Monday, September 22, 2025

tomorrowsaffairs.com

TA Tomorrow's Affairs

Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

The digital vulnerability of airports and the limits of European resilience

Last weekend, European air traffic was confronted with a crisis that came from a direction it least expected. It wasn't bad weather, a strike or a technical failure of the aircraft.

This time, the problem originated in the digital heart of the airport infrastructure – in the check-in software operated by the American company Collins Aerospace.

A cyber-attack on their system paralysed the operation of several major European airports and showed how much travel today depends on supply chains that are invisible to travellers but are key in practice.

Around 25 flights were cancelled in Brussels on Saturday, and the number rose to around 50 on Sunday. Faced with the impossibility of stabilising the system, airport management instructed the airlines to halve the number of departures for Monday.

Heathrow reported significant delays but managed to avoid major cancellations. In Berlin, queues were longer than ever, and passengers waited for hours to check in their luggage. Ireland was not spared either.

In Dublin and Cork, the second largest city in the south of the country, the problems were fewer than in Brussels or Berlin, but they were visible enough to show how an outage in one system can immediately spill across borders and affect the entire European airline network.

The European Union Agency for Cybersecurity (ENISA) confirmed that it was a ransomware attack targeting a third party, meaning that it was not the airports themselves that were targeted, but their provider.

This fact makes the incident all the more serious: it indicates that the resilience of European aviation depends not only on airports but also on the companies that provide the digital tools behind the scenes.

The weak point at the heart of the trip

The passenger check-in system seems trivial. A few clicks on the screen, a ticket and a baggage tag. But this is precisely where the chain of all further processes begins.

When this closes, everything comes to a standstill: the security check slows down, boarding is delayed, planes don't take off on time, and connections are cut short. This weekend has shown that an airport without digital check-in is as vulnerable as a hospital without electricity.

> Even when passengers had electronic tickets, baggage drop-off remained a bottleneck

In Brussels, the switch to manual procedures proved to be a temporary solution, but capacity was far below demand. Heathrow and Berlin relied on self-service kiosks and online check-ins, which mitigated some of the impact but could not prevent congestion.

Even when passengers had electronic tickets, baggage drop-off remained a bottleneck. Queues grew, nervousness spread and companies counted their losses.

Outsourcing and its consequences

The question that now arises is: to what extent is Europe prepared to transfer critical functions to third parties?

Although the airports are formally responsible, the actual operating systems are outsourced to companies that work worldwide and for dozens of customers at the same time. The failure of Collins Aerospace affects not just one airport but the entire continent.

> Europe needs to change its logic: resilience is no longer an add-on but a key element

The NIS2 directive (the new EU directive on cyber security and resilience of critical infrastructures) already categorises airports and their digital partners as critical infrastructures, but practice shows that this is not enough.

Contracts with providers have so far focused on efficiency and costs rather than resilience and security. The incident has shown that Europe needs to change its logic: resilience is no longer an add-on but a key element.

The economy of delay

Disruptions of this kind are not only measured by the number of cancelled flights. They have an impact on the entire economic system.

Delays mean additional costs for airlines – paying crews who exceed their working hours, accommodation costs for passengers who miss connections and penalties under EU passenger rights rules.

> For an economy where every minute counts, incidents like this become a serious test

Airports lose revenue from taxes and terminal sales. Travellers lose time and miss business commitments, resulting in an overall economic loss that amounts to hundreds of millions of euros on the continent.

For an economy where every minute counts, incidents like this become a serious test. This shows that digital infrastructure has a direct macroeconomic impact. If such disruptions are repeated, the consequences will not just be localised but systemic – a decline in confidence in the reliability of European transport and an increase in insurance costs for the sector as a whole.

Geopolitical dimension

What begins as a technical problem quickly takes on a political dimension. Over the past decade, Europe has made efforts to protect its energy infrastructure from cyber-attacks but has neglected transport.

Now it is clear that airports also fall into the same categories of vulnerability. If an attack on one provider can bring operations in three major European cities to a standstill, it means that a coordinated attack could have serious political consequences.

> If a cyber-attack can bring major airports to a standstill, it is not only a blow to passengers and businesses but also to Europe's political power

At a time when Europe is balancing between the war in Ukraine, relations with China and the global technology race, the ability to maintain stable air traffic is becoming part of the bigger security picture.

If a cyber-attack can bring major airports to a standstill, it is not only a blow to passengers and businesses but also to Europe's political power – disrupting supply flows, slowing diplomatic missions and raising questions about how prepared the Union would be in the event of a more serious security crisis.

What comes next?

Initial reactions indicate that Brussels will seek stricter contractual obligations and security standards for providers of digital services. This means mandatory audits, "stress tests" and even the duplication of key systems to provide a backup option. Greater transparency in the supply chain will become an obligation, not a recommendation.

Brussels will seek stricter contractual obligations and security standards for providers of digital services

Insurers will also respond. Policies covering business interruption in the aviation industry will need to include third-party liability. This will drive up costs but will also force providers to invest more in security.

Passengers may increasingly switch to digital tickets and online check-in, but this will not eliminate a key problem – baggage drop-off and reliance on a centralised system.

Changing habits only partly makes it easier, while the real responsibility lies with the airports and providers who must ensure that the system works even if it is attacked.

Lessons for Europe

This incident is a warning that Europe cannot rely on technical improvisation alone. Manual check-ins may work for a day, but they are not a solution for long-term challenges.

Europe needs to think about the resilience of its digital infrastructure, as well as the defence of its borders. Airports are hubs of mobility, and mobility is the basis of the economy and politics.

> It has been demonstrated that the digital infrastructure of airports must be treated as a strategic point

If such incidents are repeated, it is not only the punctuality of flights that is under attack but also confidence in Europe's ability to maintain mobility.

Then the question is not reduced to queues and delays but rather to the credibility of the Union before its own citizens and partners – whether it is able to maintain continuity when its key systems are under threat.

What happened at Collins Aerospace was not just a technical incident but a dress rehearsal for Europe. It has been demonstrated that the digital infrastructure of airports must be treated as a strategic point, just like energy networks or defence systems.

If Europe doesn't invest in this resilience, it will not only have long lines and cancelled flights, but it will also seem weak to its citizens and enemies. And in today's world, vulnerability rapidly becomes a weakness that others can exploit.