International Railway Journal

EU cyber reforms address risks to national railways

The benefits of digitalisation have a dark flip side: the ability of bad actors to compromise railway systems. Enno Wiebe, director general of European Rail Supply Industry Association (Unife), explains how new European legislation is helping to minimise cyber risks to rail networks.

Departure boards at Italian stations were not updated due to a cyber-attack.

Photo Credit: Shutterstock

CONSIDER for a moment the thousands of data points a rail network can offer to anyone with access: ticketing and payment information, timetables, the location of rolling stock and consignments, and other sensitive data. By themselves these individual pieces of data are of little value, but together they offer an accurate picture of what is happening across the network at any given moment.

This is excellent for legitimate actors. Digitalisation is already enhancing safety and energy efficiency, boosting operational capacity and assisting with maintenance in real time. Yet in the hands of the wrong people, this information might be used to conduct surveillance of thousands of locations, disrupt the movement of passenger or freight trains, and even military equipment within the European Union (EU).

With this threat in mind, what is the optimal way of unlocking the benefits of digitalisation while simultaneously maintaining sovereignty, security and control?

The answer to this question is quite simple: establishing a solid basis for trusting the technological components and systems that make up our networks. With the latest cybersecurity reforms in Europe, this is now not just possible but absolutely necessary.

Unife has and will continue to call for rail to be designated as a strategic sector.

Enno Wiebe

In January, the European Commission (EC) announced a comprehensive new cybersecurity package including a proposal to revise the Cybersecurity Act adopted in 2019 and amended last year. The proposal will follow ordinary legislative procedure and must be examined by the European Parliament and the European Council before final approval. A period of consultation, technical adjustment, and inter-institutional negotiation is expected before it enters into force next year.

One of the proposed changes would empower the EC to designate third-party countries and ICT suppliers as high-risk, and ban them from the supply chains of critical sectors.

A preliminary analysis shows that the rail sector could be subject to these provisions.

Under recent reforms, the European Agency for Cybersecurity (Enisa) has been empowered to work alongside national authorities in market surveillance exercises to ensure that products do not present threats to European infrastructure. Enisa is also working to identify new categories of digital products for which surveillance may be organised.

Unife believes that suppliers who might pose some element of threat must be barred from supplying to the EU. This is a bold response, but given the nature of current events, we believe it is justified. After all, trust is essential. Every functioning human system or institution operates on the principle of trust and a railway is no different.

Strategic risk

For some suppliers from non-EU countries, especially under foreign government influence, that trust should not be taken for granted. We believe that there is a strategic risk to Europe, especially regarding sovereignty and control, and we consider our role as representatives of the European rail supply industry to include alerting European institutions to these possible threats.

Last autumn a Norwegian public transport authority discovered that its new fleet of Chinese-built buses was fitted with SIM cards that could potentially offer remote access to vehicle control systems. Similar issues have emerged in other industries and sectors, from private cars to wind energy. Such a scenario with European rolling stock would, in our view, be completely unacceptable. After all, the world is a more uncertain and unpredictable place today, with shifting geopolitical allegiances. To ensure security, retain trust in the railways and limit sovereign risk, any broader initiative to tackle these challenges must be supported and enacted.

As EU member states invest or consider investing in non-EU technologies for their rail networks, we believe that procurement must take into consideration aspects other than cost. We therefore support updated public procurement initiatives, which the EU is set to deliver later this year.

As part of the cybersecurity reforms being undertaken by the EC, Unife has and will continue to call for rail to be designated as a strategic sector. Rail plays a key role in moving critical goods in supply chains and military equipment across the continent, while also possessing a significant economic and employment footprint. Cybersecurity might not always be at the forefront of purchasing decisions, but we believe the kind of thought processes outlined above will need to become part and parcel of procurement across Europe's rail sector.

There are still elements of the reform package where the EC and Enisa need to provide more clarity. The extent to which rail products will be covered by the new legislation will depend on the identification of key ICT assets and high-risk vendors by the EC. This can only be done through institutional actors like member states and EU bodies, and we remain open to working with these stakeholders. We will also continue to work with the EC to ensure that processes which govern the security of digital products within the EU function optimally, including full industry compliance with the Cyber Resilience Act by the end of 2027.

We will use our position within the EC's Cyber Resilience Act Expert Group to communicate how we can strike a balance between deploying digital products that are safe, and offering suppliers of cybersecurity software the flexibility needed to remain ahead of nefarious actors.

In a shifting world order, the roles and responsibilities of Europe's railways have expanded. Russia's war against Ukraine and broader geopolitical instability, emphasised by a new conflict in the Middle East, have only reinforced the importance of transport networks for defence. We therefore believe it is time for all of us working in the rail sector to be more proactive and that starts with being more cybersecure.

https://www.railjournal.com/opinion/eu-cyber-reforms-address-risks-to-national-railways/