on the NCF itself and its future. It is unclear whether the new headquarters is intended to house all the NCF's workforce and operations. To have a meaningful impact, the HQ must be more than a Potemkin office, an impressive site to show visiting ministers but largely empty of staff and peripheral to the main effort. If the NCF embraces the decision, however, and shifts its current workforce and future recruitment from Cheltenham (GCHQ) and MoD Corsham to the new site, there are short- and longer-term implications.

There is the question of timing and to what extent the move would affect the NCF's current staff, accustomed to its hitherto split-site location. Will the relocation decision affect retention and succession planning, particularly as all the constituent departments that comprise the NCF have national headquarters based in the South or South West? The NCF is currently a small and specialised unit. As such, its capability relies on a relatively small number of highly skilled staff. Planning the move north should consider its impact on continuity and on the retention of core staff, as well as the package necessary to continue to attract the best staff from constituent organisations' respective head offices. This might result in considerably higher staffing costs, if, for example, two-to-three-year secondments to the NCF come with relocation and accommodation allowances to attract (civilian) staff with existing long-term commitments near their parent department's head office. If the NCF is to maintain its integration with parent departments, then the government must accept that relocation is likely to incur such costs, at least in the short to medium term.

If the northern headquarters will house the majority of NCF staff, it makes sense to choose a location that is future-proofed and can accommodate the projected workforce of 3000 by 2030. The new headquarters therefore brings opportunities to attract talent from and to the North West of England, but also increases the challenges associated with managing the ambitious growth the NCF will pursue over the next decade. The right approach to implementation will put operational impact at the heart of planning. It will also strike a sensible balance between establishing a credible new headquarters and retaining the instrumental link with capabilities that will continue to be based in existing government locations. This includes operational capabilities in contributing agencies and departments, as well as the training facilities at the Defence Cyber School based at Shrivenham in Oxfordshire. If 3000 personnel are to be based at NCF headquarters by 2030, a co-located training facility would be a sensible addition – perhaps allowing remote access to the Defence Cyber School.

International cooperation

The hostile state actors, criminal groups and terrorists likely to be targeted by the NCF are also regarded as threats by the UK's closest allies. It makes no sense for the NCF to pursue these operations as if the UK alone had the intent and capability to act against these targets. Given the strong thread of international cooperation running through UK defence and security strategy, the imperative to collaborate in offensive cyber will be embraced by the NCF. This is so in an operational sense, where the UK is already engaged in operations with NATO and individual allies, but also in the more extended sense of shaping the rules and norms of responsible state behaviours pertaining to offensive cyber operations, whether conceived of as friendly or hostile. Moreover, as has been remarked numerous times by commentators, the fastest emerging norm of international affairs is the existence of cyber conflict itself. The UK's use of offensive cyber capabilities must be understood as a contribution to this development, mindful of the risk of proliferating both capabilities and undesirable behaviours.

> "Cooperation alone will not deliver the flexibility or assurance provided by the development and retention of a sovereign UK capability"

Strategically and operationally, the UK's closest relationships will continue to be with the US, wider FVEY and NATO. The UK was the first ally to offer offensive cyber capabilities to NATO and the NCF will be a significant contributor to NATO's offensive cyber ambitions via SCEPVA. Beyond NATO, the MoD and US Department of Defense 2016 memorandum of understanding implied a division of effort between the UK and US in offensive cyber operations.[81] This is sensible and should be pursued to ensure operational deconfliction, value-for-money and effectiveness. This extends beyond simply dividing up target sets and should include joint operations and reciprocal personnel secondments to USCYBERCOM. To improve interoperability and explore efficiencies, where appropriate the NCF should consider joint procurement of services, such as training suites. The NCF should review what opportunities exist for pursuing value-for-money in collaboration with the US. At the least, the NCF should exploit the benefits of its comparatively late development, actively learning lessons from the more mature US experience of developing its offensive cyber workforce and procuring services and capabilities from the private sector.[82] There is considerable scope to achieve strategic outcomes in close partnership with allies, but cooperation alone will not deliver the flexibility or assurance provided by the development and retention of a sovereign UK capability that can be used whenever necessary, including in circumstances in which allies are either not in agreement with, or are kept unaware of, UK operations. The recent UK Defence and Security Industrial Strategy recognises this need to balance development of sovereign offensive cyber capabilities with continued, close cooperation with allies.[83] Even with close allies, notably the US, these relationships must be kept under regular review to ensure cooperation continues to serve UK strategic objectives.

The creation of the NCF will not cause the UK to depart from its historical approach to the rules-based international order, nor deviate from its commitments to international treaties and institutions. The UK realises, however, that its approach to offensive cyber is not that held by all states in the international system. The NCF enters a complex and contested environment in which states indicate different perspectives on how, when and why cyber operations are permissible or not. To some states, an avowed offensive cyber capability is evidence of militaristic intentions, even if those same parties conduct or condone precisely those operations the NCF is designed to counter. The UK should continue its delicate and cooperative diplomacy on cyber operations at the UN and other fora, setting out the need for the NCF when queried, explaining what it is for and what it is not for. This includes a more explicit commitment to dialogue with the European Union than indicated in the *Integrated Review*, especially as the UK can continue to provide a transatlantic "bridging" capability. Transparency about offensive cyber will demonstrate responsible state behaviour and help build enduring norms that reduce cyber conflict, not increase it. Even if the UK cannot achieve that outcome immediately, there is diplomatic utility in being seen to conform to international law and ethics, which will be key to promoting the UK as a "responsible, democratic cyber power".[84]

Mission focus

One of the key challenges in policy and in practice will be to determine the balance between the NCF's different missions. Should it, for example, focus more of its efforts on taking down the infrastructure of ransomware cybercriminals; the tackling of online harms in cooperation with other government partners like NCA and the Department for Digital, Culture, Media and Sport (DCMS); counter-cyber operations against hostile state actors; or preparing for and engaging in integrated military operations? All are covered by the NCF's stated remit, but ministers must determine the rough balance of the NCF's operations and capability development: the NCF will not be able to do everything, nor do everything equally well. To a high degree, this will be determined through triangulation of national strategic posture, contextual operational requirements (including those of allies), and the availability of resources. It will also be shaped by the NCF's eventual development of its own sense of identity and core mission and by the requirements and priorities of other cyber-focused units like the 6th (UK) Division, with its diverse portfolio of "cyber, electronic warfare, information operations and unconventional capabilities".[85] Success will also depend on the effective implementation of the defence cyber career specialism and planned expansion of the Defence Cyber School.[86]

> "Choices about the targets and methods of NCF missions will shape the meaning of the UK's role identity as a responsible, democratic cyber power"

The NCF's mission will not remain static, whatever is decided now, although it will likely – in one form or another – remain an integral component of UK national cyber power for the foreseeable future. To a significant extent, choices about the targets and methods of NCF missions will shape the meaning of the UK's role identity as a responsible, democratic cyber power. The operational environment and the complexion of international order will change, as will the interpretation of international law, norms and ethics. The military components of the NCF mission must be supported by updated doctrine, both for cyber and for CEMA (Cyber and Electromagnetic Activities).[87]

> “The UK should be especially cautious that the NCF does not encourage further militarisation of cyberspace”

The NCF is not a conventional cyber security vehicle and should not be allowed to distract from wider strategic cyber security goals, nor indeed other national aims and ambitions. It is encouraging that MoD has rearticulated its military cyber defence mission, but cyber defence should be prioritised in other sectors too.[88] There will doubtless be a temptation in some quarters – both political and military – to assume that the NCF will be able to do things it simply cannot. The NCF should not be perceived as a technological fix to problems that offensive cyber operations are ill-suited to addressing. Its utility as a strategic capability, for instance, must be tempered by the realisation that deterrence and compellence in and through cyberspace are difficult and all but impossible to achieve solely through cyber means.[89] It offers the ability to deny, disrupt, degrade and possibly even damage specific threat actors and their infrastructures in a targeted fashion, but it will not win a war – metaphorical or actual – on its own.[90]

The NCF’s chief utility may be in counter-cybercrime operations against determined serious organised crime groups, but it is not suitable for pursuing and punishing all forms of cybercrime. The UK should be especially cautious that the NCF does not encourage further militarisation of cyberspace, thereby undercutting its overt commitments to international peace and security. This is clearly separate from the tactical and operational use of cyber operations to support integrated military operations, which will undoubtedly form a significant part of the NCF’s mission.

We do not yet know whether and how the NCF will differ substantively from its predecessors. It does, however, appear to represent a step-change in “organising for cyber”, if not a reinvention of the overall game itself. According to the *Integrated Review*, the government intends to: “make much more integrated, creative and routine use of the UK’s full spectrum of levers – including the National Cyber Force’s offensive cyber tools – to detect, disrupt and deter our adversaries.” Creative and routine use of offensive cyber suggests a significant counter-cyber role, but the most important part of the excerpt is the reference to integration. Offensive cyber is part of a wider toolkit to pursue strategic objectives.[91] The main preoccupation of cyber security and cyber strategy should remain, as UK strategy states clearly, to ensure that “the UK is secure and resilient to cyber threats, prosperous and confident in the digital world”.[92]

5. Reflections and recommendations

The National Cyber Force has emerged from a decade of incremental improvement in the collaboration between its constituent agencies and departments, a process that has not always been smooth or uncontentious. This institutional reform has occurred during a transitional period, in which several states have started to talk more openly about their offensive cyber capabilities. It has also seen the increased use of offensive cyber by states; a rise in the number with offensive cyber capabilities; and significant growth in the frequency, sophistication and harm caused by non-state activities, particularly cybercrime. The NCF is the latest manifestation of the UK government's responses to this changing operational and strategic environment, as outlined in the *Integrated Review* and elsewhere. It is authorised to act across the full spectrum of offensive cyber missions against hostile states, serious organised crime, and terrorists.[93] This open avowal, coupled with the enthusiasm expressed in recent years by government ministers, demonstrate that it is perceived as political "good news" for UK defence and security. It is presented as a vehicle of growth, jobs and opportunity at a time of difficult decisions about public expenditure and reductions in the armed forces in particular.

Beyond the headlines of political approval and the NCF's broad remit, what will the NCF actually do, and why? The threat landscape is formidable and the NCF is not backed by limitless resources; it will need to prioritise its missions. Even if it succeeds in growing capacity to 3000 personnel by 2030, this would still be half the size of USCYBERCOM today. It is not sensible to benchmark NCF capacity or actions against the US, but this underlines the need to confront hard choices about how to use offensive cyber capabilities to achieve optimal national outcomes in a constrained fiscal environment.

These decisions require strategic leadership from ministers and senior officials, so important questions about **governance and accountability** should be addressed at the earliest opportunity. Enabling the NCF as an effective force requires clarity about its **organisational configuration**, including the impact of institutional location, and **mission focus**. This will encourage pragmatic transparency about what success looks like, how it is going to be delivered, and how it will be measured. Importantly, it would be misleading and counterproductive to answer these questions absent the critical dimension of **international cooperation**. UK strategy is international by design and emphasises the salience of alliances and partnerships with states and international organisations, all respecting the rules-based international order.

Under these headings, we therefore make the following recommendations:

Governance and accountability

- UK government should ensure that its ministerial small group for cyber delivers the leadership required to provide top-level accountability and strategic direction. Led energetically by a senior minister and supported effectively by officials at the centre, it should resemble a reinstatement of the cyber sub-committee of the National Security Council.

- UK government should conduct a review of ministerial portfolios containing cyber responsibilities across government, potentially improving focus by creating "double-hatted" ministers with larger cyber portfolios that span two or more departments.

- UK government should appoint a deputy National Security Adviser for Cyber, to elevate the level of sustained central strategic thinking about and co-ordination of cyber-related defence, security and intelligence issues across and beyond government, including mission priorities for the NCF.

Organisational configuration

- UK government should establish clarity about NCF mission priorities for offensive cyber operations, including the process for allocating effort according to strategic priorities rather than via bargaining between competing institutional actors. Budgetary contributions should not translate directly into control: decisions should be made holistically. There is a clear role here for the centre of government to coordinate.

- The proposed re-location of NCF headquarters should be carefully planned and its short- to medium-term impact on NCF workforce and operations should be mitigated by efforts to ensure continuity. Resourcing should reflect the need to retain civilian staff and incentivise re-location. It may also be necessary, as the NCF grows, to establish a co-located Defence Cyber School presence.

- On workforce strategy, the Cabinet Office should lead a cross-government audit across defence, security and intelligence agencies and departments, to ensure that workforce plans are aligned and mutually reinforcing. The NCF should be situated in the context of the wider Whole Force concept (integrating civilians, regular armed forces personnel, reservists, and contractors).

International cooperation

- Operational and strategic cooperation with allies will and should continue, particularly within FVEY and NATO, but UK government should identify and discuss with other partners, notably European states and the EU, how UK cyber expertise can contribute to the collective aspirations of like-minded nations and ensure the optimal impact of UK offensive cyber capabilities.

- UK government should be proactive and transparent about the purpose and functions of the NCF in relevant international diplomacy, including its retention of a sovereign offensive cyber capability, residing principally in the NCF.

- UK government must demonstrate through operational practice and diplomacy its commitment to reducing cyber conflict by adherence to international law and thereby the promotion of norms of responsible state behaviour in cyberspace.

Mission focus

- The NCF mission should add value to, rather than detract from, overall UK cyber security priorities; it should be proportionate, not exacerbate the militarisation of cyberspace, and operate within clear legal and ethical frameworks.

- The majority of NCF operations should consist of persistent, low-level counter-cyber operations – targeting the cyber infrastructure of state actor adversaries and criminal groups – as well as tactical and operational support to integrated military operations. This is sufficiently challenging and high-priority work for the NCF to focus on; it is a better focus for the NCF than the more controversial option of targeting adversaries' critical infrastructure.

- UK government, perhaps through the Prime Minister's Implementation Unit and the National Audit Office – and with the oversight of the Intelligence and Security Committee of Parliament (ISC) - should continuously assess NCF effectiveness. The UK needs to be able to determine whether its offensive cyber strategy is succeeding, in line with its legal and ethical obligations, and to correct its course if it is not.

This list is not intended to be exhaustive, particularly as the full contours of the NCF's organisation and mission are not in the public domain. We therefore encourage continued attention to the NCF from a wide range of stakeholders, including: industry, academia, think tanks, civil society and the varied communities of cyber security policy and practice.

We do not attempt to outline a UK vision of overall cyber strategy, although the NCF will, of course, play a major role in delivering – and in so doing, developing – future iterations of national cyber strategy. Nor have we offered an analysis of international law as pertains to offensive cyber operations, or the doctrinal framework in which they may be deployed. Instead, we provide a modest set of recommendations to assist the UK government in considering the emerging role and responsibilities of the new National Cyber Force. The UK has an ambitious vision to conduct offensive cyber operations as part of a "much more integrated, creative and routine use of the UK's full spectrum of levers".[94] We offer this report to shape the public debate about how a responsible "democratic cyber power" should use its growing offensive cyber capabilities.

6. Abbreviations

ACD	Active Cyber Defence
CEMA	Cyber and Electromagnetic Activities
CyOC	NATO Cyber Operations Centre
DCMS	Department for Digital, Culture, Media and Sport
FVEY	“Five Eyes” intelligence alliance (Australia, Canada, New Zealand, UK, US)
GCHQ	Government Communications Headquarters
GGE	UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
IHL	International humanitarian law
ISC	Intelligence and Security Committee of Parliament
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NCA	National Crime Agency
NCF	National Cyber Force
NCSC	National Cyber Security Centre
NCSP	National Cyber Security Programme
NOCP	National Offensive Cyber Programme
NSA	National Security Adviser
NSC	National Security Council
SDSR	Strategic Defence and Security Review
SIS	Secret Intelligence Service (MI6)
SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies (NATO)
UN	United Nations
USCYBERCOM	US Cyber Command

About the authors

Dr Joe Devanny is Lecturer in National Security Studies in the Department of War Studies, King's College London. His research focuses on national security coordination and cyber strategy, including recent academic and thinktank publications on US cyber strategy and the ethics of offensive cyber operations. @josephdevanny

Dr Andrew Dwyer is an Addison Wheeler Research Fellow in the Department of Geography, Durham University. His research focuses on the role of automated decision making made by "artificial intelligence" applications in cyber security. He is co-director of the Offensive Cyber Working Group and was previously a postdoctoral researcher in usable security at the University of Bristol's Cyber Security Group. @DrAndrewDwyer

Amy Ertan (CISSP) is a Doctoral Candidate at the Information Security Group, Royal Holloway (University of London). She is a non-resident Visiting Scholar at the NATO Cooperative Cyber Security Centre of Excellence and a Cybersecurity Fellow at the Belfer Center for Science and International Affairs. Her research focuses on the emerging security challenges relating to military innovation, with a focus on "artificial intelligence"-enabled technologies. Amy is a co-director of the Offensive Cyber Working Group and has previously worked in strategic cyber intelligence roles @AmyErtan

Dr Tim Stevens is Senior 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), co-author of *Cyberspace and the State* (Routledge, 2011), and co-editor (with Amy Ertan and others) of *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (NATO CCD COE, 2020). @tcstvns

References

1. HM Government. 2021. *Global Britain in a Competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, 16 March, p. 21. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969402/The_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

2. HM Government. *Global Britain*.

3. HM Government. *Global Britain*, p. 14.

4. HM Government. *Global Britain*, p. 40.

5. https://www.kcl.ac.uk/research/kcl-cyber-security-research-group

6. https://offensivecyber.org/

7. HM Government. 2016. *National Cyber Security Strategy 2016-2021*, 1 November, pp. 17-19. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

8. HM Government. *National Cyber Security Strategy*, p. 19.

9. Alperovitch, D. and Ward, I. 2021. How should the US respond to the Solar-Winds and Microsoft Exchange hacks? *Lawfare*, 12 March. https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks

10. National Cyber Security Centre. n.d. Active Cyber Defence (ACD). https://www.ncsc.gov.uk/section/products-services/active-cyber-defence

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

12. HM Government. *National Cyber Security Strategy*, p. 51.

13. HM Government. *Global Britain*, p. 28.

14. Fleming, J. 2018. Director's speech at Cyber UK 2018. 12 April. https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018

15. Blitz, J. 2013. UK becomes first state to admit to offensive cyber attack capability. *Financial Times*, 29 September. https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de

16. HM Government. 2010. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 19 October, p. 27. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf

17. HM Government. 2015. *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, 23 November, p. 41. https://

assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf

18. HM Government. *National Security Strategy and Strategic Defence and Security Review*, p. 40.

19. Osborne, G, 2015. Chancellor's speech to GCHQ on cyber security. 17 November. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

20. Fallon, M. 2016. Defence Secretary's speech at the second RUSI Cyber Symposium. 20 October. https://www.gov.uk/government/speeches/defence-secretarys-speech-at-the-second-rusi-cyber-symposium

21. Fallon, M. Defence Secretary's speech at the second RUSI Cyber Symposium.

22. Fallon, M. 2017. Defence Secretary's speech at Cyber 2017 Chatham House Conference, 27 June. https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference

23. Cronk, T.M. 2016. US-UK cyber agreement opens doors for both nations. *DoD News*, 8 September. https://www.defense.gov/Explore/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/

24. Nakashima, E. 2017. US military cyber operation to attack ISIS last year sparked heated debate over alerting allies. *Washington Post*, 9 May. https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html

25. Nakashima, E. 2019. US Cyber Command operation disrupted internet access of Russian troll factory on day of 2018 midterms. *Washington Post*, 27 February. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

26. Lilly, B. and Cheravitch, J. 2020. The past, present, and future of Russia's cyber strategy and forces. In T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, and G. Visky, eds., *12th International Conference on Cyber Conflict – 20/20 Vision: The Next Decade*. Tallinn: NATO CCD COE, pp. 129-155.

27. Haynes, D. 2018. Britain to create 2,000-strong cyber force to tackle Russia threat. Sky News, 21 September. https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653

28. Wheeler, C., Shipman, T. and Hookham, M. 2018. UK war-games cyber attack on Moscow. *The Sunday Times*, 7 October. https://www.thetimes.co.uk/article/uk-war-games-cyber-attack-on-moscow-dgxz8ppv0

[29] Newton Dunn, T., Hamilton, R., Elliott, F., Evans, M. 2020. UK Targets Putin Allies. *The Times*, 24 October, Times2, pp. 1, 4. https://www.thetimes.co.uk/article/uk-targets-putin-allies-with-covert-attacks-hnl0nl27z

[30] Hannigan, R. 2019. *Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre.* Royal United Services Institute (RUSI) Occasional Papers, 27 February, p. 32. https://rusi.org/publication/occasional-papers/organising-government-cyber-creation-uks-national-cyber-security; Willett. M., 2020. Why the UK's National Cyber Force is an important step forward. International Institute of Strategic Studies, 20 November. https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force

[31] Fisher, L. 2019. Britain's parallel army of cyberwarriors. *The Times*, 17 August. https://www.thetimes.co.uk/article/britains-parallel-army-of-cyberwarriors-gzkzzdnvh

[32] National Audit Office. 2019. *Progress of the 2016–2021 National Cyber Security Programme*. 15 March. p. 47. https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf

[33] Corera, G. 2020. UK's National Cyber Force comes out of the shadows. BBC News, 20 November. https://www.bbc.com/news/amp/technology-55007946

[34] HM Government. *National Cyber Security Strategy*, p. 25.

[35] HM Government. *National Cyber Security Strategy*, p. 51.

[36] Wright, J. 2018. Cyber and international law in the 21st century. 23 May. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[37] HM Government. *National Cyber Security Strategy*, p. 18. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. At 15 March 2021, Geneva Internet Platform identified 23 countries with evidence of offensive cyber capabilities and a further 30 with indications of the same, https://dig.watch/processes/un-gge.

[38] Wright, J. Cyber and international law.

[39] Schmitt, M.N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Second edn. Cambridge: Cambridge University Press.

[40] Paris Call for Trust and Security in Cyberspace (n.d.) https://pariscall.international/en/. The US has, however, restated its commitments in other fora, e.g., US Department of State. 2019. Joint Statement on Advancing Responsible State Behavior in Cyberspace. 23 September. https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

41. Schmitt, M.N. 2018. In defense of sovereignty in cyberspace. *Just Security*, 8 May. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/; Kenny, J. 2021. France, cyber operations and sovereignty: the "purist" approach to sovereignty and contradictory state practice. *Lawfare*, 12 March. https://www.lawfareblog.com/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice

42. Wright, J. Cyber and international law.

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

44. UN General Assembly. 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 22 July. https://undocs.org/A/70/174

45. Smeets, M. 2018. The strategic promise of offensive cyber operations. *Strategic Studies Quarterly* 12(3): 90-113.

46. GCHQ. 2020. National Cyber Force transforms country's cyber capabilities to protect the UK. 19 November. https://www.gchq.gov.uk/news/national-cyber-force

47. Lonsdale, D.J. 2020. The ethics of cyber attack: Pursuing legitimate security and the common good in contemporary conflict scenarios. *Journal of Military Ethics* 19(1): 20-39.

48. Lucas, G. 2017. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare.* New York: Oxford University Press, pp. 40-41.

49. Barrett, E.T. 2013. Warfare in a new domain: the ethics of military cyber-operations. *Journal of Military Ethics* 12(1): 4-17.

50. Devanny, J. 2020. The ethics of offensive cyber operations. Foreign Policy Centre, 3 December. https://fpc.org.uk/the-ethics-of-offensive-cyber-operations/

51. GCHQ. 2018. The equities process. 29 November. https://www.gchq.gov.uk/information/equities-process

52. Schneider, J.G. 2019. Persistent engagement: Foundation, evolutions and evaluation of a strategy. *Lawfare*, 10 May. https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy

53. Healey, J. 2019. The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity* 5(1): tyz008.

54. Devanny, J. 2021. "Madman theory" or "persistent engagement"? The coherence of US cyber strategy under Trump. *Journal of Applied Security Research*, https://doi.org/10.1080/19361610.2021.1872359

55. Ministry of Defence. 2020. *The Integrated Operating Concept 2025*. 30 September. https://www.gov.uk/government/publications/the-integrated-operating-concept-2025

56. Smeets, M. 2020. US cyber strategy of persistent engagement and defend forward: Implications for the alliance and intelligence collection. *Intelligence & National Security* 35(3): 444-453.

57. Laudrain, A. 2019. France's new offensive cyber doctrine. *Lawfare*, 26 February. https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

58. Schulze, M. 2020. German military cyber operations are in a legal gray zone. *Lawfare*, 8 April. https://www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone; Federal Government. 2021. On the application of international law in cyberspace. March. https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf

59. Muller, L.P. 2019. Military offensive cyber-capabilities: Small-state perspectives. *NUPI Policy Brief* 1/2019. January. https://www.jstor.org/stable/resrep19882

60. Reuters. 2018. NATO cyber command to be fully operational in 2023. 16 October. https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9

61. Stoltenberg, J. 2019. Remarks at the Cyber Defence Pledge Conference, London. 23 May. https://www.nato.int/cps/en/natohq/opinions_166039.htm

62. HM Government. *Global Britain*, p. 20.

63. NATO. 2020. Allied Joint Doctrine for Cyberspace Operations AJP-3.20. January. https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320

64. HM Government. *Global Britain*, p. 40.

65. Corera, G. UK's National Cyber Force.

66. Ministry of Defence. 2021. *Defence in a Competitive Age.* CP 411. 22 March, p. 43. https://www.gov.uk/government/publications/defence-in-a-competitive-age

67. Bertrand, N. 2021. Biden taps intelligence veteran for new White House cybersecurity role. *Politico*, 6 January. https://www.politico.com/news/2021/01/06/biden-white-house-cybersecurity-neuberger-455508

68. Devanny, J. and Stevens, T. 2021. Written evidence submitted by Dr Joe Devanny and Dr Tim Stevens, King's College London (NSM0020), 19 March. UK Parliamentary Joint Committee on the National Security Strategy. https://committees.parliament.uk/writtenevidence/23898/pdf/

69. The Economist. 2020. Britain puts a new offensive cyber force at the heart of its defence. 1 December. https://www.economist.com/britain/2020/12/01/britain-puts-a-new-offensive-cyber-force-at-the-heart-of-its-defence

70. Ministry of Defence. *Defence in a Competitive Age*, p. 44.

71. For relevant insights into the development of cyber specialism within the US Armed Forces, see: Slayton, R. 2021. What is a cyber warrior? The emergence of US military cyber expertise, 1967-2018. *Texas National Security Review* 4(1). https://tnsr.org/2021/01/what-is-a-cyber-warrior-the-emergence-of-u-s-military-cyber-expertise-1967-2018/

72. Hannigan, R. *Organising a Government for Cyber*, p.31

73. Carter, N. 2019. Speech: Chief of the Defence Staff, General Sir Nick Carter's annual RUSI speech. 5 December. https://www.gov.uk/government/speeches/chief-of-the-defence-staff-general-sir-nick-carters-annual-rusi-speech

74. Fisher, L. Britain's parallel army.

75. Edmunds, T., Dawes, A., Higate, P., Jenkings, K.N. and Woodward, R. 2016. Reserve forces and the transformation of British military organisation: soldiers, citizens and society. *Defence Studies* 16(2): 118–136.

76. Hannan, N.K. 2015. Use of reserve forces in support of cyber-resilience for critical national infrastructure: US and UK approaches. *The RUSI Journal* 160(5): 46-50.

77. HM Government, 2021. New UK Cyber Security Council to be official governing body on training and standards. 9 February. https://www.gov.uk/government/news/new-uk-cyber-security-council-to-be-official-governing-body-on-training-and-standards

78. Prince, C. 2021. What the Integrated Review means for the UK's cyber strategy. Royal United Services Institution (RUSI), 23 March. https://rusi.org/commentary/what-integrated-review-means-uk-cyber-strategy

79. HM Government. 2021. International policy review puts cyber at the centre of the UK's security. 14 March. https://www.gov.uk/government/news/international-policy-review-puts-cyber-at-the-centre-of-the-uks-security

80. BBC News. 2021. Budget 2021: Darlington "Treasury North" move welcomed. 3 March. https://www.bbc.co.uk/news/uk-england-tees-56267333

81. Cronk, T.M. 2016. US-UK cyber agreement opens doors for both nations. *DoD News*, 8 September. https://www.defense.gov/Explore/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/

82. Gearson, J., Berry, P., Devanny, J., and Musgrave, N. 2020. The Whole Force

by Design: Optimising Defence to Meet Future Challenges. Serco Institute/ King's College London, p. 81. https://www.kcl.ac.uk/warstudies/assets/whole-force-by-design-serco-institute-kcl-report-final-13.10.20.pdf

83. HM Government, 2021. *Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors*. CP 410. 23 March, p. 21. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971983/Defence_and_Security_Industrial_Strategy_-_FINAL.pdf

84. HM Government. *Global Britain*, p. 40.

85. Ministry of Defence. *Defence in a Competitive Age*, p. 52.

86. Ministry of Defence. *Defence in a Competitive Age*, p. 45.

87. Ministry of Defence. 2016. *Cyber Primer*. Second edn. July. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf; Ministry of Defence. 2018. *Cyber and Electromagnetic Activities*. JDN 1/18. February. https://www.gov.uk/government/publications/cyber-and-electromagnetic-activities-jdn-118

88. Ministry of Defence. *Defence in a Competitive Age*, p. 44.

89. Borghard, E.D. and Lonergan, S.M., 2017. The logic of coercion in cyberspace. *Security Studies* 26(3): 452-481.

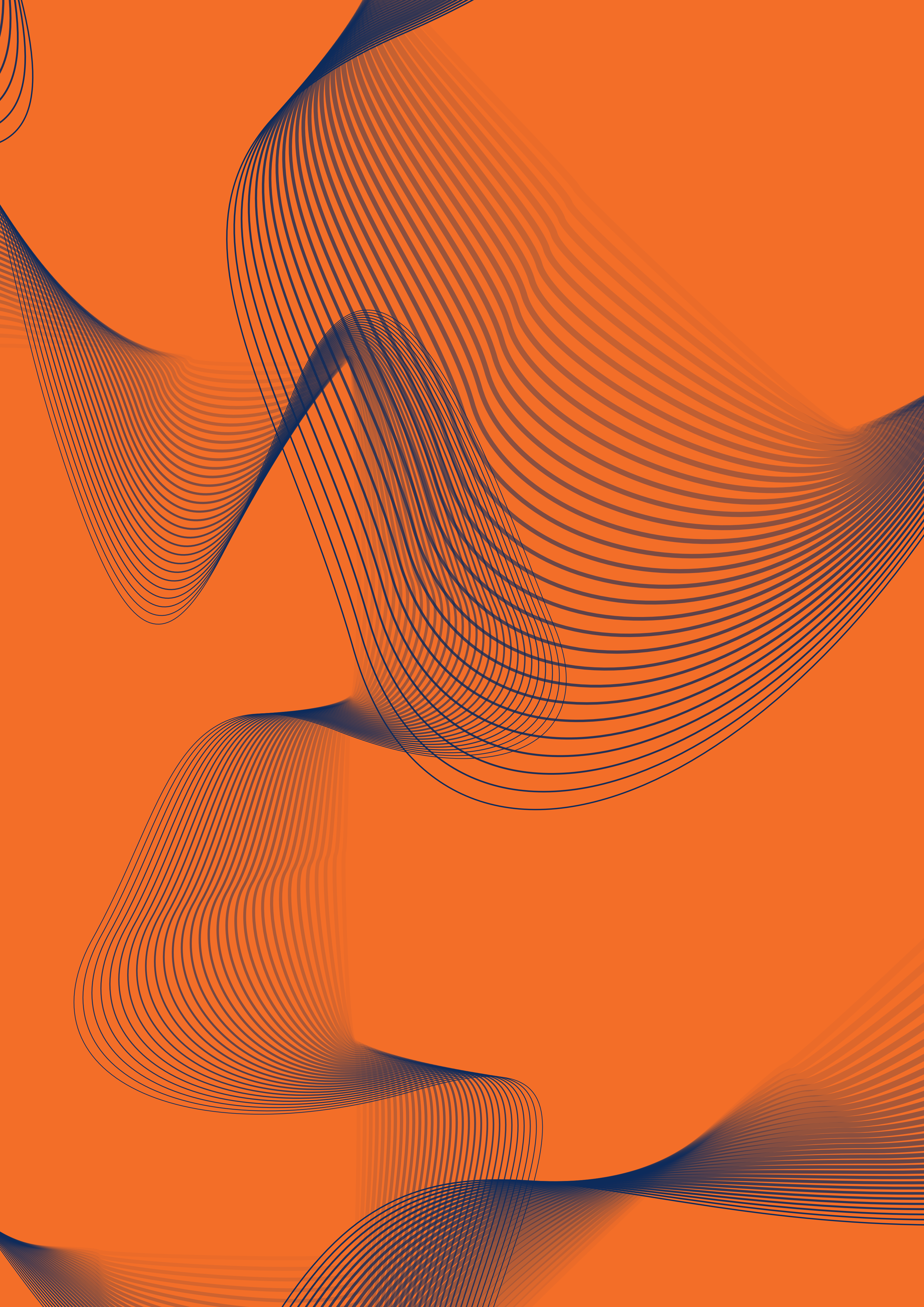
90. Rovner, J. 2021. Warfighting in cyberspace. *Lawfare*, 17 March. https://warontherocks.com/2021/03/warfighting-in-cyberspace/

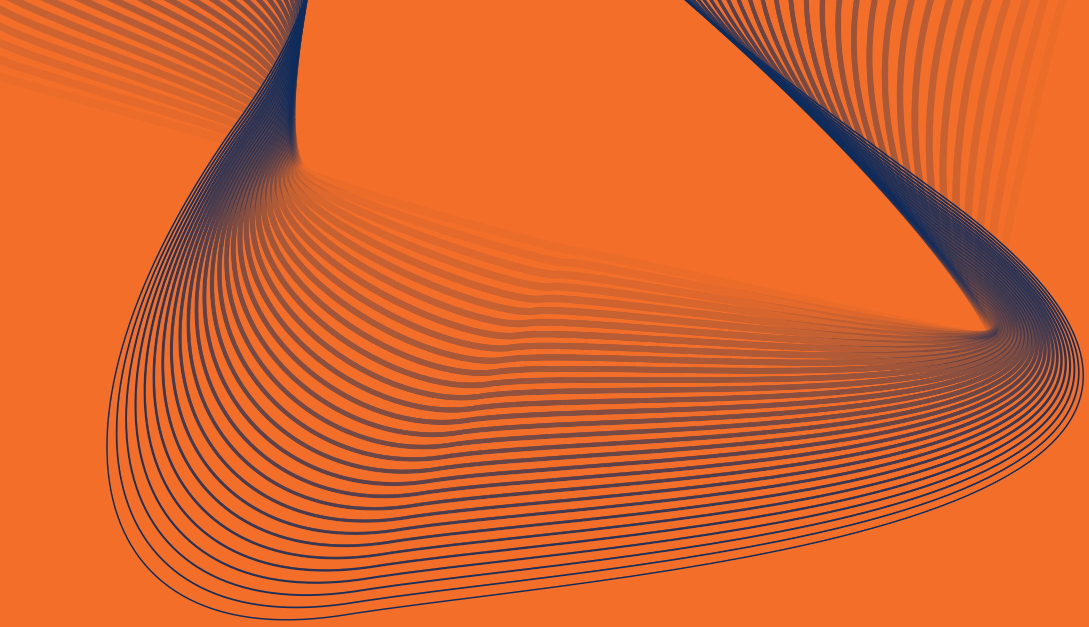
91. HM Government. *Global Britain*, p. 21.

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

93. GCHQ. National Cyber Force.

94. HM Government. *Global Britain*, p. 41.





Connect with us

@KCL_CSRG kcl.ac.uk/cyber-security-research-group

@Offensive_Cyber offensivecyber.org

@policyatkings kcl.ac.uk/policy-institute