The House of Lords Committee on Risk Assessment and Risk Planning[1]

8th January 2020

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

**Summary:**

**[S1] We believe that the UK is resilient to a large array of discrete 'extreme risk' events. However, we are unprepared for linked or systemic scenarios.**

**[S2] The UK is increasingly vulnerable through extended international supply chains, based on networked digital infrastructures, that represent a single point of failure for multiple industries.**

**[S3] The lack of coordination between government departments exacerbates barriers to integrated national risk mitigation.**

**[S4] It is hard for companies within an industry to share information with their competitors, it is hard for companies to ask suppliers about the resilience of their supply chain without violating IPR.**

**[S5] While recent events have demonstrated national resilience – for instance through the rise of homeworking, these changes have increased other vulnerabilities through our reliance on digital networked systems.**

**[S5] The UK Computing Research Community has a strong record in systemic approaches to risk management but there is a lack of uptake compared to our international competitors.**

**[S6] As a specific example, countries across Asia have been quick to exploit a number of advanced information management platforms to increase coordination between national regional and local responses (see for example the Taiwan T-road initiative and join.gov.tw).**

**[S6] We advocate a legal requirement on government to present to parliament a formal overview of national hazards and threatstogether with progress on associated mitigations at least every 4 years; mirroring international best practice.**

[1] https://committees.parliament.uk/call-for-evidence/339/risk-assessment-and-risk-planning/

1. What are the most significant extreme risks that the UK faces? Are these kinds of risks discrete, linked or systemic? What do you understand the term ‘extreme risk’ to mean?

**[1.1] The existing national risk assessments provide a clear taxonomy for discrete threats/hazards across a range of potential scenarios.**

**[1.2] However, we have particular concerns for linked and systemic risks that threaten critical infrastructures, which themselves promote national resilience and which are essential to our recovery from a broad range of possible scenarios.**

**[1.3] Digital network communications have proven to be essential in coordinating our response to recent events; systemic risks that threaten these infrastructures should be an important focus for this consultation.**

**[1.4] We understand the term ‘extreme risk’ to mean the possibility of very high levels of damage as a result of threats or hazards, whether economic or societal.**

**[1.5] Given existing levels of investment and planning, and the consequent effort afforded, extreme risks are unlikely to stem from discrete events but from systemic and linked failures.**

**[1.6] Systemic or linked failures can occur, for example from bugs in common software shared throughout the supply chain of many UK critical infrastructures or through coordinated attacks, whether cyber or physical. Insufficient analysis at regional levels can fail to identify linked risks, for example in the effect of extreme weather events on local power supplies.**

2. Are there types of risks to which the UK is particularly vulnerable or for which it is poorly prepared? What are the reasons for this?

**[2.1] Yes – there are short term concerns over our communications infrastructures and the services that they support. In spite of significant work by the National Cyber Security Centre and DCMS, the end users of network information systems often over-estimate the reliability and resilience of these systems.**

**[2.2] While other aspects of contingency planning exhibit significant ‘defence in depth’ many UK critical infrastructures rely entirely on digital network communications to coordinate their recovery from other extreme risk events.**

**[2.3] Particular concerns focus on the Control of Major Hazard (COMAH) sites, many of which rely on legacy infrastructure that remains vulnerable to cyber-attacks. The HSE has made important steps in training their inspectors to understand and identify these vulnerabilities for instance through the publication of their operational guidance. As mentioned in 2.2, one consequence of the pandemic has been to introduce network connectivity for some of these infrastructures to enable remote working; leading to a corresponding increase in the potential attack surface.**

**[2.4] In the longer term, we identify two particular concerns for national resilience from any dependence on technology that 1. is not producible/sustainable within the UK; and 2. is poorly understood by those who rely on it within the UK. In the former case, this increases our reliance on international supply chains that may themselves be compromised by an extreme risk event. In the latter case, this limits our ability to accurately assess the risk associated with any dependence on that technology.**

3. How could the Government's approach to risk assessment be strengthened to ensure that it is rigorous, wide-ranging and consistent? Your answer could refer to any aspect of the risk assessment process including, for example, its governance, the evidence base, or the degree to which it is open to scrutiny and the input of experts.

**[3.1] Many stakeholders, including asset owners as well as those involved in national initiatives to improve the resilience of critical infrastructures, are unaware of the processed used to develop and validate the national risk assessment– wider consultation would be beneficial, including (in this case) reaching out to appropriate experts in UK Universities, for example via the UKCRC, which is an expert panel of Computer Scientists in conjunction with the BCS.**

**[3.2] We would welcome similar clarity, within the constraints of national security, about the mitigations identified and actioned in response to the national risk assessment. Many of the potential stakeholders who might support the identification and validation of threats and hazards also have key insights into cost effective mitigations, which might otherwise be neglected.**

**[3.3] We would, in particular, stress the need for systemic approaches to risk that integrate technical innovation (for instance, as we have seen over the development of track and trace infrastructures) with societal measures (in terms of informing the public in a manner that encourages compliance with scientific advice).**

**[3.4] We recommend strengthening the resources available to HSE for the specialist team that inspect safety-critical electronic and software systems, in view of the increasing role of such systems, the serious threat presented by well-resourced cyber attackers, and the high salaries that expert cybersecurity specialists command in industry and commerce.**

**[3.5] We advocate the development of an evidence base that acknowledged the interactions between scientific, economic and political perspectives and which better prepares the different stakeholders to work together under the pressures of any future extreme risk events.**

4. Given the range of possible national risks, and the need to achieve a balance between efficiency and resilience, what level of assurance should the Government be seeking on the UK's resilience to hazards? What would effective national risk management achieve, and how could its success be measured?

**[4.1] Each sector needs to be assessed individually against a range of possible future scenarios; revisiting those identified in previous national risk assessments in the light of the COVID pandemic but also recent major security breaches.**

**[4.2] There are often trade-offs between the use of data to increase efficiency – by improving access and availability, for instance to patient records, and possible threats to national resilience. Any breach associated with critical data not only has confidentiality concerns but may also have implications for public safety if information is corrupted/edited.**

**[4.3] We would urge the Committee to think beyond national risk management to consider the integration of risk management by public and private bodies at local, regional and national level. National action can identify issues and priorities, but local are regional actions ensure that mitigations focussed and effective.**

**[4.4] It is also important to consider systemic interactions; specially to identify single points of failure or where inter-dependencies may undermine key infrastructures for recovery. Digital communications would be a top priority because of the increasing dependence on its services across society.**

5. How can the Government ensure that it identifies and considers as wide a range of risks as possible? What risks does the inclusion criteria for the National Security Risk Assessment exclude and what effect does this have on long-term resilience?
   (i) Should seek wider range of inputs from range of different organisations (e.g., review the risk registers of learning ftse companies, NHS and other public bodies to see what they are preparing for.
   (ii) Should run active gaming scenarios to envisage future attacks (e.g., run on banks, targeted attacks on NHS, etc.)

**[5.1] Our responses to [1.2], [1.5], [4.3] stress the need for multi-disciplinary perspectives on systemic interactions between threats and hazards – especially where single points of failure extend across multiple industries that are owned and operated by different stakeholders, for instance through common international supply chains.**

**[5.2] The National Security Risk Assessment does not specifically mention communication networks – this is an important omission, given the dependence of the UK on those infrastructures and the services they support. This may be subsumed under the first-mentioned Tier 1 risk, namely "Hostile attacks upon UK cyber space by other states and largescale cybercrime."). However, we would identify a far wider range of concerns including any interruption to these networks during the recovery from any other extreme risk event.**

6. How effectively do current ways of characterising risks (for example, the use of a five-point scoring system of a 'reasonable worst-case scenario') support evidence-based policy decisions? What other information would be useful?

**[6.1] The systemic approach advocated in this response relies upon the active involvement of a broad range of stakeholders.**

**[6.2] The different backgrounds of these different stakeholders means that there will be an increased potential for disagreement and uncertainty. Hence, considerable care should be taken to ensure the reliability, consistency and repeatability of any processes used to achieve consensus irrespective of the scoring system that is used.**

**[6.3] It is natural that there be a degree of uncertainty in any assessment of this kind, an evidence-based approach should ensure that this uncertainty is reflected in any aggregate risk assessments so that the public can have confidence in the proposed mitigations.**

**[6.4] A diverse range of public and private organisations have worked with industry regulators to implement the Network and Information Systems (NIS) Directive. Although the has not been universal success, this provides a template to improve national resilience against the wider array of threats and hazards that are identified in this consultation.**

7. How effectively do Departments mitigate risks? Does the Risk Assessment process and the Civil Contingencies Secretariat adequately support Government departments to address risks within their remits? Is further oversight or accountability required, and if so, what form should that take?

**[7.1] Prior to 2020, there was cooperation between many Government Departments in planning to mitigate future risks – for instance between BEIS and DfT. This has been more difficult since the pandemic as cooperation focuses on the immediate national needs response.**

**[7.2] Prior to 2020, there was cooperation on the implementation of mitigations. This often depended on personal working relationships, which were not always sustained after key figures retired or changed role within the Civil Service.**

**[7.3] Cooperation focussed on a narrow subset of the national risk assessment, especially Counter Terrorism and Cyber Security. It, typically, did not consider mitigations that might address systemic interactions. It was undermined by the limited scientific and engineering expertise available to many departments.**

**[7.4] We would welcome a wide-ranging review of the processes involved, including validation of the proposed mitigations. The Civil Contingencies Secretariat has the expertise needed to support these validation activities but only if individual departments have the resources and motivation to work together on the challenges that might arise under a range of extreme risk scenarios.**

8. How well are national contingency plans communicated to and understood by those at a local level, including emergency responders? What could be changed to increase the capability of local responders to effectively plan for and respond to emergencies?

**[8.1] The experience of the last twelve months has shown that there is a clear need to establish mechanisms for achieving consensus between national, regional and local agencies – especially in areas of devolved responsibility.**

**[8.2] The involvement of UK regions needs to be carefully considered, taking into account their individual contexts and priorities. The “four nations” calls that have been used extensively in recent months could be enhanced into a more systematic means of coordinating national, regional and local interventions.**

**[8.3] Emergency responders at a local level need to be provided with the rationale that supports national and regional policy. Scientific and engineering evidence needs to be communicated in a clear and concise manner so that enforcement and implementation can be explained to the public and so that local agencies do not misinterpret the intention behind policy decisions.**

**[8.3] The official means used to communicate with local responders have failed to keep pace with technical innovation. Even when emails are used rather than telephone calls, local responders typically hear about changes in national and regional policy from news outlets or from social media. This leaves them ill-prepared to tailor their operational response to changing national and regional requirements. It also provides almost no mechanisms for them to feedback local concerns to higher-level policy makers.**

9. What is the role of the individual in relation to national crises? Are there potential benefits in increasing public involvement and transparency in emergency planning? What limitations are there to this? What lessons have been learnt or should have been learnt about the approach taken to risk assessment and risk planning in this country from the COVID-19 pandemic?

**[9.1] Public awareness of extreme risks needs to be raised.**

**[9.2] There is considerable scope for the involvement of the third sector and other voluntary public groups in emergency planning.**

**[9.2] Greatest benefits may be obtained by engaging with the Professional bodies that have the technical, clinical, engineering, computational skills required to combat a range of extreme event scenarios.**

**[9.3] Private sector organisations also have a role in enabling their staff to volunteer and to participate in national initiatives to increase our ability to response to systemic threats and hazards.**

**[9.4] There is no strategy for identifying and training volunteers with the expertise needed to mitigate a broade range of systemic hazards and threats.**

**[9.5] More generally, the pandemic response has demonstrated that the public will follow detailed and specific guidance especially if they are convinced of the justification for that guidance.**

**[9.6] The public response depended upon trusted news outlets and their ability to reinforce positive advice as well as challenge the more negative influences of social media.**

10. What challenges are there in developing resilience capability? Your answer could refer to critical infrastructure, but also to systems and networks beyond those elements. What is the role of exercising to test risk preparedness, and are these methods utilised effectively in risk assessment and risk planning in this country?

**[10.1] There are organisational challenges in developing resilience capability. Within individual industries national resilience depends upon a degree of mutual support between natural competitors.**

**[10.2] The supply chain and data network interdependencies identified in previous paragraphs of this submission also implies a need to work across industry boundaries  to develop resilience capability.  Challenges include the need for customers to ask difficult questions about the degree of resilience offered by their suppliers, especially where there may be single points of failure or where supply chains extend across international borders.**

**[10.3] These challenges are exacerbated by technical complexity.    However, we encourage a comprehensive approach to building resilience, and also to making suitable arrangements for recovery in the aftermath of extreme hazards and threats.**

**[10.4] Exercising is essential. However, it is important to ensure that any exercises yield long-term benefits.  They must be resilient to changes in personnel and to organisational structures.  Their benefits must be proof against changes in particular underlying technical infrastructures.  The scenarios must remain relevant in spite of changes to the threat and hazard landscape facing the UK.**

**[10.5] The requirements outlined in [10.4] make it important to identify appropriate metrics against which to assess the generic utility of the exercises that help to validate national risk preparedness.    UKRI and UKCRC are well placed to deliver an evidence-based approach to the identification of these metrics.**

11. What can be learnt from local or corporate risk management processes, or those of other countries? Are there any specific examples of practices, processes or considerations which could improve the UK's national risk resilience? How could businesses and civil society more effectively support national resilience preparation?

**[11.1] Those mitigations that have been identified for UK national hazards and risks often lack the funding and support necessary to ensure implementation.**

**[11.2] This forms a strong contrast with corporate approaches that identify a risk owner and ensure at least annual reporting at board level.  It also forms a contrast with, for instance, the US where the Secretary of State for Defence**

**must formally account for residual risks to the Senate as part of the Defence strategy**[2]

**[11.3] UKCRC members have been engaged in the development and validation of a range of risk management processes in financial and safety-related industries. They have particular expertise in socio-technical risk management and, in particular, the assessment of risks to data processing infrastructures across distributed and dynamic networks.**

**[11.4] UKCRC members work across a broad range (all?) of UK industries working with UKRI and government departments including but not limited to BEIS, DCMS, DEFRA, DfT, FCO etc. However, these relationships with government tend to be "point to point" and focused on particular extreme scenarios rather than the integrated risk management favoured by our industrial and commercial work.**

**[11.5] Although the UK Computing research community has pioneered a wide range of risk management methods that can be used to identify and mitigate the threats and hazards to national critical infrastructures, these techniques have had relatively little impact on national strategy beyond the initial risk assessments. This forms a strong contrast with the United States where many Federal agencies have, for instance, adopted variants on the STAMP methodology developed out of MIT, which has been used widely by industry.**

12. What individual or economic behaviours would strengthen national resilience against hazards, and what mechanisms are open to the Government or society to incentivise these behaviours? How should we prioritise any changes required in approach, process or policy needed to improve risk mitigation and strengthen the UK's resilience to extreme risks and emergencies?

**[12.1] There are areas where wider national priorities, especially the UN SDGs and our commitment to carbon reduction, can align well with the individual and economic behaviours that increase resilience. For example, through the promotion of flexible models of home working.**

**[12.2] Behaviours that increase national resilience are already being adopted by employers as a result of the present crisis and as part of wider commitments to, for instance, sustainability.**

**[12.3] However, some of the individual and economic behaviours that increase our resilience to the present crisis introduce new vulnerabilities and dependencies. While the rise of home working has helped many businesses survive the pandemic, it has increased our dependency on digital infrastructures that are a key concern in this submission.**

**[12.4] The concerns identified in [12.1] - [12.3] argue for a landscape audit of national resilience against extreme hazards and threats to be presented to Parliament on a 4-yearly basis – mirroring the US National Defence Strategy.**

[2] https://www.law.cornell.edu/uscode/text/10/113