Written evidence submitted by Dr Mils Hills, Associate Professor of Risk, Resilience and Corporate Security, Northampton Business School

1. Although currently working in an academic environment, I draw on a prior career in defence research for the Ministry of Defence (beginning in 1998); heading a national capability in an area of relevance to the scope of this investigation; secondment to the Cabinet Office's Civil Contingencies Secretariat (CCS) at the time of its inception and evolution, and ongoing research for government and others.

2. I offer some select thoughts which are intended to be practical contributions to the work of the Committee. I would be happy to expand and elaborate on any sections, should it help the work of the Committee.

What are the credible threats to the UK and its interests?

3. Firstly, in relation to the range of 'credible threats to the UK and its interests' – I would recommend that several of these eventualities could be caused by natural or military risks. For example, the effects (or *consequences*) of a CBRN attack would have some overlap with the consequences of naturally occurring phenomena (e.g. outbreak of a human or livestock pandemic against which there is little or no remedy or counter-measure). Naturally, the specific political and military response to a deliberate release of agents or substances would be different – but the demands on resources (technical, personnel) would be similar.

4. In the early days of the Civil Contingencies Secretariat – the ethos was that the focus in planning and preparation for disruptive challenges ought to be 'on the consequences not the causes'. Whilst causes could be endlessly listed (e.g. the number of ways in which damage might be done to an important element of the Critical National Infrastructure), the generic consequences would be similar if not identical: albeit with ancillary responses varying – law enforcement, security and intelligence upon evidence of malign intent, other parties if not. The need to have the ability to recover or source alternative capacity (and to understand constraints on this) would be common to all scenarios.

5. Given, for example, the challenges of reaching swift and definitive attribution of cause – especially in, but not restricted to, cyberspace – recovery is likely to be achieved before ascertaining beyond reasonable doubt the cause of a crisis (e.g. livestock disease as a result of natural or unnatural processes).

6. Whilst some of these comments may not seem to be directly related to the SDSR – of course it is the military who are often turned to to deliver capability (or logistical and other solutions) even for non-directly defence contingencies.

What is the Government's ability to evaluate credible threats to the UK and its interests?

What is the Government's ability to 'think the unthinkable' and how flexible are the UK's thought process and planning process to meet the wide range of credible potential dangers?

7. With the development of 'horizon scanning' activities and roles across government, there are a good deal more 'sensors' available to detect obvious (and attempt to make sense of less definite) threats and risks to UK plc. The value of pushing out the envelope of sense-making to achieve early-warning has been recognised for some time as critical to statecraft and security:

> You are extremely well advised to listen closely to all of the signals, however faint, of impending bad news. They are your only lines of defence. You need to constantly scan your Kingdom for signals of bad things that are about to happen, whether they are of your doing or someone else's. This is the only chance you have to gain advantage - Nicolo Machiavelli, *The Prince* 1515.

8. The way in which events which are not orchestrated by an adversary can combine – perhaps in 'a perfect storm' – as well as those which are planned and executed by subtle, well-funded and ruthless enemies mean that relentless searching for assurance that there is not a drift towards what some would describe as a state of 'criticality' is vital.

9. However, this is not an easy task. Whilst some parts of government (and those organisations and friends that work with it) find such work natural and fundamental, others do not. The culture of the civil service as well as of political leadership needs to adapt at speed to free-up the ability of its sensors and sense-makers to report potential risks and threats, even though these might well be unwelcome. Having then done so, coherent and cohesive efforts must be made to act on information which demands action – rather than hoping that the situation never occurs or, worse, that we will 'muddle through'.

10. The challenge is to ensure that a questioning culture in relation to preparedness and possibility becomes second nature to all in and around government. There are strong competencies in red-teaming, scenario-based testing and other activities in defence, security and other areas and Departments. Continuity, preparedness, policy and other plans (as well as vital systems and consequence management) must be tested against robust and realistic scenarios – frequently, at low cost and with lessons identified being turned into lessons learned. Leaders, advisers, policy-makers and others must be agile, adaptive, creative and innovative in both looking at the sources of challenge and the means of engaging and resolving it.

11. Equally, cross-Departmental (and other) resources need to be able to be brought together at speed and high-impact effects brought to bear on emerging crises and potential crises. Early intervention is the goal.

12. Government has previously demonstrated its ability to 'think the unthinkable' – and much of the work of the now departed Scenario Development Team (SDT) of the Civil Contingencies Secretariat (CCS), in which I played a modest role, embodied that. Likewise, having been the first 'security anthropologist' to work in the defence research laboratory of the MoD – and having found nothing but support and endorsement of unconventional (if practical) thinking in a career in the civil service from 1998-2005 – we should praise the openmindedness of our system in contrast to that of other states!

13. I found that there was a community of colleagues across government and beyond who challenged the status quo for the benefit of government and citizens – and I know that this continues to be the case. It is of – I believe – of national strategic interest to ensure that robust challenge occurs at all levels of policy and strategy development and is folded into operational and strategic decision-making, during crisis and before. This will not be comfortable for all.

Does the Government have the ability for generic capability and capacity building in the event of an unforeseen threat?

14. In my experience, Government does have the ability for some generic capability and capacity-building appropriate to understanding and engaging unforeseen threats – but often freedom of manoeuvre for decision-makers (at strategic and other levels) is diminished because operational and other individuals await total certainty that a risk or threat is real before acting or escalating. Further, although there has been a good deal of rhetoric about being able to 'ramp up' both known and other resources and expertise from the public and private sector – in reality this is not quite how events pan out.

15. Whilst the growth of Reserve formations in the Armed forces and the National Crime Agency (NCA) are to be welcomed - in terms of enabling those who wish to serve the country but who are not able (or best suited) to be full-time, say, soldiers or police officers – much more could be done to enable the state to access their knowledge and ideas. There is a great deal of untapped potential (of all ages and across technical and other disciplines) which could be embraced and leveraged – were a few of the hurdles that currently exist be dismantled, as has admirably been the case in some parts of the defence community.

5 October 2015