GEOPOLITICS | ARTICLE TRANSLATED FROM SPANISH

Infrastructure Is Becoming the West's Greatest Vulnerability

A succession of failures, acts of sabotage and cyberattacks is forcing Europe and the United States to respond — and loosen the purse strings — to modernise systems designed for an analogue world.

Ignacio Fariza | Madrid | 21 November 2026, 17:13 CET

Original publication: EL PAÍS | Original title: "Las infraestructuras se convierten en el gran flanco débil de Occidente"

This is an unofficial English translation of the Spanish article for reference; it is not an authorised English edition.

The biggest air traffic control system outage in United States history abruptly halted take-offs and landings for four and a half hours in the country with the world's busiest skies. The airspace had not been forced into such silence since September 11. To make matters worse, it was the afternoon of Friday the 13th, and Microsoft, a technology company underpinning everyday operations at businesses around the world, was still struggling to recover from the biggest blackout in its history. US authorities attributed the aviation shutdown to a technical problem, but the White House's cybersecurity director was forced to leave his post a week later.

Days earlier, bomb threats had brought operations at schools, on aircraft and on trains to a halt in several EU countries, with the recent accidents in Spain still fresh in people's minds. Thousands of freezers in European supermarkets had suddenly warmed up amid a wave of cyberattacks, causing losses running into billions and leaving people deeply uneasy. Even France's national blood service was targeted. These were three more incidents in the so-called hybrid war, in which suspicions proliferate — France and Belgium have explicitly pointed to Iran in the freezer attacks — but those responsible are careful not to claim credit. On Thursday, the European Commission itself suffered a cyberattack whose consequences remain difficult to assess.

These incidents — to which we must add the 2025 blackout on the Iberian Peninsula and the recent failure of the US intelligence services' internal communications network — differ in nature, yet all have one thing in common: they expose the fragility of critical infrastructure and intensify the dangerous public perception that no one and nothing is safe. The systems and mechanisms on which hundreds of millions of people across the West rely in everyday life are considerably less dependable than had been assumed for decades.

This renewed vulnerability, in turn, has three dimensions. Psychological, because it causes personal anxiety. Sociological, because it calls into question the very foundations of social trust. And political, because, amid a particularly intense electoral cycle, it encourages support for parties promising to tear everything down and start again. The far right, always quick to seize the opportunity, channels vast amounts of populism and hatred through this dangerous opening — with considerable rewards at the ballot box.

Infrastructure fragility is an unpalatable problem with too many ingredients. Buildings and systems are ageing, designed more for the analogue era than the digital one, and for years they have not received the investment needed for anything beyond a cosmetic facelift, according to more than half a dozen specialists consulted for this article. There are dangerous adversaries in an increasingly hostile world: not since the Second World War have so many conflicts been underway. And there is accelerating global warming, causing ever greater damage. These overlapping pressures make the situation more urgent. Infrastructure is serious business, and after almost two decades of painfully inadequate investment since the financial crisis — public as well as private — the West has little time left to lose.

“The combination of hostile states, integrated computer systems and artificial intelligence is making threats increasingly frequent,” warns Jim Hall of the University of Oxford. In the field of climate risk, where the need for action is equally pressing, Beniamino Russo of the Polytechnic University of Catalonia has long warned that “much infrastructure was built according to the parameters of a past that will never return” and that “design criteria must be adapted, because the whole context has changed.”

What is happening? “Unfortunately, we live in a hybrid world, in which systems that were once purely physical now experience failures of a digital nature,” says Dimitris Simos, a professor of cybersecurity at the University of Salzburg. “So ageing is only part of the problem: the real weakest link is the combination of legacy systems and new digital technologies that must remain compatible with operations never designed for them.” This means, for example, that “standard cybersecurity solutions cannot simply be transferred to the safety systems of an aircraft or a power station.” Two technological eras coexist, with all the risks that entails.

“This recent sequence of events shows that infrastructure fragility is not a symptom of underdevelopment but a side effect of modernisation,” adds Simos, who has written extensively on the subject. “Electricity grids, airports and railway systems have been extensively digitalised, and the more digital and interconnected they become, the more new risks emerge. We systematically underestimate the fragility of interdependent systems: a small disruption at a single point can cascade through the entire system.”

The word “infrastructure” has an exceptionally broad meaning. It refers to physical assets, certainly, but increasingly to virtual ones too, as services account for a growing share of the global economy, particularly in the West. “The countries that understand this fragility earliest will also be the first to respond,” warn experts from the Organisation for Economic Co-operation and Development (OECD) in a special report published on Monday, while the shock of the previous week was still being felt. “And those that respond first will achieve better outcomes.”

“Western societies and economies rely heavily on complex and interconnected systems, which deliver enormous benefits when they work but have paralysing effects when they fail,” explains Timothy Less of the Centre for Risk Studies at the University of Cambridge. “And that, of course, has geopolitical implications, because these infrastructures represent a strategic vulnerability and an obvious target for hostile states seeking to harm us through hybrid tactics. Whether recent incidents were deliberately caused or resulted from technical problems, they illustrate the damage that failure of these systems can inflict.”

Less names specific countries. “Russia in particular, but also Iran, have identified this vulnerability: cyberattacks and physical sabotage allow them, at relatively low cost, to cause economic disruption, generate public anxiety and undermine trust in Western governments.” It is an extraordinarily effective combination, achieved at very low cost and without crossing the threshold into conventional warfare that might trigger a military response. “Given that there is little prospect of relations with either of these two countries improving in the near future, the West must prepare for further hybrid attacks, possibly on a larger scale,” warns the former British diplomat.

Year after year and decade after decade, the systems that support and sustain the everyday lives of Western societies and economies have become ever more interdependent. “Often in ways that remain invisible until something fails,” observes Stergios Mitoulis, founder and director of the Centre for Global Infrastructure Resilience at University College London. There is no reason to expect that trend to reverse.

A problem does not have to be particularly severe to cause major disruption: it is enough for it to affect a component on which other services depend. “Airports, railways, hospitals and businesses depend on electricity, communications and, increasingly, shared digital services. That allows failures to spread far beyond their point of origin,” explains the Greek academic.

“What we must understand is that national security depends not only on military capability but also on the resilience of these essential infrastructures, including the new risks posed by sabotage and cyberattacks,” Mitoulis adds. He also calls for essential services to undergo regular stress testing: “What would happen if electricity and communications failed at the same time? How could hospitals or transport networks

continue to operate safely?" Ultimately, success, he concludes, "means maintaining the reliability of essential services throughout their service life and learning from every disruption to reduce the consequences of the next one."

A question of money

The major business consultancies — the world of money, in other words — have been sounding the alarm for some time, using staggering figures. McKinsey estimates that the world will need to invest more than an additional $100 trillion (€90 trillion) in infrastructure by 2040, almost 50 times Spain's GDP. Boston Consulting Group puts Europe's needs alone at more than €12 trillion, with renewal particularly urgent there: spending 3.5% of GDP on this purpose, equivalent to roughly $800 billion a year, nearly three times the current level. Energy and urban development top the list.

The succession of shocks, to put it mildly, is also a reminder that infrastructure — particularly sophisticated infrastructure — is more delicate, and that maintenance is often its most important investment. "Many bridges, railway lines and other essential assets were designed decades ago for different demands, climatic conditions and technologies. Some have already exceeded their originally intended service life," explains Sotirios Argyroudis of Brunel University London. The challenge, he concludes, is not simply to maintain or replace ageing infrastructure, but to understand how vulnerable it is to today's demands.

"Unfortunately, political incentives always encourage favouring the new over the old: building is attractive; repairing is not," concludes Edward Glaeser of Harvard University. "I do not think we should conclude that all critical infrastructure in advanced economies is at risk, but clearly some has not received the attention it needs. It is a source of vulnerability, and adversaries will seek to exploit it."