

Written evidence submitted by Dr Joe Devanny and Dr Tim Stevens, King's College London

Key Points

- The new National Security Adviser should commission a wide-ranging review of the units, structures and processes at the centre of government to support the National Security Council (p.1).
- The new NSA should consider creating a deputy National Security Adviser position exclusively for cyber strategy and coordination, science and technology, emulating a similar appointment in the Biden administration's National Security staff (pp.2-3).
- In the longer term, improving effective coordination of cyber across government might require more extensive reform, beyond the national security machinery at the centre (p.3).

Context

This evidence is submitted as a short proposal to the Joint Committee on the National Security Strategy's (JCNSS) inquiry into the UK National Security Machinery. It follows – but is independent of – previous submissions to this inquiry by several of our colleagues in the Department of War Studies at King's College London (NSM0002, NSM0008, and NSM0009). It draws principally on the authors' research on UK national security coordination¹ and cyber strategy.²

Details

This written evidence proposes that **the Cabinet Office should convene a three-month review of the units, structures and processes supporting the National Security Council (NSC)**. It is the right time to commission such a review, given Stephen Lovegrove's recent appointment as the fifth substantive National Security Adviser (NSA) since the post's creation in 2010.

The evidence provided to this inquiry by the Cabinet Office states that a 'rapid' review of implementation will be conducted.³ Respectfully, this might be the wrong approach. Review of implementation should not be separated from review of pre-decision advice, structures and processes.⁴ In contrast, we propose that the review should be holistic and given sufficient time to examine issues thoroughly, leading to useful recommendations across all aspects of the centre's support for the NSC. The review would ideally be led by someone outside the Cabinet Office, independent but commanding the confidence of the NSA to produce a rigorous report and constructive recommendations. Several former senior officials – some of whom have contributed to your inquiry – would be good candidates to lead such a review.

¹ See, for example: Joe Devanny and Josh Harris, 2014. *The National Security Council: National security at the centre of government*. Institute for Government; Joe Devanny, 2015. Co-ordinating UK Foreign and Security Policy. *The RUSI Journal* 160(6): 20-26, DOI: [10.1080/03071847.2015.1122977](https://doi.org/10.1080/03071847.2015.1122977)

² Joe Devanny, 2020. The Ethics of Offensive Cyber Operations. *Foreign Policy Centre*, <https://fpc.org.uk/the-ethics-of-offensive-cyber-operations/>; Joe Devanny, 2021. 'Madman Theory' or 'Persistent Engagement'? The Coherence of US Cyber Strategy under Trump, *Journal of Applied Security Research*, DOI: [10.1080/19361610.2021.1872359](https://doi.org/10.1080/19361610.2021.1872359); David J. Betz and Tim Stevens, 2011. *Cyberspace and the State: Toward a Strategy for Cyber-power*. London: International Institute for Strategic Studies; Amy Ertan, Kathryn Floyd, Piret Pernik, and Tim Stevens (eds.), 2021. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinn: NATO CCD COE; Joe Devanny, Andrew Dwyer, Amy Ertan, and Tim Stevens, *The National Cyber Force that Britain Needs?* London: The Policy Institute at King's College London (forthcoming).

³ HM Government, 2021. Written evidence submitted by the Cabinet Office, 21 February, NSM0019, 2, <https://committees.parliament.uk/writtenevidence/23130/pdf/>

⁴ *Ibid.*

Such a review is unlikely to be published, but the Cabinet Office would benefit generally from better communication about national security developments at the centre.⁵ It might therefore consider the timely publication of a sanitised summary of the review's findings.

The review should consider the fluctuating size and configuration of central national security arrangements – whether styled as a secretariat or different units – since the creation of the NSC in 2010. It should audit the workforce strategy relating to existing staff, roles and expertise, identifying consequential gaps and ways to fill them. One example should be the configuration of senior advisory roles under the NSA. The number of deputy NSAs and their portfolio divisions has fluctuated under different NSAs. This is understandable: NSAs come to the role with distinct career experiences and benefit from different configurations of supporting officials. Some issues, however, would gain from more sustained and continuous top-level focus, notwithstanding the background and preferences of each incoming NSA.

One of these is cyber strategy: **the review should consider creating a deputy NSA role focused primarily on cyber strategy and coordination, as well as the wider science and technology agenda highlighted by the Integrated Review.** There should be a deputy NSA with bandwidth to coordinate across and beyond government (e.g., with the private sector, civil society, and with counterparts overseas) on all aspects of cyber strategy, encompassing cyber security, digital espionage, and offensive cyber operations.⁶ A deputy NSA (Cyber, Science and Technology (CST)) would, for example, be the obvious person to lead an audit of cross-government cyber workforce strategy. This would be consistent with the recent pledge in the Integrated Review to pursue a 'more coherent approach' to cyber strategy, including the issues of skills and recruitment.⁷ Given that the Integrated Review situates cyber within a broader prioritisation of science and technology, it would be appropriate for one deputy NSA to own the whole CST portfolio.

The Biden administration recently drew a similar conclusion about the need for such a role, creating a deputy NSA for cyber and emerging technologies on the White House national security staff. The UK should not do this simply because the US government has, but there is value in having clear counterparts, as the existence of the NSA role itself demonstrates. Nor is the current situation regarding UK cyber strategy coordination identical with the situation inherited by the Biden administration from its predecessor.⁸ The UK should do this, primarily, because major issues of government strategy require coordination and it is striking that a deputy NSA-level cyber-focused position has not yet been created to lead that effort from the Cabinet Office.

The current alternative does not afford sufficient bandwidth to focus on these issues: the intelligence, security and resilience portfolio is simply too broad. It should be re-distributed into a series of more streamlined and focused deputy NSA portfolios. Whilst different senior officials in the national security apparatus have always had cyber responsibilities in their wider portfolio, there is a sufficient quantity of high-priority, cross-government and whole-

⁵ For example, few appointments below NSA-level are consistently announced or published accessibly.

⁶ For one illustration of some of the issues to be addressed in the UK government's approach to the development and use of offensive cyber capabilities, see Devanny, 2020. *The Ethics of Offensive Cyber Operations*.

⁷ HM Government, 2021. *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, CP403, 16 March, 41, <https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy>

⁸ For an overview of US cyber strategy under Trump, see: Devanny, 2021. 'Madman Theory' or 'Persistent Engagement'?

of-system work across the full spectrum of cyber strategy – and the growing role of science and technology in UK strategy – to merit the creation of such a senior position solely focused on these issues. The creation of the deputy NSA (CST) role would sensibly be supplemented with a larger unit of officials working on CST, reporting directly to the new deputy. It would be prudent for the NSC to reconstitute a sub-committee on Cyber to reflect ministerial recognition of the national security priority of cyber strategy. The deputy NSA would logically act as Secretary of this sub-committee, and also Chair of its flanking (Officials) committee to shepherd its deliberations and follow-up. It is currently unclear to what extent – and in what ways – the absence of a sub-committee of the NSC will be mitigated by the Integrated Review’s announcement that the government has ‘formed a ministerial small group to cohere cyber decision-making across government.’⁹ Without further details of the small group and its operation, this might be a distinction without a difference. But the creation of a more senior role to lead on cyber strategy and coordination from the Cabinet Office would most probably only improve the supporting arrangements enabling the effectiveness of that ministerial group.

A deputy NSA (CST) would be an incremental improvement, not a panacea. Deeply-embedded challenges must be overcome if government is to implement a coherent cyber strategy. It must ensure the right balance between cyber defence, cyber security and offensive cyber. Furthermore, it is presently unclear who, if anyone, is responsible for ensuring the integration of cyber with related cross-government strategies for data and digital. The centre’s shaping, convening and brokering roles in addressing these issues transcend the narrow, traditional sphere of national security. In the longer term, one solution might be to create a more expansive, high-level role: a permanent-secretary grade post of Prime Minister’s Adviser on Cyber, Data, Digital and Technology. Such a role would entail its own problems – not least in clarifying a division of responsibilities with the NSA – but it would underline the cross-cutting nature of these issues and the need for high-level leadership from the centre.

There is long-standing recognition that cyber strategy is a top national priority. This is evident, for example, in three iterations of national cyber security strategy since 2009. It is therefore an aberration that the centre of government does not currently have a director-general level official solely focused on cyber strategy and coordination. It is similarly unfortunate that the ministerial sub-committee of the NSC focused on cyber, which had been chaired by a senior Cabinet Minister during the first half of the NSC’s existence, subsequently fell through the cracks of the transitions between successive Prime Ministers.

In this respect, the new ministerial small group on cyber could be a welcome development, although its membership, remit and supporting structures should be clarified and, where necessary, enhanced. The centre of government needs to exercise a strong grip in shaping and implementing a comprehensive, whole-of-system cyber strategy – or, as the Integrated Review somewhat inscrutably calls it, a ‘whole-of-cyber’ approach to cyber strategy.¹⁰ Particularly with the Integrated Review’s emphasis on cyber and wider science/technology dimensions of national security and international policy, the recommendations in this submission aim to elevate and improve central capacity to support the NSC in pursuing these objectives.

⁹ HM Government, *Global Britain in a competitive age*, 40.

¹⁰ *Ibid.*

Dr Joe Devanny is Lecturer in National Security Studies in the Department of War Studies, King's College London. He co-convenes the National Security Studies postgraduate module and short course. His research focuses on national security coordination and cyber strategy.

*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 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 of *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (NATO CCD COE, 2020).*

19 March 2021