

# Securing Low-Carbon AI







# Securing Low-Carbon AI

**Author:** Steve Rumbold

## Summary

AI demand and net-zero ambitions combine to fuel increased interest in new nuclear and other forms of low-carbon electricity generation. Big tech companies are investing in small modular reactors (SMRs) and even exploring recommissioning old nuclear power stations with high generating capacity. Large new nuclear power stations continue to be constructed, and global investment in renewables and interconnectors is increasing.

At the same time, energy networks are being targeted by state actors as part of hybrid warfare and sub-threshold<sup>1</sup> disruption campaigns. Data centers supporting AI are normally highly resilient, designed to operate for extended periods without power from the grid. However, targeted physical and cyber-physical attacks on energy infrastructure could challenge this resilience. Assessment of the most serious national-level risks offers interesting context but is limited as a reference point for private sector operators. Systemic risks are not fully understood. Innovation that produces efficiencies may also offer attractive new targets for adversaries. Resilience regulation has evolved to acknowledge not just the physical aspects of cybersecurity but also direct sabotage, requiring operators to better understand physical risks to their assets and develop mitigation plans. Whatever national or regional rules apply, private sector organizations need a coherent approach.

How should we think about high-impact, low-probability risks from targeted threats affecting critical infrastructure services? How can we better understand systemic risk across cyber and physical domains? How do we convert postulated strategic risk into prioritized actions?

Interpretation and compliance with regulations like the EU's Network and Information Systems Directive (NIS2) and Critical Entities Resilience Directive (due to come into effect for designated critical entities, including the energy and digital infrastructure sectors, in July 2026) is a start, but operators need to plan beyond mere compliance. Because impacts go beyond individual enterprises, public and private sectors must enhance their coordination to coherently knit together national-level strategic risks and operational-level risks. Over the last 20 years, security cooperation between asset operators and national technical authorities and regulators has evolved—this must now include co-operation between subject matter experts and the military, as the UK's recent Strategic Defence Review (SDR) highlights. We can use high-level risk registers as a starting point, then drill down to plausible scenarios applicable to operators, to flush out actionable decisions that address risk. We can use modern data science to elucidate complex systemic risks at scale. At an operational level, we can use cyber risk quantification and physical risk quantification to measure risk, including financial impacts, with more confidence, enabling better mitigation options.

<sup>1</sup> Below the threshold for an active state of war to exist, also known as "gray zone" activities.



# Data Centers Are Power Hungry, with a Low-Carbon Appetite

## Concentrated Power Needs

The UN's International Energy Agency (IEA) stated in its 2024 World Energy Outlook<sup>2</sup> that “a substantial increase in electricity consumption from data centers appears inevitable.” In the UK, around 500 data centers currently consume 2.5%<sup>3</sup> of all electricity in the UK. In Ireland (about 120 data centers), the figure is 21%<sup>4</sup>. Those figures are projected to reach 6% and 30% respectively by 2030. In the U.S., the figures are estimated to grow from 4% in 2024 to between 4.6% and 9.1%.<sup>5</sup> High loads are required for both cooling and computation (generative AI searches use 10 times more power than normal Google searches). Despite gains in efficiency over the last decade, these more active servers demand substantial cooling. And, of course, more people and technologies are using AI, so we need more data center capacity. The IEA reported the average increase in installed servers was 4% per year from 2010 to 2020, but since 2020 this could be up to around 15% per year. However, from a security and resilience perspective, the concentration of data centers within national electricity grids poses a more relevant challenge. U.S. data centers are highly concentrated regionally (e.g., in Virginia); the same is true in the UK for (Greater London) and in Ireland (Dublin). This concentration of electricity use is summarized by the IEA:

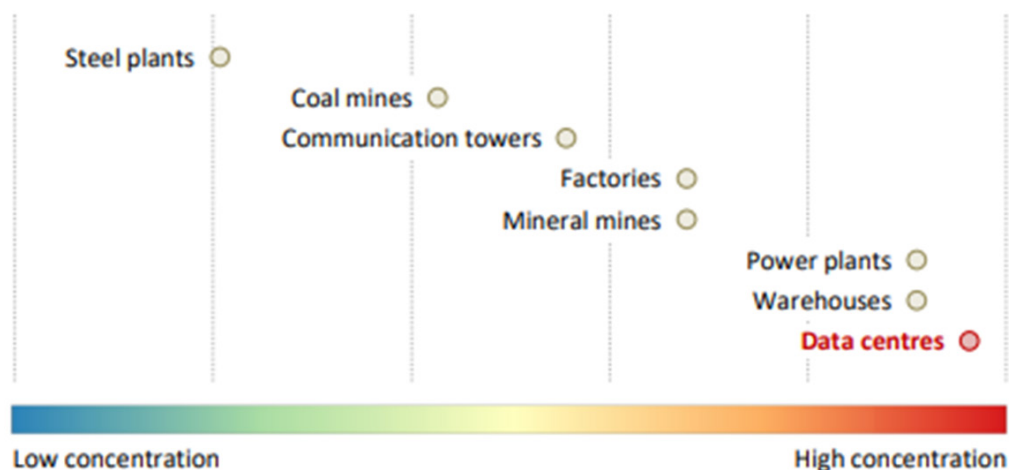


Figure 1: Concentration of Power-Hungry Sectors (Source: IEA World Energy Outlook 2024)

Geographical concentration and high electricity demand may exacerbate business continuity risks in the face of intelligent threat actors.

## Low-Carbon Needs

Data centers are under pressure to reduce carbon footprints by using low-carbon sources. Every big tech company has made a commitment to net zero ambitions. In the UK, the generation mix will change by 2030, with offshore wind and other renewables dominating. Battery storage offers a means to store energy for peak demand and a response mechanism for sudden frequency drops. Nuclear continues to provide low-carbon “firm” load to the grid, with new nuclear projects backfilling nuclear plants that are nearing end of life (e.g., Hinkley Point C and Sizewell C). Globally, there is increasing interest in SMRs to provide reliable low-carbon generation for data center hubs. Nuclear is a good option for data centers because it supplies reliable baseload and is highly resilient and secure by design, due to stringent nuclear safety and security requirements. Amazon Web Services chief executive Matt Garman recently cited nuclear power as a “great solution” to data centers’ needs and “an excellent source of zero-carbon, 24/7 power.”<sup>6</sup> This seems like a sensible partnership for data centers, which are also designed to be extremely resilient (driven by high availability requirements). However, nuclear power stations take time to build, partly because of those same stringent safety and security requirements.

<sup>2</sup> <https://www.iea.org/reports/world-energy-outlook-2024>

<sup>3</sup> [Electricity System Operator Data Centre Report 2022](#)

<sup>4</sup> [Data Centres Metered Electricity Consumption 2023—Central Statistics Office](#)

<sup>5</sup> [EPRI “Powering Intelligence” 2024 white paper](#)

<sup>6</sup> <https://www.bbc.co.uk/news/articles/cewd5014wpno>

## Interconnections

Data and electricity interconnectors can increase overall resilience and help keep up with demand. For offshore generation, offshore hybrid assets (OHAs) can provide more efficient connections from multiple sources. However, the benefit of connecting energy networks is balanced by the potential vulnerabilities of single-node targets for adversaries.

## National-Level Risks—UK Example

The UK government publishes a National Risk Register (NRR), which is a public-facing version of a non-public National Security Risk Assessment. Like all risk registers, especially ones that translate to a 5x5 matrix, it needs to be understood in context. As a strategic overview with very broad scope, it is not a detailed decision support tool, and—unlike its classified cousin, which is continuously updated—it has only been published publicly twice: once in 2023 and again in January 2025.<sup>7</sup> And out of the 89 risks it describes, only a very few moved at all from 2023 to 2025. But it's still good to know what types of risk government worries about, so if something catches your eye as a risk practitioner, that may be a starting point for scenario planning. Figure 2 below shows a selection of big-ticket items that should at least give pause for thought:

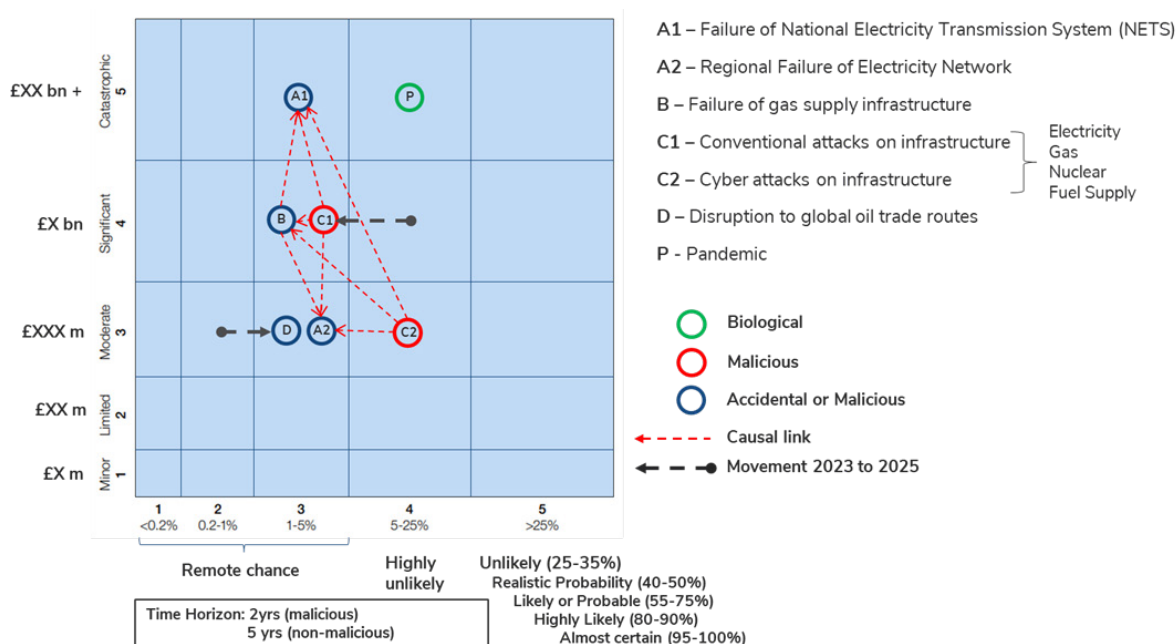


Figure 2: A Selection of Risks from the UK's 2025 National Risk Register

### (P) Pandemic

A well-established national risk well before the global COVID-19 outbreak (since at least 2011). It appears here as a comparator, sitting in the “catastrophic” range.

### (A1) Failure of National Electricity Transmission System (NETS):

Another catastrophic-level risk, even with an assumption of black-start recovery within seven days, the impact is in the tens of billions of GBP. There is up to a 5% chance of it occurring (in the NRR this is an “any cause” risk, so it includes faults and hazards as well as malicious initiating events). Interconnectors and Battery Energy Storage Systems (BESS) play an increasingly important role in maintaining the balance between supply-and-demand and frequency response. A sudden drop in frequency caused by the loss of an interconnector on October 8, 2024, was controlled using immediate battery energy, and on January 8, 2025, the supply/demand reserve margin was maintained by ensuring that an interconnector was restored quickly to full capacity. A data center well provisioned with fuel for its generators might continue to operate, but for its output to be useful, AI users would have to be similarly resilient.

<sup>7</sup> Previously a National Risk Assessment was produced annually but not made public.

## (A2) Regional Failure of Electricity Network

Although placed in the same likelihood band as A1, this is a lower, “moderate” impact (hundreds of millions in financial terms), given this applies regionally rather than nationally. However, a regional loss could affect densely populated areas or areas with a high concentration of data centers. At a lower level, even a local failure can result in major disruption, depending on the consumer’s risk tolerance to high-impact, low-probability events and their impact on budget and business operations. For example, data centers connected to the North Hyde electricity substation in London, which became suddenly unavailable in March 2025 due to a fire, stayed online. The resilience calculus differed from that of Heathrow Airport, which decided that the low likelihood of the multiple transformer failures, high cost of redundant connections, and overriding customer safety imperative meant a relatively high level of potential business interruption was a risk worth taking.

## (B) Failure of Gas Supply Infrastructure

Gas turbine power stations still contribute a relatively high percentage of power to electricity supply in the UK, also important for black-start scenarios due to their ability to self-start from battery and diesel generators. About a third of the UK’s gas supply comes from Norway via an undersea pipeline. Norway also supplies the EU with about a third of its gas supply, either via pipeline or liquefied natural gas. Like A1 and A2, this is an “any cause” scenario but could include conventional or cyber sabotage as an initiating cause.

## (C1) Conventional Attacks on Infrastructure

We know that attacking critical infrastructure, especially energy networks, using physical means (e.g., missiles or sabotage) is a common feature of conventional warfighting operations in open-conflict scenarios. It has also featured in terrorist planning and is a firm characteristic of hybrid and ‘gray-zone’ warfare. Notwithstanding ongoing questions over attribution or deliberate targeting, we know subsea energy and data infrastructure is vulnerable to kinetic operations falling under the threshold for an act of war.

## (C2) Cyberattacks on Infrastructure

Perhaps even a darker shade of gray in terms of attribution are cyberattacks on critical infrastructure, with the potential to lead to extensive systemic impacts. At one level, these occur daily (probing for vulnerabilities). It is also highly likely that sophisticated threat actors could already be pre-positioned on networks to prepare the ground for attack execution. In times of open conflict, cyberattack may either go hand in hand with or give way to conventional attacks.

## (D) Disruption to Global Oil Trade Routes

Closely associated with geopolitical forces, disruption to the availability of oil has major knock-on effects from both macroeconomic and operational perspectives. Approximately 33% of global liquid oil imports ship via the Strait of Hormuz,<sup>8</sup> the same region targeted by Houthi maritime attacks in recent years. The price of oil inevitably affects investment decisions and financial stability generally, but its availability can also affect resilience directly because emergency generators rely on fuel and oil supply.

<sup>8</sup> <https://www.iea.org/commentaries/the-world-cant-afford-to-relax-about-oil-security>



# Systemic Risk and Sabotage

While there is a danger of assigning too much precision to strategic risks, there is also peril in not being precise enough about operational risks that can contribute to systemic failure. Low-carbon energy sources and increased interconnection are valuable ways of meeting AI power needs with net-zero ambitions. However, these approaches may inadvertently create vulnerabilities and offer attractive opportunities for adversaries who may be willing to use physical and cyber means to disrupt essential services. The interconnected nature of these risks is recognized by governments, exemplified by resilience-focused legislation. The private sector's control of most aspects of critical national infrastructure in the face of state-sponsored sabotage techniques means that private-public collaboration efforts must operate on all levels, from the strategic to the tactical. Security challenges are summarized below:

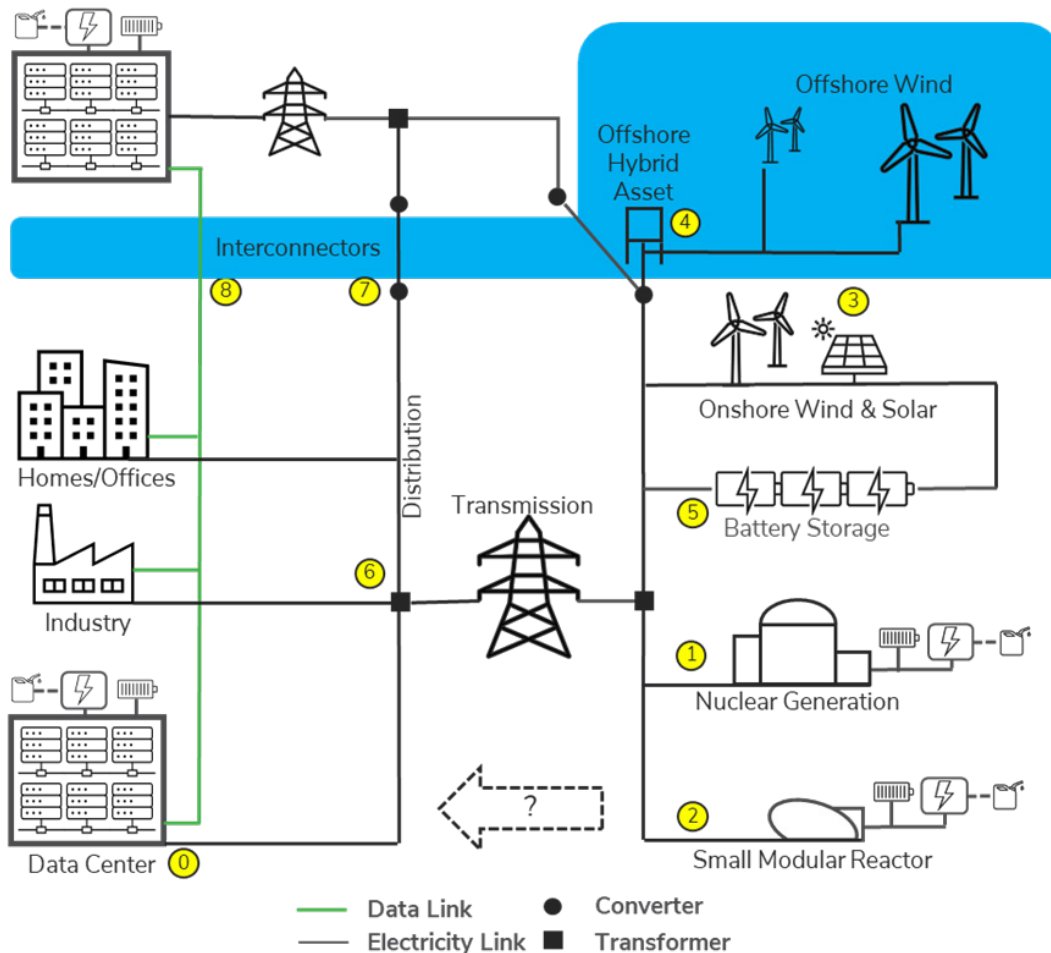


Figure 3: Simplified Schematic of Users and Typical Low-Carbon Generation Components



**0 — Data Centers:** Data centers are generally both highly secure and highly resilient by design. A core design principle is that grid power should not be relied upon; therefore in theory AI applications can continue to be powered continuously if an uninterruptible power supply is in place and there is fuel and oil for the generators. And even then, multiple data connections mean that critical applications don't rely on a single data center. This generally makes for a low return on risk investment for adversaries for a single act of physical sabotage.



**1 — Large New Nuclear or Recommissioned Nuclear:** From a security and resilience perspective, civil nuclear power is very mature. State-agreed design basis threat (DBT) assessments express government risk appetite and drive physical protective security measures. Security planning and operations are well resourced, normally including on-site armed response capabilities. Security and safety work hand in hand, and both are highly regulated. However, recommissioned nuclear power stations like Three Mile Island may have legacy issues where protective security addressing modern threats must be layered onto older infrastructure.



**2 — Small Modular Reactors:** SMRs are advanced nuclear reactors that have a power-generating capacity of up to 300 megawatts electric (MW[e]) per unit, about one-third of traditional nuclear power reactors.<sup>9</sup> SMRs co-located within large data center complexes are being considered for future on-site, reliable generation capability. Like their larger cousins, SMRs are also subject to national nuclear security regulations, which set a very high bar. SMR engineering advances in passive safety could reduce the potential for unacceptable radiological consequences to occur, no matter what the initiating event (i.e., fault/hazard or malicious action). The size and other design aspects of SMRs (for example, if they are underground or even underwater, with limited access) may also require fewer on-site security resources, easing cost burden. However, if the adversary aim is to curtail electricity generation, rather than cause a nuclear safety issue, SMRs may offer different opportunities for sabotage. The fear and anxiety in the general population associated with any attack on a civil nuclear site, and the potential curtailing of SMR programs, could be just as damaging as actual loss of generation.



**3 — Renewables (Wind and Solar):** The wide area characteristic and multiplicity of individual units may seem to spread the risk of sabotage. However, many renewable units are centrally controlled by operational technology, which is vulnerable to sabotage, especially if access control to physical components is poor. Another issue is supply chain vulnerabilities. Some components of turbines are only produced by a handful of suppliers. Photovoltaic solar panels rely on inverters, the loss or malfunction of which can result in sudden loss of supply. In May 2025, Chinese-made “kill switches” were found in U.S. solar farms, prompting immediate government response. This was not long after a massive countrywide electricity outage in Spain, likely caused by a sudden loss of solar-generated power.



**4 — Offshore Hybrid Assets (OHAs):** Efficiencies can be derived from connecting multiple offshore assets to one node (an OHA), effectively creating a network that can also act as an interconnector. However, mastering complexity and cost by creating nodes can also concentrate risk. Again, this may be controllable when faults and hazards are assessed as part of safety and reliability design, but targeted kinetic or cyberattack may result in different and unexpected outcomes.



**5 — Battery Storage:** As mentioned above, these assets are increasingly important for grid frequency stability, as fewer generation assets with rotational parts (and therefore inertia, which buys time to bring on alternative energy supply) are available. On the downside, new BESS are being built quickly and are arguably more vulnerable to sabotage than big traditional power stations.



**6 — Transmission and Distribution:** The fire at the North Hyde substation in March 2025 proved two things. First, critical national infrastructure hubs (in this case, Heathrow Airport) could be vulnerable to rare but essentially single-point failures of this scale. Second, data centers connected to the same hub managed to operate as if nothing had happened, due to their built-in power resilience. In May 2025 fires at electricity substations in Nice and Cannes, France, were understood to be started deliberately by single-issue groups, causing significant disruption. Arson is known to be a favored tactic for hybrid warfare operators, and electricity substations are an obvious target.



**7 — Electricity Interconnectors:** A more integrated energy system and less reliance on Russian gas in Europe mean that the number of electricity interconnectors is increasing, and these interconnectors are required for data center operations and planning. They also represent targets for both maritime and land-based sabotage (all interconnectors require a converter station at each end, also controlling flow via operational technology). Redundancy and separation help, but some countries rely more on imported electricity than others, and some geographies have less concentrated undersea cables than others.







**8 — Data Interconnectors:** Like their electricity cousins, data interconnectors are increasingly at risk from sabotage when run along the seabed. Separation and redundancy help, of course (they break all the time due to the harsh sea environment and genuine accidents), but this works better as an engineering risk response than as a security strategy.

<sup>9</sup> <https://www.iaea.org>. In the UK, SMRs and advanced modular reactors are both described as “advanced nuclear technologies.” Micro modular reactors are also under development

# Government Responses







**Defense and National Security:** In the maritime environment, there is a clear need for state intervention to protect critical infrastructure. For example, NATO's Baltic Sentry operation was in direct response to multiple instances of subsea infrastructure damage, likely part of state-sponsored sub-threshold disruption campaigns. NATO doctrine highlights the need for increased cooperation between infrastructure operators and the military. The UK's June 2025 Strategic Defence Review (SDR) calls this need out and signposts the need for further work in this area. This will require a new mindset across governments, militaries, private sector operators and regulators.

## UK Strategic Defence Review 2025: Recommendation 27

-  Much greater focus is needed on ensuring the UK's critical national infrastructure (CNI) is protected from attack **below and above the threshold of war**. Defence should more actively support the Cabinet Office in its work to set and enforce robust standards of protection and resilience for infrastructure, defining and prioritising the CNI on which Defence and wider Government relies in the first instance. A more comprehensive approach should include:
-  Strengthening Government powers to protect CNI where necessary, completing the process of **updating existing legislation or bringing forward new legislation by the end of this Parliament (2029)**.
  -  Exploring options for a 'new deal' for the **protection of CNI in partnership with private-sector and allied operators**. As part of this, the MOD should develop options for the protection of CNI in the event of crisis or conflict, including a new Reserve Force, with plans presented to the Secretary of State by December 2026. 

Accompanying the SDR, the UK's National Security Strategy 2025 also highlights a connection between hostile state activities and critical national infrastructure:

## UK National Security Strategy 2025

-  **Threats to the homeland from state actors are increasing.** The UK is directly threatened by hostile activities including assassination, intimidation, espionage, **sabotage, cyber attacks** and other forms of democratic interference... 
- 
-  ...critical national infrastructure – including **undersea cables, energy pipelines**, transportation and logistics hubs – will continue to be a target. It may become more difficult to identify hostile state activity as they make use of terrorist and criminal groups as their proxies. Our reliance on **data centres** and other forms of digital infrastructure will also increase vulnerabilities to cyber attack... 
- 
-  plans for Home Defence will focus on the **protection of critical national infrastructure and countering sabotage during a crisis**... 

**Regulation:** In the U.S., the Federal Energy Regulation Commission has ordered a refinement of the Critical Infrastructure Protection standard for physical security of the bulk power system, due to evolution of threat. In the EU the overall regulatory approach is chiefly described in the Critical Entities Resilience Directive (CER), which adopts an "any cause" approach but specifically calls out sabotage and hybrid warfare as threats, acknowledging that physical threats require risk assessment and mitigation alongside approaches for resilience against cyberattack, like NIS2 and the Digital Operational Resilience Act. Since 2018 the UK has had its own version of NIS to improve resilience for essential services. In 2023, regulators for the downstream gas and electricity sector added additional requirements for "Protecting Against Non-Cyber Risks" to the existing Cyber Assessment Framework. The UK's Cybersecurity Resilience Bill, due to be enacted in 2025, will expand the scope of the NIS, and it is likely that a UK form of the CER will follow. Essentially, energy infrastructure is raising its security game to have a more similar approach to that in place across most civil nuclear security regimes, even if "appropriate and proportionate" security design is different due to non-radioactive outcomes. But the need to assess risk and then produce a plan and maintain it is common to all regulatory approaches.



# Conclusions

**Threat Assessment:** Resilience plans need to be based on a clear understanding of both threat and risk. They are not the same thing. A design basis threat, reflective of government agencies' advice as well as overall government risk appetite, is used by some sectors to determine what a security design should reasonably protect against, in terms of adversary intent, capability, and tactics, techniques and procedures. This approach would be beneficial for all critical sectors, if appropriate expertise is available.

**Risk Assessment (Plausibility):** At a strategic level, when making the decision to put effort into resilience planning, likelihood matters less than whether a scenario is applicable and plausible. If the reasonable worst-case impact is high enough to your organization (or country), you need to have a resilience plan.

**Risk Assessment (Likelihood for Security Design):** The likelihood of accidents and hazards can be calculated using techniques such as probabilistic safety assessment (essentially an actuarial approach). Cyber risk quantification techniques exist for attacks targeting digital assets. Assessing the likelihood of sabotage by intelligent threat actors targeting tangible assets directly, potentially more than one of them simultaneously, is more problematic. To date this has required an essentially deterministic approach, in other words once a design basis threat is agreed, protective security planning is based a probability factor of the threat materializing of 1.0 (100%). This approach is necessary because an assumed capability side of the threat equation can be countered by engineered resistance and planned responses, and because the intent side is volatile and binary (i.e. an attack will occur or it won't, so it's sensible to assume it will). Investment decisions in hardened infrastructure and protective security also need a stable design to enable cost-effective construction and operation.

**Risk Assessment (Impact and Vulnerability):** This is where operators of energy infrastructure can make the most valuable headway toward resilience. Impacts can be postulated using digital models and a deep well of engineering knowledge that can simulate systemic risk. The same is true for vulnerabilities. An engineer is less likely to be concerned about whether it's arson or not, just that there is the potential for fire. Equally, in the cyber domain, a technical vulnerability can be discovered and addressed, whatever the likelihood that any threat actor may choose to exploit it (someone probably will, after all).

**Risk Assessment (Continuous):** Research conducted in 2012 by the U.S. Nuclear Regulatory Commission into SMR security highlights how a "Probabilistic Risk Assessment" approach<sup>10</sup> could dovetail with the traditionally deterministic method to inform SMR security design. Since 2012, protective security has become a component of a wider resilience approach, in which the ability to be more agile in the face of a developing threat landscape has become increasingly important. Advances in open-source intelligence, enhanced by AI, create the possibility of understanding and measuring a changing threat landscape, which can complement the initial and then periodic assessment which influences physical security design. Identifying and measuring potential vulnerabilities and impacts means that this can be translated into a risk assessment. This is especially relevant to private sector operators who will need to provide early warning of specific threats to infrastructure which may require state-level assistance for enhanced deterrence, detection, and response. The combination of continuous threat and risk assessment with cyber risk quantification for operational technology can result in a form of physical risk quantification.

**Right-Sized Security Effects:** The most effective security and resilience plans will use threat and risk assessments to be clear about the security effects they wish to achieve and will acknowledge interdependencies, trade-offs, and opportunities across safety, security, and operational efficiency, and across the physical and cyber domains.

**Resilience Plans:** The need to understand both cyber and physical threats in resilience plans is by now very clear. Many operators of critical infrastructure will now also need to plan for how they will interact with public sector civilian and even military response assets, potentially in a multinational environment. They will also have to be clear about how coordinated efforts between different operators and potentially across sectors can address systemic risks.

<sup>10</sup> [NRC Position Paper on Physical Security for Small Modular Reactors](#)



---

#### About Kroll

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at [Kroll.com](https://kroll.com).

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.