5th ERA-ENISA Conference on Cybersecurity in Railways

Distinguished representatives of the European Union Agency for Railways and the European Union Agency for Cybersecurity, dear colleagues, and cybersecurity and railway-sector professionals,

I am very pleased to welcome you to Tallinn at the fifth Conference on Cybersecurity in Railways!

It is quite logical that this conference has moved from Lille and Athens to Tallinn this time.

Here, to Estonia – known as a digital state – where, on NATO's eastern flank, we are developing the largest infrastructure project in the Baltic region and one of Europe's most large-scale high-speed rail connections. Tallinn is also home to NATO's Cooperative Cyber Defence Centre of Excellence.

Today you are dealing with two questions that are very familiar to Estonia.

1. How do we keep railways functioning as the backbone of our everyday economy and people's mobility?
2. And how do we ensure that this backbone does not break under the pressure of hybrid attacks, cyber threats and sabotage?

The experience of recent years in Europe shows that attacks against railways are no longer a theoretical scenario. They are part of everyday reality.

Over the last two years, Russian hackers have carried out thousands of cyberattacks on the railway infrastructure of the European Union.

- The signalling systems of the Czech railway company have come under attack, disrupting the ticketing system.
- Near Bremen, a railway cable shaft was set on fire, leading to a full day of disruption on the line between Hamburg and Bremen.
- In Spain, cable theft and a technical failure disrupted high-speed train services for two days, leaving more than 10 000 people stranded on the line between Madrid and Seville.
- In Estonia, an attack targeted the ticketing system of the passenger rail company, making it difficult to buy train tickets both online and on board.

These are just a few examples – different facets of one and the same hybrid campaign.

In the Baltic region, there is another dimension that is becoming increasingly important: the disruption of satellite navigation and communications.

Estonia and our neighbours have witnessed a sharp increase in GPS jamming, both in aviation and in maritime transport. In some cases this has led to flight interruptions, and at times up to 85% of flights to and from Estonia experience navigation disturbances at some point.

But these disruptions are increasingly reaching land as well. Precise location information, the correct time and reliable communications are just as critical in rail traffic management, in logistics chains and in military planning as they are in aviation.

If satellite navigation or communications fail, the rest of the system – including the railway – must be designed so that it does not collapse like a row of dominoes.

In recent years, Estonian Railways has therefore taken very significant steps forward.

- We are electrifying and digitalising the entire core railway network and increasing train speeds on it.
- And we are thoroughly upgrading our control, signalling and communications systems.

A large part of this work means replacing legacy technology – phasing out Soviet-era systems and introducing modern, software-based control and signalling solutions.

On the one hand, this makes the railway safer and more efficient. On the other hand, the more we rely on software and networked solutions, the more important it becomes that cybersecurity is built in from the outset, rather than bolted on as an afterthought.

In other words: cyber and physical security must go hand in hand. No electrified line, new control centre or communication project can move forward today without a cybersecurity perspective.

Secondly, Estonia is building Rail Baltica together with Latvia and Lithuania.

For the Baltic States, Rail Baltica is much more than a new high-speed railway. It is:

- a new main axis for passenger and freight transport,
- our economic corridor to Europe,
- and, from the perspective of the EU and NATO, one of the key corridors for allied movements on the eastern flank of the Baltic Sea.

The European Commission recently presented a new development plan for high-speed rail. This once again confirmed that Rail Baltica is seen as one of the strategic core routes connecting European capitals and major centres. It is a very clear signal that all of Europe views Rail Baltica as a shared priority.

Our goal is that, in five years' time – in 2030 – the railway will be ready.

And it goes without saying: if we are building a railway that must be able, in a crisis, to carry NATO supplies, then it has to be designed to withstand cyberattacks, satellite navigation disturbances and acts of sabotage.

Cybersecurity requirements in Rail Baltica have therefore been written into the design guidelines, the architecture of the technical systems and the conditions of the tenders. The same principle must also apply to future maintenance and operation contracts.

I want to emphasise that regulations and requirements are undoubtedly an important part of security, but they are not the whole story.

There are two other essential elements.

1. First – situational awareness.

We cannot afford to have anyone working in an information vacuum. We must share information about attacks, incidents and emerging trends before they escalate into a crisis – whether we are talking about cyberattacks, sabotage, or disruptions to communications and navigation.

Hybrid influencing activities do not respect national or sectoral borders, which means our defence must also be interconnected rather than fragmented.

Monitoring the patterns of hybrid attacks and being able to respond quickly are just as important for vital services as any new technical security measure. Today's conference is a good example of how to strengthen this shared situational picture.

2. Second – people, skills and exercising.

We may have the best technology in the world, but if, at the moment of an attack, our team is exhausted, understaffed, or has never practised a similar scenario in a realistic exercise, that may become our weakest link.

We need more joint exercises, more cooperation between different authorities, companies and cybersecurity units, and more practical training specifically focused on industrial control systems and the particularities of rail.

In cybersecurity, no one can cope by struggling alone.

Estonia's location has compelled us to deal with cyber and security issues earlier, and in some cases more intensively, than some larger countries.

We are used to taking responsibility for our own security – doing ourselves what needs to be done, and doing it together with our allies.

We want to share what we have learned and, just as importantly, to listen to what others have learned – whether that experience comes from the Czech Republic, Spain, Germany or right here in the Baltic region.

So thank you to ERA and ENISA for bringing this conference to Estonia.

And thank you to all of you for taking the time to come here – to what is becoming an increasingly important railway hub – to strengthen together this invisible, yet ever more crucial, layer of defence.

As President of the European Commission Ursula von der Leyen said here in Tallinn a few years ago: "Critical infrastructure is the new frontier of warfare. And Europe will be prepared."

For today, I wish you two things: substantive discussions and fewer cyber incidents.

And when the conference day is over, I hope you will also find a little time to enjoy Tallinn itself – not only your hotel and the conference room.

In the Old Town, on Town Hall Square, there is a Christmas market which, by the way, has been named the best Christmas market in Europe.

Welcome to Estonia, and I wish you every success in your work!