National Security Strategy Joint Committee

Call for Evidence on National Security Structures for Future Emergencies[1]

21st April 2021 (deadline 30th April)

Compiled on behalf of the UK Computing Research Committee, UKCRC.

UKCRC is an Expert Panel of 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 computing 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.

Prof. Chris Johnson
Pro Vice Chancellor (Engineering and Physical Sciences), Queen's University Belfast.
c.w.johnson@qub.ac.uk

Response:

[1] (Addressing) The link between the Strategic Framework and spending reviews.

> [1.1] The Integrated Review makes it clear that "redoubling our commitment to research and development, bolstering our global network of innovation partnerships and improving our national skills"[2] will lay the foundations for future prosperity and thereby help secure the nation.
>
> [1.2] However, the disruption in the immediate aftermath of Brexit has been compounded by the effects of the pandemic. Tight constraints have been imposed on spending through UKRI, at least in the short term. International links have been broken or suspended through the loss of funding to GCRF projects. Improvements in the national skill base – especially in critical areas connected to Computing Science have been challenged by the difficulties and learning deficits faced by many students as they enter Higher Education.
>
> [1.3] We are in strong support of the objectives espoused in the integrated review of Security, Defence, Development and Foreign Policy. We require a sustained and systematic approach to the concerns listed in [1.2] if UK S&T is

[1] https://committees.parliament.uk/call-for-evidence/361/national-security-machinery/

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

to achieve those objectives and lead our recovery from the pandemic. Spending reviews play an important role in provide the resources needed but they can only form part of a wider landscape of concerns when, for instance, much UK research in Computing Science is cross-subsidised by large numbers of overseas students; only a portion of whom continue into the UK workforce.

[2] How departments tackle cross-cutting challenges with clearer accountability for delivery; deeper integration across government, building on the Fusion Doctrine.

[2.1] Significant steps have been made to encourage this deeper integration across departments.

[2.2] In particular, there is good evidence of cooperation especially within the implementation of the Network and Information Systems Directive; intended in part to secure national critical infrastructures. Cabinet Office, BEIS and DCMS have worked with NCSC and the UK research community to extend best practice to the regulatory agencies ("Competent Authorities") and the, typically private, companies that operate our essential services[3]. This has begun the address the supply chain issues and concerns over digital sovereignty that are mentioned in the integrated review.

[2.3] The strong record of UK researchers within the development of critical infrastructures, including but not limited to 5G, has not driven the development of domestic industry capable of meeting our needs or yet of competing with overseas suppliers. The sometimes-contradictory messages about the policy behind, for instance digital sovereignty, can have devastating effects on UK researchers when different departments do not speak with one voice. For instance, the decision to limit involvement of particular overseas companies in UK infrastructures by one area of government can lead to the withdrawal of research funding from Early Career researchers previously encouraged by other areas. These negative effects have arisen in precisely those areas that are of greatest importance to our national defence and security.

[3] What "a comprehensive national resilience strategy" should entail.

[3.1] Given the diversification of technological excellence across the globe, which is partly a result of the success of UK Universities in educating large numbers of overseas students in STEM research, the UK will continue to rely on potential adversaries and competitors for core components of our computational and communications infrastructure.

[3.2] There is a delicate balance to be struck between 'technology nationalism' and 'digital sovereignty'. On the one hand, the UK benefits immensely from our diverse, international supply chain; providing access to leading technologies that support industry and enrich our daily lives. On the other hand, this creates almost unique levels of inter-dependency and vulnerability to disruptions in global supply chains either as a result of policy changes or other contingencies.

[3] See for example https://ritics.org

[3.3] We cannot, nor should we, try to make ourselves self-sufficient across the broad range of emerging technologies. Digital fragmentation and the diversification of technical engineering talent across the world makes it unlikely that we would ever be able to sustain leadership across anything but a small subset of infrastructures.

[3.4] We would, however, advocate a risk-based approach that identifies and safeguards the technical and engineering infrastructures upon which the UK depends. Where appropriate this may be done through global inter-dependencies across diversified supply chains. In other contexts, we should take the considered decision to work with like-minded nations to ensure we do not become dependent on any other single nation for core infrastructure technologies that might then be used as a strong external lever on UK foreign and domestic policy.

[3.5] Means of identifying and mitigating the risks from cross-border supply-chains are extremely primitive. As mentioned previously, the majority of UK infrastructure remains in private hands. There are few mechanisms by which companies can make informed procurement decisions that are aligned with national defence and security aspirations.

[3.6] In some cases, the industrial control systems and operational technologies (as opposed to information technologies) that underpin our infrastructures can take more than a decade to update. Even if the levers needed to influence change were developed, as alluded to in [3.2], the UK would remain vulnerable for a significant time into the future.

[3.7] The issues identified in [3.3] apply to the MoD as much as to UK infrastructure. Many of the PLCs, sensors and actuators that raise concerns within power distribution networks also provide the backbone on naval vessels.

[3.8] GCHQ and the NCSC have provided guidance, such as the Cyber Assessment Framework, but implementation has been slow and piecemeal. There is a need to develop a coherent view of where attention needs to be focussed to achieve minimum standards informed by changing risks.

[3.9] A comprehensive national resilience strategy would, therefore, identify those areas where the UK relies on cross-border supply chains ensuring that UKRI/InnovateUK are empowered to encourage support for domestic suppliers where possible.

[3.10] Where it is infeasible to develop domestic competitors in the small number of these core strategic technologies and where no other friendly sources can feasibly be secured then the intelligence and defence agencies should ensure that the operators of essential services have visibility of their potential vulnerabilities. Even where there are legacy systems, it is typically possible to introduce a degree of diversity in the underlying infrastructures that would provide resilience if any single supplier were to be compromised.

[3.11] These approaches increase the costs of infrastructure providers but only where diversity is not already a regulatory expectation; systemic approaches would therefore involve risk-informed decision making across Government departments work with regulators and industry leaders. We would seem to be a long way from a situation in which this model might work and there also remain questions about the appetite for such intervention – however, without greater coordination we are unlikely to meet the ambitions in the integrated review.

[4] What "the responsible use of new data platforms, digital tools and participative processes to support policy-making and improve inclusivity and transparency" should entail.

[4.1] In the past, there has been a lack of coherent leadership in "the responsible use of new data platforms, digital tools and participative processes to support policy-making and improve inclusivity and transparency".

[4.2] Many government departments lacked the technical resources to engage in a sustained dialogue over these issues. Partly in consequence, a series of proposals were put forward that could not be implemented across our distributed communications and data infrastructures, see[4] for a notoriously bad case study.

[4.3] More recently, we have seen a number of excellent initiatives, in particular from the Competition and Markets Authority and HM Treasury, that demonstrate the convergence of policy and technical insight[5]. For instance, the CMA have established coherent means to ensure 'influencers' [6] and on-line gambling companies [7] continue to comply with UK law. We also welcome their work on algorithms, competition and consumer harm which identifies a number of the domestic and foreign policy concerns relating to the use of AI[8].

[4.4] We would also encourage the Committee to consider and promote the recent work of HM Treasury on the UK approach to Cryptoassets and Stablecoins as a further strong example of government considering the implications of technical innovation on both domestic and foreign policy[9] with clear implications for national security and SOC.

[5] How 'red-teaming' might be introduced into national security decision-making; and

[4] https://www.gov.uk/government/consultations/child-safety-online-age-verification-for-pornography

[5] Our response to this and the next question is aligned with a separate UKCRC submission to the Foreign Affairs Committee Call for Evidence on "Tech and the Future of UK Foreign Policy".

[6] https://www.gov.uk/cma-cases/social-media-endorsements

[7] https://www.gov.uk/cma-cases/online-gambling

[8] https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers

[9] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf

the pros and cons of the proposed Performance & Planning Framework, Evaluation Taskforce and Outcome Delivery Plans.

[5.1] Red teaming has arguably been of greatest benefit when there are objective measures of performance and any exercises are exposed to robust, independent, verification/validation. As a particular example, the NATO Locked Shields exercise has had a transformative effect on French military preparedness in cyber. Notably poor performances against international competitors triggered investment that led to their success in subsequent competitions[10].

[5.2] Red teaming is least effective when it is used to demonstrate the sufficiency of existing policies and mechanisms. It can reinforce complacency and unwarranted optimism if there is insufficient independence and challenge to existing structures.

[5.3] The comments in [5.2] have to be balanced against the damage that can be done when the lessons learned from red teaming are viewed as "failures" rather than opportunities to improve and strengthen national resilience. Openness and transparency – especially in terms of subsequent interventions and within the obvious limits imposed by national security, increase confidence that these activities are more than "tick box" exercises.

[6] How well the National Security Council and/or Cabinet Office ensures that preparedness plans are resourced and exercised, and how their lessons are learned/implemented.

[6.1] The highest risks are very difficult to reduce to acceptable levels of probability or impact and the work required would be long and costly. As they are also relatively unlikely to materialise in the following five years, it is hard to justify very substantial investments on them in any individual spending round.

[6.2] However, the pandemic has had a significant effect on the public perception of these risks – and on our preparedness to mitigate those risks.

[6.3] We would urge the Cabinet Office and the NSC to consider the development of a Digital Resilience and Response Unit to safeguard and coordinate the response of private and public data and networks to future contingencies . Such an organisation should be aware of and sensitive to the privacy concerns that, for instance, frustrated the delivery of track and trace technologies and in using digital infrastructures to ensure compliance with isolation requirements after overseas travel.

[6.4] Some aspects of the proposal in [6.3] would also require close coordination with DCMS and the other agencies mentioned above, in connection to the delivery of the NIS directive but focussing more on the coordination of the OES under contingency rather than the mitigation of risk prior to any incident. However, the proposed DRRU would also provide an

[10] https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019/

ideal red team to help assess the effectiveness of NIS implementation; being largely independent of the existing implementation groups and other lead government Departments.

[7] How well funding/resources are linked to national security decisions.

[7.1] We strongly encourage investment in the R&D required to answer the challenges mentioned in [6.3]; recent experience has demonstrated the need for a “systems approach” that relies not only on technological, organisational and policy preparedness but also an understanding of the human factors issues that determine whether any intervention will be accepted and used by the public.

[8] The collection, use and analysis of data across national security relevant departments, and the mechanism for the NSC collecting evidence to aid its decision-making.

[8.1] UK research is world leading in the areas of data science and machine learning. However, only a very small proportion of our community has any awareness of the evidence and data used across national security relevant departments. Even less have any idea about the mechanism for the NSC collecting evidence to aid its decision-making.

[8.2] We would welcome opportunities to assist in the integrated approach being advocated and to help the UYK achieve greater levels of resilience to the threats that lie ahead.

[8.3] One aspect of this is the binary nature of the processes used to achieve relevant security clearances; the delays in completing DV do not fit well with a flexible and responsive approach to future challenges.

[8.4] Some thought might be given to maintaining a wider panel of researchers with appropriate clearances or to more flexible arrangements and with correspondingly more limited access privileges to ensure that the defence and security communities do have access to our leading researchers, which is arguably not the case at present.

[9]

a) How the NSC maintains its centrality in the policy-making process, sets ministerial direction and oversees implementation of national security decisions.

b) The appropriate role and remit of the National Security Adviser, including the NSA’s required interaction with the NSC, COBR and ministers.

c) The interaction of the NSC and COBR systems.

d) The role of key Government departments and agencies in national security policy making.

e) The coherence of the NSC committee structures, as reshaped in this Parliament and further revised to address Covid.

f) [12] How well the ‘Fusion Doctrine’ is embedded, learning the lessons from Covid.

[7.1] This is largely outside the scope of UKCRC, as a representative body for UK computing research. However, many of our members work for individual government departments often at ministerial direction but without any visibility of how their work aligns to the priorities established by NSC.

[7.2] Similarly, the lead UK funding agencies, UKRI, do not reference NSC priorities. This is not a criticism but a reflection of the manner in which UK R&D priorities are closely influenced by government departments and BEIS, in particular.

[7.3] The lack of visibility of NSC priorities makes it difficult for some of the World’s leading researchers in Computing Science to see how their work might contribute to the integrated and systemic approach to defence, national security and foreign policy envisaged in the recent integrated review.

[7.4] For instance, existing funding mechanisms rarely take an integrated view – for instance, encouraging technological innovation to support foreign policy, defence and national security. Calls for research only consider pairwise interactions at most.

[7.5] We stand willing to help find links between different areas of UK research needed to achieve the Prime Minister’s vision. However, this will require very different ways of doing business – breaking silos and reorienting engineers and scientists through cooperation between NSC, the lead government departments and UKRI.