Written evidence submitted by Haydn Belfield and Tildy Stokes.

1. How vulnerable are our space assets to deliberate attack, both physical and otherwise, and what steps can be taken to improve their resilience (with regard both to defence capabilities and other critical national infrastructure)?

Our work at the Centre for the Study of Existential Risk and the Centre for Long-Term Resilience focuses on extreme risks. These are high impact threats which have a global reach, and result in a loss of 10% or more of the population (for example, a nuclear war or a pandemic). . It is therefore fundamentally important that we mitigate and prepare for extreme risks. Our space assets are critical national infrastructure: we rely on them for communication, transport and logistics, and early warning systems. Damage to space assets could severely impact our resilience, making us more vulnerable to extreme risks. This inquiry submission focusses on building resilience to extreme risks into the UK's Space agenda.

a) The 'three lines of defence' risk management model:

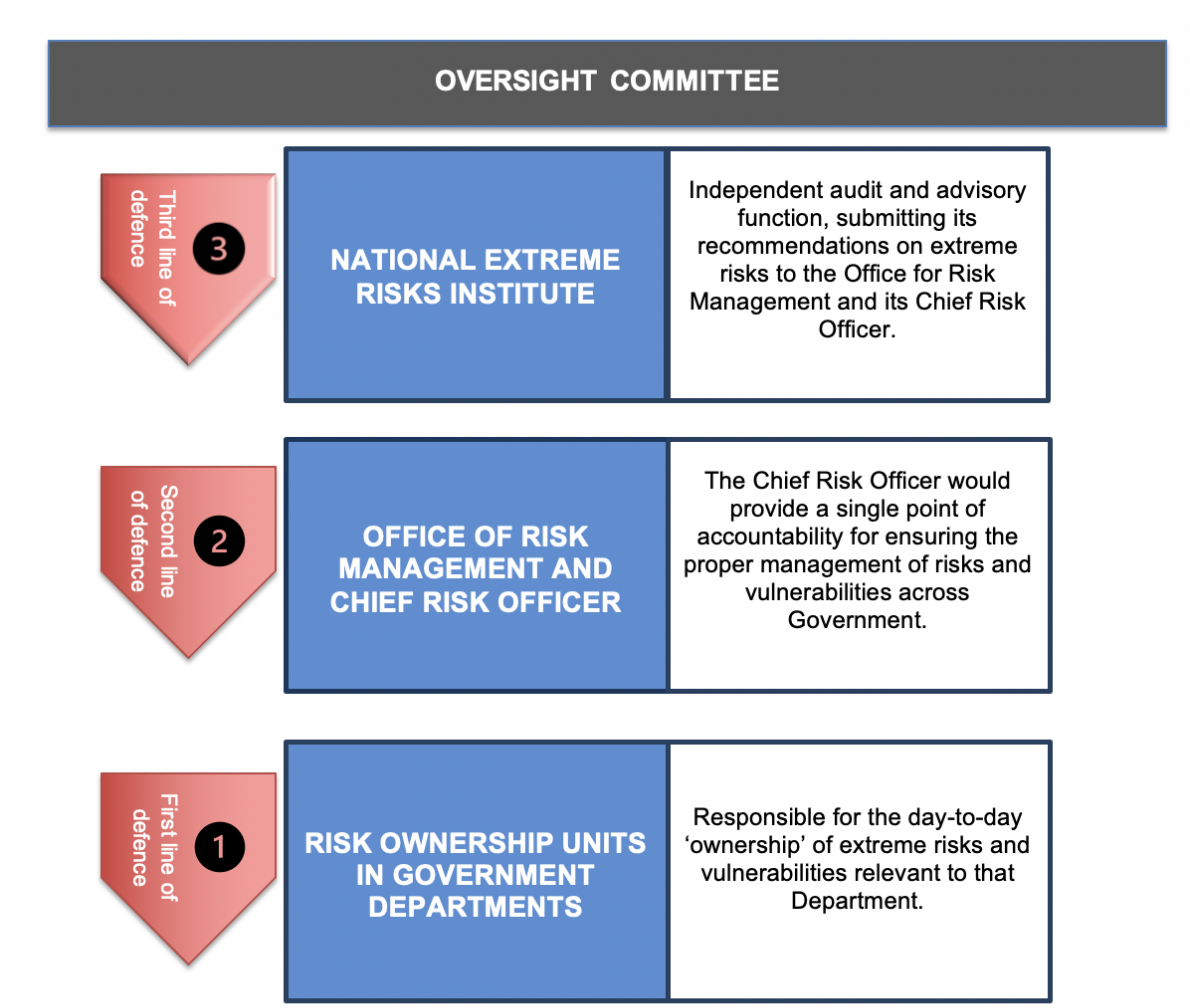
The Centre for Long-Term Resilience is encouraging the Government to adopt a 'three lines of defence' model for risk management, as mentioned in the Government's 2020 Orange Book. This would improve extreme risk assessment and ownership across Government. We suggest that a 'three lines of defence' model be adopted for our space assets, with risk ownership units in Departments supported by an Office of Risk Management, audited by a National Extreme Risks Institute.

UK space policy, and associated international engagement, should be informed by a three lines of defence approach to risk management. Below is a description and diagram of the model. For more details, see our recent report: Future Proof .

As we have seen from Covid-19, there are clear lessons to be learned about how to better assess and manage risks. A clearly defined single point of accountability for risks in Government will help transform the UK's resilience to future extreme risks.

Improving the Government's approach to risk management will need strong leadership from the centre of Government, along with iterative work between policy officials, politicians and risk experts from a range of sectors.

We suggest the structure pictured below, based on the 'Three Lines of Defence' model which is standard practice across industry.



b) Set up throughout-lifetime stress-testing of computer and AI system safety and security.

For the UK's national security, it is important to stress-test computer systems thoroughly to test its resilience and identify flaws. This is particularly important within space policy, considering the critical nature of computer systems in this area. To do this well, there must be an incentive structure to point out problems, rather than underplay them.

Stress-testing allows systems to be assessed for flaws and vulnerabilities before they can be exploited by adversaries, or before accidents involving new systems occur. This is particularly important given the Government's decision to incorporate AI into its defence capabilities.

The Government announced in November 2020 that it would create a new AI agency and re-orient its defence capability towards emerging threats.[1] It is vitally important that any new AI-related bodies prioritise the secure and safe development of AI, and in particular that they set up throughout-lifetime stress-testing of computer and AI system safety and security.

We recommend that the computer and AI systems used in space assets be stress-tested during development, testing, training, early deployment, at regular intervals, and before retirement of relevant systems. The Government should also have dedicated 'white hats' stress test their systems by attempting to compromise their software and hardware vulnerabilities, through social engineering and by designing adversarial environments.

c) Normalise red-teaming in Government, including creating a dedicated red team to conduct frequent scenario exercises.

It is vital to scan for and discover vulnerabilities to UK space infrastructure, and other critical national infrastructure (CNI), thus avoiding and anticipating as many disasters as possible. A team recruited with the skills to do this well can reduce groupthink and question key assumptions.

We recommend establishing a red team of experts tasked with running scenario exercises to focus on major attacks on, and accidents involving, UK critical infrastructure - including of space assets - and then implementing the recommendations from their findings into the Space agenda.

d) Fund a comprehensive evaluation of the actions required to increase the resilience of the electrical grid

The electrical grid is at risk from an array of both natural and manmade threats, any one of which could cause widespread disruption, including to the UK's critical infrastructure. If the grid is damaged or disabled, communication networks will collapse, oil and gas distribution will halt, water purification and distribution will cease functioning, and effective governance will face severe strains. In the worst-case scenario, nuclear reactors could also melt down. The grid's ability to withstand the impact of these threats is a major concern for national security.

A key natural threat is solar storms, which could also impact or disable space assets. Space assets can also be crucial early warning systems for monitoring solar activity.

[1] This was announced as part of the UK's November 2020 announcement that it would spend £16.5 billion on defence spending: https://www.bbc.co.uk/news/uk-54988870

There is an opportunity to make Britain a global leader in electrical grid resilience and preparedness for the next century of risks. This effort should produce specific policies, procedures, and technological solutions, together with implementation timelines and an estimate of required resources.

It should include action plans in the following areas:

- **Improving the UK's ability to identify threats and vulnerabilities:** Produce standards and guidelines for threat identification and emergency response planning and preparation, which are accepted and implemented by the energy sector.
- **Increasing the ability to protect against threats and vulnerabilities:** Establish a nationwide network of resiliency test platforms that are long-duration, blackout-survivable microgrids. These should be located in facilities controlled by the Government, in stable areas that are free from flooding, severe weather and other high impact disasters.
- **Improving recovery capacity and time:** Design ultra-secure, low-power, self-healing wireless networks capable of bypassing compromised network components, while maintaining essential connectivity to critical grid assets. This should be designed to preserve fail safe operations that engage within minutes of a cyber attack.

2. Where can the UK most effectively develop and deploy its own sovereign defence capabilities, with particular regard to:

- Space Situational Awareness
- PNT (Position, Navigation, Timing) services, in the context of the UK's exit from the EU's Galileo and EGNOS programmes
- Intelligence, Surveillance and Reconnaissance
- Communications

a) Avoid complex signal processing in defence satellites

Doing any serious signal processing onboard defence satellites (especially advanced signal processing, such as machine vision) should be avoided for three reasons:

- From an engineering perspective we should avoid complex computation with high electricity needs in orbit.
- From a risk perspective, there is more reason to doubt the validity of the signal coming down.

- These systems have a highly vulnerable attack surface.

If machine learning processing is to be conducted, it should not be done in-time, in-orbit. However, our more general recommendation is caution on incorporating AI systems into nuclear command, control, communications, computers, intelligence, surveillance and reconnaissance (NC4ISR). As evidenced by the sobering history of nuclear near misses, introducing AI systems (or automation) into NC4ISR could increase the risk of an accidental launch, without proportional benefits - due to system error and/or automation bias.

We recommend that the Ministry of Defence investigates the process that the UK would need to undertake to make a credible commitment that it will not incorporate AI systems into NC4ISR.

4. What should be the priorities of the new Space Command, and how will its structures facilitate integration across all military domains and co-operation with commercial space operations?

a) Invest further in improving long-term forecasting and planning for possible threats to CNI

Forecasting[2] can help predict the probabilities of future disasters or attacks, thus helping allocate resources towards risks that are the most serious and the most likely. Thus far, forecasting has mainly focused on generating near-term predictions, but there is ample scope for this to change.

We recommend extensive research into improving forecasting techniques, for example through the use of quantified falsifiable predictions, and full inference cycle tournaments, as proposed by Professor Philip Tetlock.[3]

The Government should build on work done in the US by the Intelligence Advanced Research Projects Activity's[4] intelligence community prediction market and from the Center for Security and Emerging Technologies new policy forecasting project, Foretell.[5]

13th July 2021

---

[2] https://blog.longnow.org/02015/11/30/philip-tetlock-seminar-media/
[3] https://www.sas.upenn.edu/tetlock/
[4] https://www.iarpa.gov/index.php/about-iarpa; https://cset.georgetown.edu/research/future-indices/
[5] https://www.iarpa.gov/index.php/about-iarpa; https://cset.georgetown.edu/research/future-indices/