KCS Group International

We look at the world differently...

UK & Europe's Critical Infrastructure

January 2026

For the past 18-24 months, KCS Group International has been warning – repeatedly and with increasing urgency - that Europe's critical infrastructure is dangerously exposed. What was once a forecast is now an undeniable reality. Russia's hybrid operations have not only intensified but quadrupled in 2025, exploiting every weakness in a system that has been allowed to decay. Yet, governments remain paralysed, unable or unwilling to respond with the speed and cohesion the situation demands. This paralysis is not confined to the UK; it is a Europe-wide failure.

"We are a soft target in this shadow war."

This is a sober assessment of a continent whose defences have been eroded by decades of complacency. Accumulated structural weaknesses have created vulnerabilities which now align perfectly with Russia's doctrine of ambiguity and deniability. Much of Europe's critical infrastructure still relies on legacy technology and obsolete software, never designed to withstand sustained, state-sponsored sabotage.

Compounding this vulnerability is the ownership model itself. Over 80% of our critical infrastructure is privately owned, designed to create short-term returns, not resilience. Accountability is fragmented across regulators, operators and governments, creating a patchwork of responsibility where strategic risk is routinely externalised - until the moment it is exploited. A stark example of this is our undersea cable exposure. Europe's lifelines for data, communications, and finance, lie largely unprotected on the ocean floor – accessible to any actor with the capacity and intent to interfere. They are ideal targets: high-impact, low-visibility and easily deniable. A single disruption can ripple across economies, governments and societies.

Russia has spent years – arguably decades - mapping these vulnerabilities with forensic precision. What we are witnessing now is not opportunism but the execution of a long-prepared strategy. The intent is clear: to inflict damage, sow uncertainty and weaken Europe's ability to respond collectively.

Conclusion

The question is no longer *if* the next attack will occur, but *how severe it will be* - and whether our governments will finally recognise that critical infrastructure protection, attribution and response are collective security obligations, not optional national add-ons or private-sector afterthoughts. Fragmentation is a gift to hostile actors. Unity is the only credible defence.

Private enterprise must rethink priorities: short-term returns cannot come at the expense of national security. The cost of inaction is rising sharply and it is measured in strategic vulnerability, not quarterly earnings.

The UK and Europe are now in a shadow war it did not choose but one it must now learn to fight.

KCS Group International – Strategic Intelligence & Corporate Security

KCS Group International is a leading provider of security and intelligence services, operating in some of the world's most difficult environments on complex cases of fraud, theft, corruption or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients identify and deal with any risks, weaknesses and threats which could impact on their business, financially or reputationally.

Our key areas of expertise include: Corporate Intelligence Services – New market or sector entry research – Know your customer screening.

In addition, we offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits – providing unparalleled analysis, contingency planning and implementation.

To find out more or to arrange a meeting to discuss your business needs, please email the team at info@kcsgroup.com or call (00 44) 20 7245 1191 – www.kcsgroup.com