Published on

https://www.parliament.uk/business/committees/committees-a-z/joint-select/national-security-strategy/inquiries/parliament-2017/cyber-security-cni-17-19/publications/
so that could go on the UKCRC website now.

Written Evidence from UK Computing Research Committee, UKCRC (CNI0005)

Evidence on the Terms of Inquiry:

Cyber Security: Critical National Infrastructure

On behalf of the UK Computing Research Committee, UKCRC. Prepared by: Professor Chris Johnson,

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.

We very much welcome the launch of the inquiry as a development of the National Cyber Security Strategy and the previous 2017 report into UK National Security in a Digital World.

The following paragraphs provide specific responses to the terms of reference:

TOR 1:
The types and sources of cyber threats to Critical National Infrastructure (CNI) in the UK.

1. **Increasing Diversity of State Actors:** We have seen a proliferation and diversification in the types and sources of cyber threats to UK CNI. Members of UKCRC are responsible for hosting the Civil Nuclear forensic labs and note that the attacks on the Ukraine over the last two years have motivated a widespread investment in offensive techniques by other nation states, at least partially motivated to develop deterrent capability. These new state threats have strong implications for the UK with an increasing recognition that our CNIs depend on legacy systems and infrastructure. These will remain vulnerable within the short to medium term; we lack the financial and technical resources to replace systems that were never intended to be cyber-secure. The growing technical capacity to launch state sponsored attacks on CNI does not seem to have been matched by policy development – it is unclear under what circumstances such potential threats might be launched against the UK.

2. **Increasing Range of Criminal Threats:** UK CNIs are increasingly concerned about the implications of criminal threats – for instance, through ransomware illustrated by the effects of WannaCry on the NHS. It is likely that there will be 'leakage' from state sponsored techniques to criminals (the SMB vulnerability exploited by WannaCry was originally identified by the NSA). We also expect a continued use and increased sophistication in social forms of attack; such as SpearPhishing informed by the triangulation of personal data over social networks.

3. Existing UK CNI Vulnerabilities Motivate new Threats: Our vulnerabilities are not simply technical, stemming from legacy systems that were never intended to be secure, but also

relate to policy and process issues. UK CRC members have worked with the HSE who published the first guidance to

inspectors for the cyber security of industrial control systems in 2017. However, UK industry needs guidance and support, for example, on how to demonstrate that security patches do not compromise existing safety requirements for CNI software. It is likely that the nature of the threats will change as more actors understand the potential vulnerabilities in UK CNI.

4. **New UK CNI Vulnerabilities Motivate new Threats: The Industrial Internet of Things (IIoT) raises a host of well-documented concerns – exposing insecure legacy control networks (Modbus, Profibus) through TCP/IP gateways and routers making UK CNI vulnerable to the forms of attack witnessed in the Ukraine. NCSC should issue guidance on the protection of these bridging devices, just as they have for domestic smart meters.**
5. **New Technical Threats (eg Artificial Intelligence)** The threat landscape is also likely to change through technical innovation, for example, members of UK CRC are engaged in using Artificial Intelligence and Machine Learning techniques to attack software infrastructures. The AI algorithms use knowledge of previous vulnerabilities to automatically look for new weaknesses without human intervention using a technique called 'fuzzing'. These threat developments will create significant challenges for CNI operators, for the NCSC and individual government departments. There is a danger that we are protecting our systems against the previous generation of attack methods.

TOR 2:
The extent to which the Government's definition of 'critical national infrastructure' is still valid in an interconnected economy;

6. **Need to Support CNI Operators Outside the NIS Directive:** Members of UK CRC have assisted individual Government departments, including BEIS and DfT, to map vulnerabilities introduced through rapid change in the connected economy. This work supports the integration of the EC Network and Information Systems (NIS) directive into UK law. Existing UK NIS proposals are pragmatic and proportionate but they exclude many CNI operators (eg regional airports) that have a significant impact on communities. If their systems are compromised, these wider elements within the UK CNI can undermine core elements of UK infrastructures.
7. **Need to Help Operators Accurately Assess Resilience of Supply Chain Data/Processing Service Providers:** Many of the key software systems used in UK CNI have a checkered history having been sold between different companies in the last 5-10 years. As threats develop there is an urgent need to help operators make informed decisions about the procurement of more secure replacements – especially where they rely on out-sourcing. 'Software as a service' procurement models are very common and the resulting contracts will specify KPIs but prevent UK CNI operators from asking detailed technical questions about the underlying cyber security of their supply chain. A small number of UK data service providers support many different areas of CNI; this creates the potential for what the US DHS term a 'cyber storm' crossing CNI infrastructures. There are also concerns when these providers operate across national borders and where the mutual reporting arrangements that under the NIS may not be supported post-Brexit. There is a need to consider 'critical national infrastructure' within an internationally 'interconnected economy'.

TOR 3:
Learning points drawn from the 2011 Cyber Security Strategy and the fitness for purpose of the 2016 Cyber Security Strategy in relation to CNI;

8. There is broad support from across the UK CRC for these initiatives but also recognition of the continual need to revise and update these initiatives – see previous comments on threats and new recognition of continued vulnerabilities in UK CNI. We would also stress the need to

review the existing organizational roles and responsibilities (see later responses for comments on need to coordinate and clarify the public-private interface in CNI).

TOR 4:
The effectiveness of the strategic lead provided by the National Security Council, Government Departments and agencies, and the National Cyber Security Centre, and the coherence of cross-government activity;

9. **Need to Sustain Career Development for Cyber Expertise in UK Civil Service:** There are specific problems in the retention of key staff; as a result civil servants with no background in cyber security often lead major CNI projects. This creates concerns when they lack the technical background to make informed decisions; for example about regulatory guidance or measures to improve the cyber maturity of the UK CNI supply chain. The high rate of turnover means that the investment some of our best young civil servants make to understand the key issues in cyber security are often lost as they move to other roles or departments.
10. NCSC helps address obvious skill gaps but their resources are extremely limited. For example, there are 3 or 4 individuals in NCSC with any significant expertise in aviation. They participate in many national and international initiatives and at the same time act as technical from drones through to cyber threats to physical security at airports.
11. As we move towards the implementation of NIS, NCSC lacks the human resources required to fully support all government departments and regulatory organizations involved in CNI.

12. **Need to Review Links between GCHQ and NCSC:** Senior NCSC staff with an intelligence background find it hard to share appropriate information with external parties – including CNI operators. This leads to claims that “the flow of CNI information is one-way; from industry into the NCSC”. This is changing over time but old habits die hard and in the meantime there is an urgent need for technical guidance on appropriate measures to protect UK CNI.

TOR 5:
The effectiveness of the Government's relationships with, respectively, private-sector operators and regulators in protecting CNI from cyber attack;

13. **Need to Coordinate Efforts to Solve Problems Already Identified by Industry and Government in CNI:** Prof. Chris Johnson (drafting this UK CRC response) helps chair the UK NCSC Steering Group for the Community of Interest in Industrial Control Systems – this is the main forum for private- sector operators, regulators and government agencies to address key technical challenges in the protection of CNI. There has been very mixed success in sustaining this forum; we have developed a “problem book” of concerns identified by industry and validated by the NCSC. However, we lack the resources to directly commission work to address these problems and all members (government, industry, regulators, academia) are fully pressed to meet the day-to-day demands within their own organizations. Many of these concerns, such as the tension between safety and security regulations, remain unchanged/unaddressed in 2-3 years while the threats continue to rise.

TOR 6:
The balance of responsibilities between the Government and private-sector operators in protecting CNI against cyber attack;

14. **Need to Clarify Role of NCSC:** The changing remit of the CPNI and NCSC has contributed to significant confusion across UK CNI about the balance of responsibilities. Our members undertaking work for individual government departments have found CNI operators whose CISO has never heard of the NCSC. There are strong regional differences – with the probability of direct contact between CNI operators and NCSC rapidly declining outside the Home Counties.

15. **Urgent Need for NCSC to Provide Clear Guidance on Industrial Cybersecurity:** Previous CPNI guidance on the cyber security of Industrial Control Systems was extremely useful to UK CNI operators. The NCSC no longer supports these documents. We are in an interregnum during which promised NCSC materials are yet to be published. This is understandable but unfortunate.
16. **Need for UK CNI CERT:** We regret the demise of UK CERT (Computer Emergency Response Team). This became part of the NCSC but it has not been resourced. In consequence, even those CNI operators with direct contact to NCSC have no idea of the level of technical or other resources that might be available to detect and recover from an Operational Technology (OT) incident involving UK infrastructure.

TOR 7:
The consistency of approach in the UK to legislation, regulation and standards governing each CNI sector and cyber security;

17. **Lack of Consistency and Regulatory Uncertainty Remains a Problem** The NIS implementation has led to significant dialogue across CNI industry sectors. However, there are differences between government departments and beyond that to the Competent Authorities that will have a profound impact on the future integrity of UK infrastructures. Although some regulators are training staff to fill aspects of the CA role, eg HSE, others lag far behind. Significant questions remain about their competence. It seems clear that some regulators and government departments have potentially unrealistic assumptions about the level of support that will be available from the NCSC.
18. **Lack of Standards and UK Guidance on Acceptable Means of Compliance:** There are few applicable standards in the cyber security of CNI. Those that are available (such as IEC 62443) are not widely used. Regulators have a limited ability to interpret their requirements within the UK context. This exacerbates the problems created in the interregnum between CPNI and NCSC guidance, especially within industrial control. The HSE guidance to inspectors is very useful in this respect (http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf) and they plan 10 case studies to validate the concepts and deliver version 2 over the next 12-18 months. However, the HSE have deliberately omitted any requirements on incident recovery or the interaction with the NIS. This creates further potential for inconsistency.
19. **Areas of Improvement:** Some government agencies have yet to consider cyber security as an issue. For example, the Air Accident Investigation Branch may at some point be required to consider cyber security concerns as a cause in a formal accident investigation. There seems to be little progress in this area.

TOR 8:
The availability of skills and expertise to the relevant Government Departments and agencies, to regulators and to private-sector operators of CNI;

20. This has been covered in previous responses.

TOR 9:
The extent to which the UK's approach to the cyber security of CNI draws on or represents international best practice.

21. **Safeguard Funding for Internationally Leading CNI Research:** The UK Research Institutes (RI) funded jointly by the Research Councils (EPSRC) and NCSC have raised our international profile in this area. However, funding for original work within the RI in Industrial Control Systems is not being. CNI operators need fundamental help to determine how to patch/update CNI software without compromising safety; how to integrate safety and security risk assessments; how to support the human factors of CNI regulation in private/public partnerships; how to increase confidence across extended CNI supply chains; how to support incident reporting and forensic analysis in industrial control systems. The lack of research funding on these topics creates major concerns for the long-term health of UK CNI. In contrast, each of these topics is covered by a dedicated research program in the United States, Israel, Singapore etc.

22. **Develop Strategic International Research Collaborations Post-Brexit:** The potential loss of access to EC results and funding is a significant issue. This occurs at a time when our international competitors have formed strategic research alliances – the Dutch government have a preferential research exchange and joint funding program on the cyber security of Industrial Control Systems with the US Department of Homeland Security, Israeli research teams are working on joint CNI projects with Singapore. We would urge the committee to consider these issues and also the degree to which UK Universities and CNI operators are encouraged to work together.