https://www.gov.uk/government/publications/integrated-review-call-for-evidence

Integrated Review: Call for Evidence response template

It is recommended that you read the full call for evidence document before completing your response. Please note that the text boxes used in this template can be expanded to accommodate additional text.

Guidance for respondents

- In your response, please clarify which questions you're answering, by referring to the relevant numbers assigned to each question.
- You do not need to respond to all of the questions if they are not all relevant to you, and you may wish to provide a single answer to multiple questions.
- The questions asked are very broad in nature. This is to give you the scope to focus on a specific sub- issue or priority, according to your own, or your organisation's, area of expertise.
- There is no minimum word limit. We strongly encourage a maximum limit of 500 words per question (not including references). We recommend providing responses which contextualise, and summarise the key points of, the evidence they reference, as these are likely to be most effective. Given the volume of responses expected, submissions exceeding this recommended length may not be read in their entirety.
- Please include references in your response where applicable. We request that you include a bibliography at the end of your response, within the box provided. This does not count towards the recommended word limit.

Responses should arrive no later than **Friday 11:59pm BST on 11th September 2020,** with early responses encouraged where possible.

For further information on how we handle your personal data please read the Integrated Review Call for Evidence Privacy Notice.

Please send your response, attaching the papers you have referenced, to:

IRcallforevidence@cabinetoffice.gov.uk

Or alternatively by post to:
Integrated Review Team,
Cabinet Office,
70 Whitehall,
London,
SW1A 2AS

Quoting the reference "**Integrated Review Call for Evidence 2020**"

General Information

1. **Full name (including title)**

Prof. Chris Johnson

2. **Mark the statement below [X] as applicable.**

[X] I have read the Integrated Review Call for Evidence Privacy Notice and understand that any responses submitted by organisations or representatives of organisations may be published in full.

2. **Are you responding (please mark the relevant box [X]):**

[] as an individual (please complete 3 to 5 below)

[X] on behalf of an organisation / company (please complete 6 to 9 below)

If you are responding as an individual:

3. **E-mail address**

4. **Address**

5. **Please mark the statement below [X] as applicable.**

[] I have read the Integrated Review Call for Evidence Privacy Notice and am content for my name to be published alongside my response.

[ ] I have read the Integrated Review Call for Evidence Privacy Notice and am not content for my name to be published alongside my response.

The Privacy Notice can be found on the Integrated Review Call for Evidence webpage.

If you are responding on behalf of an organisation / company:

6. **Organisation / Company**

UK Computing Research Committee (UKCRC)

The UK CRC is an Expert Panel of all three UK Professional Bodies in Computing: the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

7. Position within Company / Organisation

Executive committee member responsible for government/parliamentary consultations

8. E-mail address

c.w.johnson@qub.ac.uk

9. Address

Prof. Chris Johnson, FRSE, FRAeS, FBCS,
Pro Vice Chancellor - Engineering and Physical Sciences,
Queen's University Belfast,
6-8 Malone Road, Belfast, BT7 1NN.

Call for Evidence questions

1. What are the key opportunities, challenges, threats and vulnerabilities facing the UK now? (Submissions focusing on rapidly evolving areas such as science, technology, data, cyber, and space are particularly welcome.)

2. What are the key global and domestic trends affecting UK international policy and national security out to 2030, and how should the government prioritise its efforts in response to these?

3. What are the key steps the UK should take to maximise its resilience to natural hazards and malicious threats? How can we build a whole of society approach to tackle these challenges?

4. What are the most effective ways for the UK to build alliances and soft power?

5. What changes are needed to Defence so that it can underpin the UK's security and respond to the challenges and opportunities we face? (Submissions focusing on the changing character of warfare, broader concepts of deterrence, technological advantage and the role of the Armed Forces in building national resilience are particularly welcome.)

6. How should the UK change its governance of international policy and national security in order to seize future opportunities and meet future challenges? (Submissions focusing on the engagement of an increasing range of stakeholders while maintaining clear responsibility, accountability, and speed of action are particularly welcome.)

7. What lessons can we learn from the UK's international delivery over the past 5 years? Which are the key successes we should look to develop and build on, and where could we learn from things that didn't go well?

8. How should UK systems and capabilities be reformed to improve the development and delivery of national strategy?

Please provide your response in the box below. Make sure to note the "Guidance for respondents" provided above before completing.

- *What are the key opportunities, challenges, threats and vulnerabilities facing the UK now? (Submissions focusing on rapidly evolving areas such as science, technology, data, cyber, and space are particularly welcome.)*

Opportunities: Achieving the UK's ambition to achieve top tier status in Science and Technology, building on key national strengths for example in Data Science, demands that Her Majesty's Government (HMG) takes an active, forward-leaning approach, preserving the benefits of our current open Science and Technology ecosystem while taking a more deliberate, long term-approach to identifying and incentivising Science and Technology developments. HMG needs to work with UK Computing research across academia and industry to deliver UK strategic advantage in security, resilience and global influence.

Challenges: This is dependent not just on nurturing our research, development and innovation infrastructures but also on investment in the people and capabilities that protect our Scientific, Technological and Data assets. The UK needs to protect technological innovations and IPR without undermining the free exchange of ideas that underpins Open Science. The inherent contradiction between these two requirements will be a key challenge for UKRI and for any future ARPA agency in sustaining **and** protecting our Science and Engineering base.

Our ability to effect and support digital transformation depends on international supply chains – that include both technological systems of systems but also intellectual capital – some of which is based in states that may not be entirely aligned with UK policy. China's key role in shaping and contesting the landscape in Science, Technology and Data requires us to build our capability here, too.

Connected to our dependency on international supply chains, is the recognition that the UK lacks influence over key scientific and engineering organisations that will have a direct impact on our future security, resilience and prosperity. The UK needs to gain more control of and influence over international ICT initiatives, especially the Internet —we have had patchy involvement and influence. Similar comments might be made over our involvement in international initiatives for cyber security, via for example ICSPA https://icspa.org/. We cannot simply focus our involvement on the Five Eyes when mutual inter-dependencies stretch way beyond our immediate and preferred partners.

The loss of civilised behaviour "at the top" is an enormous danger, even in our allies and notably in the USA. Asserting UK presence is vital, focusing on science and engineering — building on the huge body of talent in Universities, and not just in the 'obvious' places. Matching the right individuals to the leadership roles that are needed is an urgent task — notably for UK ARPA.

Threats: Small changes in policy can have massive implications for the UK Science, Technology and Data landscape. The recent debate over the future of 5G and new initiatives in enforcing 'secure by design' requirements on digital and IoT infrastructures provide examples. UK Computing Research is ready to respond to the changes in policy that are a direct response to threats to both national and personal security. However, delays in the funding mechanisms and other supporting measures that help industry and academia meet these new threats means that the UK remains vulnerable long after the policy has changed.

More specific threats include the immediate challenge to democracy posed by the indirect influence of social media and digital information channels. It is unclear that DCMS or OFCOM have sufficient technical resources to address these challenges in a coherent manner.

Vulnerabilities: The UK is increasingly vulnerable through our dependency on global supply chains and yet at the same time, the diversity of potential partners post Brexit creates opportunities to increase resilience in key areas. This may, however, imply a degree of guidance from regulatory agencies that are poorly resourced to provide the support that industry requires – for instance, to ensure that our critical infrastructures do not all purchase industrial control systems from a single supplier or several from the same nation. There is an urgent need for HMG to work with the NCSC and the UK Computing Research Community in innovative ways – for example through secondments and joint PhDs to ensure that government departments including BEIS, DCMS and FCO as well as the regulatory agencies – especially the HSE, CAA, OFGEM etc have sufficient technical

and intellectual capital to identify and intervene in a minimal manner to mitigate these growing dependencies and vulnerabilities.

- *What are the key global and domestic trends affecting UK international policy and national security out to 2030, and how should the government prioritise its efforts in response to these?*

The UK needs to regain its position as a major, independent player on the world stage – the loss of the EU as a platform for cooperation and joint leadership creates opportunities but leaves us exposed. The scale of funding available for research and development across the defence, security and intelligence industries in the EU and in North America raises significant and sustained questions about the ability of the UK to keep pace or make advances without specific and detailed agreements and with sufficient financial support.

Post Covid, resilience and systems thinking should become a focus for new forms of cooperation between government, industry and academia. There have been notable successes – for example, the NCSC/EPSRC Research Institutes in cyber-security that bring together these different stakeholders. However, there continue to be tensions between the priorities of the research funding bodies and those of the NCSC – Cyber Security has come from the National Cyber Security Programme rather than from the Science budget. The defence review provides us with an opportunity to rethink the future Academic Centres of Excellence. One aspect of this is to create a new vision of the role for UK research organisations, especially Universities, in creating thought leadership for national resilience. If our aim is a general raising of educational levels around cyber security, and a general growth of the research base, then the most appropriate route would be through the Science budget and within normal University funding for undergraduates. Alternatively, the UK may need to develop a closer relationship between the NCSC and the resources across our Science and Technology landscape – especially to address the growing attack surface and supply chain dependency. This requires more focussed, dedicated funding mechanisms than exist today. Both approaches need to be underpinned with the understanding that many future problems will be caused not just by cyberattacks but by challenges of many sorts including natural disasters and failures around ICT and software (esp. critical infrastructure and services).

The government should prioritise its efforts to reshape, and where necessary, create a scientific strategy and intelligence function. At present, individuals with appropriate skills are scattered through individual government departments and funding councils. However, their insights are almost never coordinated; they lack power and agency – there is no common or coherent voice helping inform policy with a clear vision of how science and technology can be harnessed to address the global challenges and opportunities identified in our response to point 1 (above). Globally there is a cohort of nations who have achieved this vision (most notably Singapore, Israel) and they consequently punch above their weight in many areas of intelligence, resilience and security.

In order to achieve this vision, we need:

a) **Better foresight** through a science and technology scanning function, integrated across-government, which can access high quality evidence and expertise from academia, private sector, and other areas of government. This would deliver deep insight into adversary ambition and capability; and would provide mechanisms to understand the 'so what' (risks, opportunities, implications) for our National Security mission and interests. As a specific example, the creation of a resilient and secure society in a post-quantum world is a focus for such a 'so what' analysis that needs to be aligned with policy and technology.

b) New analysis capabilities to dissect **Science and Technology as a domain of strategic advantage;** understand the UK's position within the competitive global landscape; to identify where and how UK advantage can be generated; and to couple this to the mechanisms for generating that advantage.

c) To **expand and diversify our reach into the innovation ecosystem**, creating and supporting markets and securing supply chains that will deliver the technology on which our future national interests and NS mission depend. This requires a portfolio approach that gives us enough depth on high-risk but potentially game-changing Big Bets and delivers optionality in our technology choices. We must translate cutting-edge technology into strategic advantage and Mission capability. This requires collaboration across research, industry and government that ignores traditional boundaries and divisions between disciplines and is sensitive to the need for a systemic, socio-technical systems perspective to these topics.

d) To **deepen the relationship between National Security and the research base**, leveraging this for mutual benefit.

e) To **step up the underpinning science capabilities that support our National Security Mission**, and partner with world-class Centres of Excellence to mutual benefit. We will secure our tier 1 position in critical National Security-relevant capabilities, e.g., Cryptography as a core component of our "Great Science Power" status and global influence.

f) R&D investments and partnerships that enable us to **keep pace with our most capable adversaries in cyber defence** (and offence), underpinning our ability to protect UK data, and our increasingly digitised critical infrastructure.

We need to achieve all of these aims within policies, processes and organisational structures that enable people to thrive – economically, socially, creatively and without undermining the core values and beliefs shared by the different communities that together help unite our Nation.

- *What are the key steps the UK should take to maximise its resilience to natural hazards and malicious threats? How can we build a whole of society approach to tackle these challenges?*

Resilience tends only to be taken seriously after major incidents – this creates problems because consequent investments tend to focus on the previous contingency without considering the broader range of future threats and vulnerabilities. We would welcome a sustained effort whereby approaches to resilience are seen as vital for the UK's future;

Cabinet office plays a critical role in coordinating a unified national programme that has been weakened in recent years because many relevant issues have been split between a multiple of departments and agencies that are more or less prepared to meet their obligations. As a specific example, although DCMS has coordinated significant change in the implementation of the NIS directive, these changes have been very inconsistent across the different lead Departments/Competent Authorities in various industries. In consequence, it is clear that some areas of our critical infrastructure are significantly more resilient than others.

It is also important to learn from the integrated and "systems of systems" approach adopted by some non-government agencies to aspects of these topics. For instance, the activities of the BSI in City Resilience, Smart and Sustainable Cities and Communities, and in other, related areas of standardisation are excellent examples of the systemic approach. There is much potential for innovation and also employment in infrastructure and services (and research and development).

There is a chronic lack of coordination at every level between those agencies dealing with natural hazards and those dealing with malicious threats. Some areas are considering the confluence of these – where an adversary uses a natural hazard to exacerbate or mask other forms of attack but our level of preparedness mirrors that for pandemics in 2019.

- *What are the most effective ways for the UK to build alliances and soft power?*

Post-Brexit we see the need to reach out to other countries and administrations in a spirit of cooperation and help but also to be clear about local and regional strategies in a coherent manner. Often research funding – for example through GCRF and the Newton fund, delivers piecemeal support for our partners without any longer term sustained benefits in terms on influence or strategic regional relationships. These schemes have tended to favour traditional approaches to development research – very few offer coherent systemic improvements in underlying technological infrastructures which forms a strong contrast with the approach being adopted by Chinese investments and partnerships. We welcome the integration of the Department of Foreign Aid and the FCO as a first step in this more strategic and regionally focussed vision of intelligence, security and defence – especially where there is some consideration of our key dependencies on, as well as diversity in, international supply chains.

We also encourage greater and more active participation in research initiatives promoted by major international organisations, such as the UN, NATO, and the OECD. One proposal might be to support/create research offices to help replace the mechanisms that delivered significant success for UK computing research in European partnerships and consortia.

- *What changes are needed to Defence so that it can underpin the UK's security and respond to the challenges and opportunities we face? (Submissions focusing on the changing character of warfare, broader concepts of deterrence, technological*

advantage and the role of the Armed Forces in building national resilience are particularly welcome.)

We foresee greater interaction between the physical and cyber domains with levels of capability in one area that compensate for weaknesses in others – enabling countries to have considerable impact on an adversary's physical forces without themselves having comparable conventional assets. We also foresee the ability for adversaries to have a growing range of physical effects on UK critical infrastructure that stop short of outright conflict – for example, slowing the exchange of air traffic control data on domestic flights every time a Royal Navy vessel enters the South China sea. There is, therefore, a need to combine technical insight with a detailed knowledge of policy, diplomacy and of envisonment to help anticipate future threat scenarios. Existing military structures within the UK often place cyber capability in specialist units that lack clear interaction with the higher-level policy considerations. These have little or no interaction with the private sector critical infrastructure providers and sometimes little interaction with colleagues in the intelligence agency. Our assets are too few, dispersed and uncoordinated.

- *How should the UK change its governance of international policy and national security in order to seize future opportunities and meet future challenges? (Submissions focusing on the engagement of an increasing range of stakeholders while maintaining clear responsibility, accountability, and speed of action are particularly welcome.)*

This has been addressed in each of the previous sections.

In terms of international strategy, we would argue for a rejuvenation of the research links with the Five Eyes or CANZUK countries to mirror strategic intelligence, security and defence relationships. There have been one-off grant calls, but few opportunities for joint research programmes in the longer term, or sustained exchanges of students or staff. We need science and engineering teams in the UK to have an exposure to wider ideas within their own disciplines but also the different industrial, regulatory and policy contexts that characterise our closest allies.

We would also benefit from a more joined-up approach to the promotion of UK capability in these strategically important areas. The UK presence at major international events in cyber security has for too long seemed to be archaic and amateur in comparison to competitor nations.

A UK ARPA could bring fast understanding and solutions in these important areas. Otherwise, Universities in all their diversity can and should act as a tremendous resource for future thinking and practice.

- *What lessons can we learn from the UK's international delivery over the past 5 years? Which are the key successes we should look to develop and build on, and where could we learn from things that didn't go well?*

Previous sections have argued for the need to re-establish the UK's leading presence – through the capabilities of science and engineering as well as in the arts and design areas. We have in the past been leaders of systemic forms of analysis as well as the underlying core disciplines – however, we have been extremely bad at integration these different traditions and at using these capabilities in a way that increases national resilience.

- *How should UK systems and capabilities be reformed to improve the development and delivery of national strategy?*

The defence review creates a range of new opportunities informed by the concerns identified throughout his response:

a) We must **understand the S&T-driven threats and vulnerabilities** most critical to our national interests, NS mission and operating model, and be able to exploit that knowledge to our advantage.

b) A system to **weigh the benefits and risks of international collaboration** on a scale that is calibrated to our strategic national goals: coupling strategic decisions on where the UK wants to 'own', 'collaborate' or 'access' technology to decisions around the nature of the collaborative partnerships we build, and to the mechanisms for balancing opportunity and risk (investment screening, evaluating risk in R&D collaboration).

c) Engagement and outreach that enables **a mindset shift that helps secure the integrity of our research and innovation system**: from sensitive research, IP and knowhow, to safeguarding British academic values. We will build and deploy a repertoire of effective interventions that reduce our vulnerability, including the proactive pursuit of opportunities to design out and/or mitigate harm.

d) **We treat our data as a national asset.** We keep pace with our most capable partners and adversaries in cyber defence (and offence). Our approach takes a systems view of our increasingly digital critical national infrastructure. We maximise the value to UK society from the UK's data assets; and powerfully apply British values, ethics and privacy standards in our approach.

e) **UK influence in S, T & Data at the heart of our international diplomacy**, shaping international norms, and securing an advantageous regulatory environment.

f) **S&T as a core element of improved HMG policy capability.** Policy is supported by excellent science assurance and underpinned by data, and policy makers have the skills and knowledge to exploit these effectively. We ensure we have a pipeline that will supply the S, T and digital skills we (HMG and NS specifically) need.