FINANCIAL TIMES – 18 SETTEMBRE 2025

Europe needs to wake up to its internet network vulnerability

di Richard Milne

Trains stranded in remote areas for hours, mobile networks down, schools and shops plunged into darkness — the electricity blackout that hit large parts of Spain and Portugal earlier this year had plenty of dystopian echoes.

Similar, more localised blackouts at Heathrow airport and the strategic Swedish island of Gotland have also grabbed the headlines in an era of growing anxiety over the prospect of sabotage, particularly from the likes of Russia.

But experts say there is a less appreciated but just as serious risk in the vulnerability of European internet networks. Any problems with them would affect companies and their manufacturing sites, public services and consumers in ways that many may never have considered.

“Everything is so interconnected in IT infrastructure, more than most people believe, maybe more than in electricity,” says Patrik Fältström, chief security officer at Netnod, the Swedish group owned by a non-profit foundation that runs crucial online infrastructure around the world, including internet exchanges.

Netnod is sounding the alarm, believing companies and policymakers alike need to think more seriously or risk whole swaths of the economy being easily knocked out by simple cyber attacks.

It is clear many companies are woefully unprepared. “IT was something for the entire IT department only. I didn’t realise how wrong that was until suddenly we lost everything in a cyber attack. We ran our IT pretty efficiently, which was fine — until something went wrong,” says the former chief executive of a European company hit by an attack in recent years. The company itself was largely paralysed for days, and it took months to get fully back to normal.

Sabotage events recently such as the cutting of data cables (and plenty else) in the Baltic Sea and damage to mobile masts across Sweden have highlighted the issue, with many politicians across Europe worrying that the region is moving into a state somewhere between war and peace.

To improve resilience for societies and business, it cannot be just left to each organisation to act in isolation, often procuring internet and IT services according to cost, not availability under adverse scenarios. Governments and companies need to think more about how they keep their essential services operating, whether through attack or natural disaster.

Netnod, which runs the largest internet exchange in the Nordics, has plenty of experience of helping with infrastructure in countries involved in conflicts.

Fältström says one of the biggest problems is that internet users — be they private sector or government — do not tend to have a plan if they lose their main service provider. So they often have no backup if that provider runs into trouble. If that happens, the issue then becomes that the users find they have dependencies in ways that many organisations do not understand — that the operation of machinery in a plant or delivery of food to the elderly is intimately linked to the internet.

And there are more systemic vulnerabilities. In Sweden, most of the critical internet infrastructure is centralised in Stockholm, with nodes leading away from it into different parts of the country. “The network in Sweden is far too dependent on Stockholm — and it’s the same in many countries,” says Fältström.

That presents an attractive target for a malign actor, aware that they can create maximum impact with relatively limited action. What is perhaps scariest is how many of society’s crucial functions — such as water, television or electricity grids themselves — are themselves dependent on this vulnerable internet infrastructure.

Russia’s full-scale invasion of Ukraine in 2022 has slowly woken up European countries from decades of thinking there would be eternal peace. But executives and experts say the alarm has been heard more clearly in some areas than others, with defence being one obvious point.

But as the electricity blackouts show, there is a remarkable lack of thinking about societal resilience and paying extra to ensure systems work better in times of a crisis. The logistics crisis following the Covid-19 pandemic showed companies the importance of bolstering manufacturing supply chains. Those lessons need to learnt more broadly. Fältström and others worry that the next event — be it in internet infrastructure or elsewhere — could have more serious consequences.