Evidence to ESNZ Parliamentary Committee meeting of 3 June 2026

Introduction

This paper provides answers to questions submitted to Chris Few by the Energy Security and Net Zero Committee in preparation for its committee meeting of 3 June.

Questions and Answers

Question 1: What are the cybersecurity risks in moving to an energy system based on more diffuse renewable energy and what steps does the Government and its agencies need to take to mitigate them?

Answer: Increased use of renewable energy tends to require more dynamic management of both reactive power and load balancing. Both aspects create new opportunities for cyber-attackers and hence increase cyber risks.

Reactive power is generated by capacitance and inductance within the high voltage components of an electricity grid. It generates heat in the transmission lines and hence consumes transmission capacity, but it does not create useable power. High levels of reactive power can trip transmission line over-voltage protection relays, potentially leading to cascade failures and blackouts. Reactive power appears to have been a factor in the Iberian power incident in 2025 and many other power failures.

The relevance of reactive power to renewable energy and cybersecurity is that the reactive power output of many sources of renewable energy can be remotely configured. Wind turbines and solar panels connect to the electricity grid via inverters that convert low voltage direct current to high voltage alternating current. These can be configured to inject reactive power; i.e. current that is 90 degrees out of phase with voltage. This can be useful to cancel out existing reactive power that is out of phase by 90 degrees in the opposite direction, but it also creates a new attack vector. The increasing use of remotely controllable inverters creates a possible new attack vector of manipulating their reactive power output. This could be used to trip transmission line over-voltage protection relays.

Load balancing: An electricity grid needs to balance power generation with load in real time. For several reasons, this function becomes more complicated as an energy system transitions to diffuse renewable energy sources. With more energy sources, the system operator has to manage more operators. Changes of power output are more frequent, some of which are due to unpredicted weather conditions. Unlike thermal power stations, renewable energy sources do not provide inertia. This means that a difference between generation and load creates a larger shift in grid voltage frequency from the intended 50Hz.

More dynamic load balancing also creates new opportunities for cyber-attackers. A loss of visibility of the state of the electricity grid (e.g. transmission line voltage levels) will more quickly lead to grid instability and possibly automated load shedding. The reduction in inertia means that a cyber-attacker has to disrupt less generation to trip the Low Frequency Demand Disconnect (LFDD) scheme. As the grid frequency drops below 48.8Hz, the LFDD will disconnect consumers to regain balance between load and generation.

What does this mean for government and its agencies? It means that using generic cyber security frameworks such as the NCSC Cyber Assessment Framework or the NIST Cyber Security Framework are not sufficient for managing the cyber security of electricity grids. There are cyber-attack vectors that are specific to electricity grids and their potential to cause impact to electricity consumers can only be understood by analysis of the grid as a whole. In my view, government needs a method for assessing the cyber security of the electricity grid that systematically seeks out possible loss scenarios through disruption of the control and protection systems and then assesses how feasible it is for a cyber-attacker to cause them. This may lead to new regulatory cybersecurity requirements designed to meet specific attack scenarios.

Question 2: What lessons should the UK learn from the recent cyberattack on Poland's energy grid?

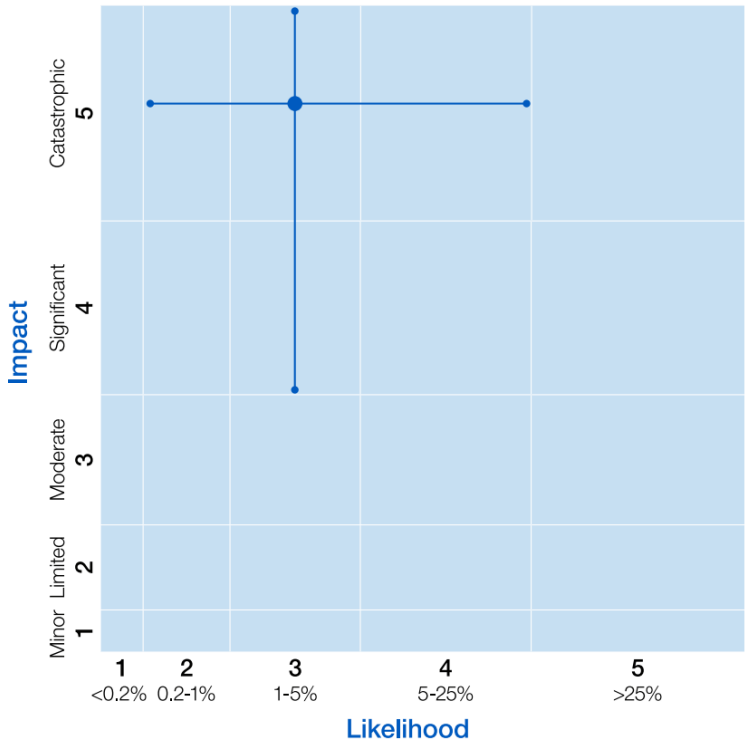
Answer: It is a useful reminder that advanced cyber-attackers may target energy systems. It raises the question of whether any of the UK OESs should be explicitly required to defend against them.

Question 3: Is there sufficient Government and regulatory oversight of the cyber protection of electricity transmission networks?

Answer: In my view the Government and regulatory oversight of the cyber protection of energy networks, including the electricity transmission networks, would be more effective if the national cyber risk appetite was more clearly defined.

As background, Figure 1 is taken from the most recent version of the National Risk Register. It shows the risk of failure of the 'National Electricity Transmission System' (NETS) from malicious and non-malicious scenarios. The impact is from a single failure.

Figure 1 - Risk of failure of the national electricity transmission system.



Economic impact Scale

Scale	Economic cost
5	Tens of billions £
4	Billions of £
3	Hundreds of millions of £
2	Tens of millions of £
1	Millions of £

Likelihood for malicious scenarios is assessed over 2 years and non-malicious over 5 years.

Source: National Risk Register 2025, https://assets.publishing.service.gov.uk/media/67b5f85732b2aab18314bbe4/National_Risk_Register_2025.pdf

A key point in Figure 1 is the size of the likelihood error bar. The bar extends from 0.2% to 25%, over a hundred-fold increase across the range. Even this may understate the uncertainty in risk because cyber-attacks are not independent events. One advanced attack may be followed by many more.

Similar diagrams to Figure 1 can be drawn for just the cyber risks for the whole UK electricity grid, for the gas equivalent and for their combination. The NIS regulations devolve responsibility for cyber risk management to the Operators of Essential Services (OESs) but, to my knowledge, how much risk they are entitled to accept on behalf of UK citizens is not defined.

We are living through an unusually turbulent period both in terms of global politics and in the application of AI to cybersecurity. The past reliability of our energy networks may not be a good guide to its future. At the same time, the UK is investing heavily to enable the energy transition. After 6 years working in cyber risk teams at Ofgem and National Grid it is not clear to me what types of cyber-attacker HMG now expects OESs to protect the energy networks from. Should the OESs aim to defend against nation state level attacks, compromised supply chains, subverted insiders with privileged access to energy systems, or combinations of all of these? If so, what does that mean for the cybersecurity requirements for the electricity transmission network, including future parts being designed today and intended for use for many years ahead?

My suggestion is that DESNZ should take an initial risk averse position and clearly state a security objective to prevent any cyber-attack on energy systems from causing economic impact to the UK of more than a given amount, e.g. £1billion. The more detail there is in the definitions of the attackers' presumed capabilities, the more clearly the security objectives can be stated.

I understand that the potential cost of this security will be of concern to the Secretary of State, but this can largely be managed through the RIIO framework. By setting a high-level energy network security objective, the OESs should propose the best options through their RIIO submission, and the key risk management decisions will be made by Ofgem and DESNZ through the determinations process. From what I have seen this should provide better direction and oversight than current practices allow.

A good security solution will not necessarily require higher levels of security for each component of our energy networks. To cause the level of impact shown in Figure 1 (tens of billions of £s), a cyber-attacker must defeat multiple layers of defence in both the cyber and physical systems. The most plausible high impact scenarios require a series of attacker actions to manipulate physical systems. New forms of monitoring cyber and physical events could be introduced with the goal of recognising and blocking sequences of malicious commands before high impact occurs.

Question 4: Are cyber resilience measures sufficiently aligned across the different CNI sectors?

Answer: I don't have much sight of alignment across other CNI sectors. However, what might also be of interest is analysis of the interdependencies between them. For example, there are interdependencies between the gas and electricity networks, and it is possible for a cyber-attack on one to affect the other.

Question 5: Do you consider DESNZ and Ofgem's proposals for reform of cyber regulation in downstream gas and electricity adequate?

Answer: I see the consultation as a welcome initiative, and I have responded to it. However, I see the bulk of the cyber risks to the energy sector coming from the transmission networks for gas and electricity. If the cyber-attacker cannot reach the transmission network control and protection systems operated by NESO, National Grid and National Gas, it becomes much harder to cause a national blackout.

Question 6: What cybersecurity measures should be included in the Government's forthcoming Energy Resilience Strategy?

I believe there needs to be a rigorous method for assessing how sophisticated a cyber-attacker needs to be to disrupt critical cyber-physical systems such as the GB electricity transmission network. Without this, there will always be uncertainty in whether security objectives are being achieved. An outline proposal for this was published in an academic work based on work that I led at Ofgem.[1] The concept was updated whilst at National Grid and submitted as part of the ET RIIO-T3 proposal. A more refined version is available on request.

Question 7 - How should any additional cybersecurity measures introduced by the Energy Resilience Strategy be funded?

I believe it would be very beneficial to the energy sector if there was a freely available open standard for rigorously assessing the cyber security of critical cyber-physical systems. As a public good, its development should be publicly funded by either DESNZ or DSIT. For OESs subject to the RIIO framework, the costs of cybersecurity should be recovered through the framework. For Ofgem licensees outside of RIIO, the costs should be borne by the licensees.

Question 8 - Are threat reporting pathways clear for those in the energy industry and is there a need for the Government to provide more visible, formalised support in reporting suspicious activity?

Answer: Sorry, I don't have any detailed knowledge of this issue.

Chris Few

22 May 2026

Ex-employee of National Grid and Ofgem

Chris Few | LinkedIn

[1] PeerJ HVA_CPS proposal: a process for hazardous vulnerability analysis in distributed cyber-physical systems