The UK's Integrated Review and the future of cyber

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

Theme

Cyber is a centrally crucial element to the UK's future vision of national security. The *Integrated Review* considers cyber as a core component of national power, rather than a mere security issue in and of itself.

Summary

The long-awaited *Integrated Review* was released in March by the British government, promising the most radical shakeup in the UK's national security since the Cold War. Cyber in all its forms is weaved throughout the document; with a future vision to centre British national security around advanced technology, the bar for the next National Cyber Security Strategy (NCSS) has been set very high. This paper will examine what the *Integrated Review* indicates about the future directions for UK cyber, highlighting the key issues that the new strategy must address to fulfil the high ambitions set by British policymakers.

Analysis

The *Integrated Review* [1] is an ambitious document by any measure, seeking to comprehensively review in one report the UK's national security, defence, foreign policy and development agenda for years, even the decade, to come. Its coverage includes conflict and insecurity, an upscaling of deployable nuclear warheads, climate change and biodiversity, health resilience and an Indo-Pacific tilt in strategic focus to recognise the shifting power dynamics to the global south.

Despite this breadth of coverage, however, cyber is a centrally crucial component to the UK's future vision of national security, weaved throughout the *Integrated Review*. Simply put, the UK now sees cyber as a core component of national power, rather than a mere security issue in and of itself. However, the UK seeks to achieve its ambitions on the world stage post-Brexit with the application of cyber power will being central to the pursuit, and its importance to the *Integrated Review* must be examined.

Among the core of how the UK envisages this evolution taking place, the Foreign Secretary Dominic Raab's recent speech to the UK's *Cyber UK* 2021 conference serves as the best framework to consider its evolution. According to the Foreign Secretary, a modern cyber power is made up of three components, 'resilient defences, offensive

[1] Cabinet Office (2021), The Integrated Review, 16/III/2021, HMG, https://www.gov.uk/government/collections/the-integrated-review-2021.
[2] Foreign Commonwealth & Development Office (2021), 'CYBERUK conference 2021: Foreign Secretary's speech', 12/V/2021, https://www.gov.uk/government/speeches/cyberuk-conference-2021-foreign-secretarys-speech.

[3] GCHQ (2019), 'Director's speech on Cyber Power – as delivered', 29/III/2019, https://www.gchq.gov.uk/speech/jeremy-fleming-fullerton-speech-singapore-2019.

capabilities and global diplomatic clout…'.[2] This framework is clearly heavily informed by the GCHQ Director Jeremy Fleming's earlier speech to the International Institute of Strategic Studies in 2019, when he explicitly asked the question of what constitutes a cyber power. His speech identified the defence of the digital homeland, public trust and moral authority derived from legal and ethical frameworks, and the ability to project cyber capabilities as the answer.[3]

What does the Integrated Review say?

Due to the nature of the *Integrated Review*, with its very large coverage of numerous areas, there is a need to summarise the UK's view of cyber in the document. Immediately, the *Integrated Review* highlights the UK's current place as the world's third most capable cyber power, borrowing from the Harvard Belfer Center's *National Cyber Power Index* (NCPI) as its source.[4]

In his speech, GCHQ Director Jeremy Fleming defines a nation as a cyber power 'if it is able to direct or influence the behaviour of others in cyberspace'. Yet the *Integrated Review* introduces a more expansive, aspirational concept of the cyber power the UK wishes to be, that the UK should be a 'responsible, democratic cyber power' that abides a core principle, 'the digital age still requires us to be governed by the rule of law' according to the speech. The UK is positioning its behaviour and application of cyber power as one that uses these means for the benefit of the international community, in contrast to authoritarian regimes and criminal gangs who 'indiscriminately' use cyber-attacks for their own ends.[5]

But raises the question of why the UK needs to enhance itself as a responsible, democratic cyber power. The *Integrated Review* answers this by illustrating a far more challenging international arena: cyberspace 'will be an increasingly contested domain' in geopolitics where 'systemic competition will further test the line between peace and war'.[6] The use of cyber-attacks is one of many means employed by malign actors to achieve objectives 'without open confrontation or conflict'. This has led to the point where 'the international order is more fragmented, characterised by intensifying competition between states over interests, norms, and values.' In his above-mentioned speech, Foreign Secretary Dominic Raab described this situation as a 'clash of values' that is playing out between those states seeking to preserve an open order versus those promoting a more authoritarian vision.

[4] Julia Voo et al. (2020), 'National Cyber Power Index 2020', September, p. 8, https://www.belfercenter.org/publication/national-cyber-power-index-2020.

[5] Cabinet Office (2021), *op. cit.*, p. 40.

[6] *Ibid.*, p. 28 and 27, respectively.

[7] *Ibid.*, p. 11 and 18, respectively.

[8] *Ibid.*, p. 21.

[9] *Ibid.*, p. 55.

This situation results in a clear view on the part of the UK, that 'a defence of the status quo is no longer sufficient for the decade ahead' and as a result, the *Integrated Review* argues for 'shaping the international order of the future… in which open societies and open economies can flourish'.[7] The rest of the *Integrated Review* operates from this premise, whether focusing on the increase to the UK nuclear warhead stockpile, the Indo-Pacific tilt, or indeed cyber: the *Integrated Review* calls on the UK to recognise that the focus on maintaining the status quo from the end of the Cold War needs to be abandoned in favour of greater proactivity in 'dynamically shaping the post-COVID order'.[8]

The *Integrated Review* paints a challenging international picture for the UK and it also tables a high ambition for British policy but cyber especially. This leads to the question of how the UK will deliver on this ambition to not only shape the future international order, but to 'promote a free, open, peaceful and secure cyberspace'.[9] The answer, as Foreign Secretary Dominic Raab stated, lies in how the UK develops its resilience, offensive cyber and cyber diplomacy.

Domestic national resilience

If there is one word that most closely resembles British efforts on cyber security in the decade of the 2010s, it is resilience. Resilience has been the core byword against which national strategy efforts have so far been geared towards. In both the 2011[10] and 2016[11] versions of the NCSS resilience was a key objective and the strongest point of focus, as well as demonstrable success, for the UK.

The single clearest measure to achieve domestic national resilience was the establishment of the National Cyber Security Centre (NCSC) under the direction of the intelligence service GCHQ, which amalgamated numerous elements of disparate government departments that were operating in cyber security to centralise the NCSC as the 'national technical authority'. In its latest annual review, the NCSC had its busiest year yet to the end of 2020, handling 723 cyber security incidents and providing support to over 1,200 victims.[12]

The importance of resilience is noted in the *Integrated Review* with cyber security referred to as 'the foundation for cyber power' that the UK seeks to enhance.[13] Foreign Secretary Dominic Raab best detailed how the pathway to resilience will continue, when he said that the NCSC's Active Cyber Defence service is expanding outwards beyond just UK Government users to the wider society at large.

[7] Ibid., p. 11 and 18, respectively.

[8] Ibid., p. 21.

[9] Ibid., p. 55.

[10] HMG (2011), 'The UK Cyber Security Strategy', November, p. 21, https://www.gov.uk/government/publications/cyber-security-strategy.

[11] HMG (2016), 'National Cyber Security Strategy 2016-2021', November, p. 25, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[12] NCSC (2020), 'Annual Review 2020', November, p. 14, https://www.ncsc.gov.uk/news/annual-review-2020.

[13] Cabinet Office (2021), op. cit., p. 40.

Raab also made specific mention to measures beyond simply the technical to achieve resilience, reminding the audience at the Cyber UK conference that legislative measures are also in preparation. Specifically, the Online Harms Bill that aims 'to protect consumers from the harms associated with cyber-attacks on things like smartphones, smart TVs, cameras and speakers'. The enhancement of domestic national resilience is, therefore, not only a story of better technology, but also better legal frameworks to help ensure that technologies are both secure by design and subject to clear legislative requirements.

Despite the undoubted success of resilience efforts, however, the direction of travel for UK cyber clearly indicates that resilience alone is not enough. For all the success of the NCSC, the number and severity of incidents has been increasing year-on-year since its launch. The UK's efforts to build resilience are constantly matched –arguably even outpaced– by the incessant waves of cyber criminality and incidents. While resilience is the bedrock of cyber security across the UK, the number and severity of incidents and victims all serves to illustrate a broader yet unspoken truth that the *Integrated Review* moves on to addressing, that resilience alone is necessary but not sufficient to achieving the UK's cyber goals.

Offensive cyber operations

With the stated desire for the UK to reshape the future international order, the means to achieve such an aim must necessarily be proactive; for UK cyber power this means developing and using offensive cyber capabilities. The 2016 NCSS acknowledged the existence of a National Offensive Cyber Programme, yet any details about the programme and the UK's offensive cyber capabilities themselves have remained strictly classified.[14] While specific details remain classified, a big indicator arrived prior to the *Integrated Review* when the UK announced the formation of the National Cyber Force (NCF) in November 2020.[15]

The NCF was further detailed in the *Integrated Review*, being described as conducting 'targeted, responsible offensive cyber operations to support the UK's national security priorities, bringing together defence and intelligence capabilities'. These capabilities are drawn from GCHQ, the Ministry of Defence (MoD), the Secret Intelligence Service (SIS/MI6) and the Defence Science and Technology Laboratory (Dstl),[16] with the units' funding coming from the MoD.[17]

Beyond these rudimentary details, little is known about exactly what the NCF will do, yet there are some details given away elsewhere. According to the speech of the GCHQ Director Jeremy Fleming, the UK's development of offensive cyber capabilities began during the conflict in Afghanistan, noting that in 'recent years, we've worked even more

[14] Conrad Prince (2020), 'On the Offensive: The UK's New Cyber Force', 23/XI/2020, https://rusi.org/commentary/offensive-uk-new-cyber-force.
[15] GCHQ (2020), 'National Cyber Force transforms country's cyber capabilities to protect the UK', 19/XI/2020, https://www.gchq.gov.uk/news/national-cyber-force.
[16] Cabinet Office (2021), op. cit., p. 42.
[17] Ibid., Annex A, p. 101.

closely with the Ministry of Defence and key allies to grow these capabilities at pace'. And the use of these methods has continued in support of military operations in Iraq 'to disrupt Daesh's battlefield communications, which helped coalition forces to take ISIL fighters by surprise. Then again in Syria, we also impaired the ability of Daesh to produce and spread their poisonous propaganda.'

The big question, however, is not what the UK has done with its offensive cyber capabilities in the past, but what it intends to do with them in the future. How far exactly will the NCF be tasked to go in tackling cyber adversaries? Will this include state actors and risk escalation? Will there be take-down actions conducted against cyber-criminal groups based in other legal jurisdictions? Mission creep could be a real challenge facing the NCF and, as Devanny & Stevens point out, it will be constrained by its budget and size in what it can realistically achieve.

The NCF has an ambitious growth target to reach by 2030, roughly 3,000 staff, yet even that target would be less than half the size of the current US Cyber Command. Consequently, whatever the broad appetite the UK has, the NCF 'cannot perform all these missions equally well. Priorities will need to be established to help… focus its efforts and achieve optimum impact.'[18] How far the NCF operates simply to support the UK's armed forces remains open, versus carrying out independent operations beyond direct military support.

There are therefore two main tensions the UK needs to resolve in its development and use of offensive cyber through the NCF. First, how to reconcile the UK's pursuit of a broad agenda to reshape the future international order in cyberspace with cyber operations within stringent, and still nascent, resources. There is a risk simply that the UK's policy appetite is bigger than the means on offer to deliver. Secondly, can the UK preserve an open, peaceful, secure and free cyberspace while at the same time using offensive cyber capabilities that risk militarising the Internet further? How the UK applies its offensive cyber capabilities in practice will go far in displaying exactly how responsible and democratic the UK's cyber power truly is.

Cyber diplomacy

This brings focus to the realm of cyber diplomacy. It is clear that no actor can wield unlimited force in cyberspace, and that the best way for the UK to achieve its cyber aims and more is through influence. The *Integrated Review* details numerous areas where the UK is engaged in cyber diplomacy. Beyond the UK's on-going involvement with the UN bodies on cyber security –the Open-Ended Working Group (OEWG) and Government Group of Experts (GGE)– these include cyber security capacity building programmes and establishing cross-government dialogues with 20 countries.

The aim of UK cyber diplomacy is very simple, 'to grow the international coalition working with us to strengthen the case for a free, open, peaceful and secure cyberspace, and to respond to and deter state-directed malicious cyber activity'.[19] The clash of values that

[18] Joe Devanny & Time Stevens (2021), 'What will Britain's new Cyber Force actually do?', War on the Rocks, 26/V/2021, https://warontherocks.com/2021/05/what-will-britains-new-cyber-force-actually-do/.
[19] Cabinet Office (2021), op. cit., p. 45.

Foreign Secretary Dominic Raab referred to informs the desire of UK cyber diplomacy to ensure that cyberspace evolves 'in a way that reflects democratic values and interests'. This means increased support for the continuation of the multi-stakeholder model of Internet governance, but also a recognition of the need to respond to malicious actors and behaviour where 'we will shape new rules'.[20]

The UK's diplomatic objectives extend beyond just dealing with malevolent behaviour, however, there are three other objectives outlined in the document. First, ensuring the protection of human rights online in the same fashion as offline. Secondly, ensuring transparency and accountability in the design and deployment of new technologies. Third, championing the flow of data internationally to avoid any form of digital protectionism emerging.[21] UK cyber diplomacy is the arena where efforts stand to deliver the greatest impact, especially for the international community at large. Where disproportionate attention will no doubt be paid to the NCF and how the UK develops and uses its offensive cyber capabilities, it must be recognised that the vast majority of activities carried out by the UK will be aimed to influence and shape, not force, the future direction of Internet governance and online behaviours.

Cyber diplomacy is also the arena of arguably greatest opportunity for the UK in the years to come, with numerous friendly countries sharing similar interests in regions of vital importance to global geopolitics. Japan will be a crucial ally in the UK's Indo-Pacific tilt, the future relationship with the EU bloc can be greatly enhanced by UK progress in developing robust policy solutions that the EU may not, for simply two examples of where a post-Brexit UK can pursue new alignments in cyber diplomacy. This is of course in addition to continued participation within existing Internet governance mechanisms and contesting digital authoritarianism at the UN.

Resilience may offer tangible metrics to measure against, and the NCF will constantly grab headlines with the precedents it sets in defending the UK online, but the country's biggest battlefront in the geopolitical contest for cyberspace lies in diplomacy. This is because a pure reliance on resilience and offence alone can only guarantee an increasingly militarised cyberspace, where one's offence is hoped to craft a suitable deterrent against attacking UK interests for fear of reprisals. Instead, cyber diplomacy stands to grow the coalition of those who wish to see an open cyberspace maintained for all, where malicious behaviour is both made technically harder to achieve as well as adhered to in normative frameworks. Bilateral dialogues and agreements will be pivotal in weaving a global web of cyber alliances that serve both UK interests and safeguard the free and open cyberspace sought after.

Conclusion

To conclude, the Integrated Review places the UK on a bold new footing for its approach to cyber moving ahead. It has graduated the place of cyber from the mere security issue it was labelled as over a decade ago to a now fully-fledged instrument of national power. Furthermore, the UK has shown its desire and intention to enhance its cyber power not

[20] Ibid., p. 56.

[21] Ibid., p. 57.

only to protect itself, but to take a leading role in reshaping the post-COVID international order and ensure that cyberspace continues to reflect democratic values and interests.

Despite acknowledgement of the very big and laudable objectives the UK has shown in the *Integrated Review*, it must be noted that the document sets an incredibly high bar for the still upcoming *National Cyber Security Strategy* to reach. The UK has high-minded ambitions but ultimately very finite resources, and it must achieve them while also needing to contend with the challenges of economic recovery following the COVID pandemic. For the *National Cyber Security Strategy* to be a credible path to these objectives, it must provide a realistic blueprint for mission achievement that sets incredibly clear priorities for the various elements of UK cyber power to pursue.

The latest version of the *National Cyber Security Strategy* put forward a three-D articulation of the UK's strategy between 2016 and 2021: Defend, Deter, Develop.[22] The *Integrated Review* seems to have already given advance notice of the new three-D formula the UK will table in the new *National Cyber Security Strategy*: Detect, Deter, Disrupt.[23] The reflex to simple, marketable formulas risks instituting short-sightedness on the part of policymakers, who must bridge resilience and offensive cyber to wider diplomacy. In short, the next *National Cyber Security Strategy* must also include a full acknowledgment of the place, role and importance of diplomacy in achieving British objectives. With this in mind, the UK should consider adding a fourth D, Dialogue.

The *Integrated Review* most certainly has placed the UK on the correct path in its development of cyber power, certainly in rhetoric. In graduating cyber from a security issue to a matter of geopolitical importance and an instrument of national power, the UK has recognised the greatest weakness from its previous strategy, its failure to robustly engage the international arena in cyber. The focus on resilience has of course been necessary, but the evidence is clear: resilience is not a sufficient condition to achieve the future for cyberspace the UK wishes to achieve. The *Integrated Review* signals the UK's intent to move into its post-Brexit future by shaping the future international order, including cyberspace. The challenge now is how exactly to achieve that, which is a question the next *National Cyber Security Strategy* must answer.

[22] HMG (2016), op. cit., p. 9.
[23] Cabinet Office (2021), op. cit., p. 40.