In this article, the CIT`s Chair of the CUI Committee, Adriaan Hagdorn (NS), addresses the very topical issue of rail transport and cyber security.

The NIS Directive and the Cyber Security Act

General

As in many fields, digitalisation and automation have also increased in the rail transport sector. ERTMS will be rolled out in the EU in the coming decades. Logistics and information chains are mostly fully digitalised: electronic bills for goods and e-tickets for passengers have become commonplace. Arrival and departure information, travel and passenger information, information about the cargo, in particular about dangerous goods, about bookings, tariffs and the general terms and conditions are all processed electronically. The TSI TAP and TSI TAF provides harmonized requirements for the necessary ICT architecture. That will not only increase interoperability and convenience for passengers and shippers, but also imposes general requirements on the safety, reliability and availability of the information systems.

However, there is a downside: network and information systems might be vulnerable to cybercriminals, as two examples in the rail transport show. In May 2017, DB Bahn was one of the victims of the WannaCry ransomware globalhack which prevented passenger information from being displayed at stations and made online ticketing impossible for some time. In April 2018, a customer database of Britain's Great Western Railways was hacked, compromising the personal data of about a thousand customers.

European legislation is one of the tools – besides technical and organisational measures and so on – to improve cybersecurity in the EU to an acceptable level. This article provides a brief overview of the current and some future European legislation, which is or will be important for railway undertakings and infrastructure managers.

The NIS Directive

General

The NIS Directive (Directive (EU) 2016/1148 laying down measures for a high common level of security of network and information systems) aims to achieve a high, unified, and coherent common level of security of network and information systems in the EU to support and promote society and the economy, increase digital resilience and reduce the impact of cyber incidents. The underlying aim of the NIS Directive is to protect and to improve the functioning of the internal European market.

The NIS Directive uses a broad definition of 'network and information systems'. These are:

a) *an electronic communications network within the meaning of Article 2(a) of*

Directive 2002/21/EC,

b) *any device or group of interconnected[5] or related devices, one or more of which, pursuant to a program, performs automatic processing of digital data, or*
c) *digital data stored, processed, retrieved or transmitted through the elements referred to in points (a) and (b) for the purposes of their operation, use, protection and maintenance;*

Therefore it concerns the combination of (interlinked) hardware, software and the data processed by it. Apart from a very general reference to the Internet, the NIS Directive does not elaborate on this.

The NIS Directive defines 'security of network and information systems' as

> *the ability of network and information systems to resist, at a given level of confidence, actions that compromise the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or the related services offered by or accessible via these network and information systems.*

The NIS Directive is a minimum directive, except in the case of digital service providers where it is stipulated that Member States may not impose any other security or reporting obligations. For the operators of essential services (OES) discussed below, Member States are free to impose a higher level of security.

To the extent that EU legislation prescribes a different or higher level of security, the NIS Directive is without prejudice to such other legislation. This is the case, for example, with the General Data Protection Regulation (GDPR) that also prescribes that appropriate technical and organisational measures must be taken to achieve a security level for the processing of personal data that is appropriate to the potential risks.

Member States may also take other measures independently of the NIS Directive to protect essential State functions, national security or public order.

The NIS Directive contains no standards for the intended high common level of security or for the degree of reliability. This puts the harmonization of the desired level of security in the EU into perspective. For instance the Netherlands opted for an instrumental approachwhereby primarily an OES must determine for itself, within the frameworks of the Dutch Network and Information Systems Security Act (via which the NIS Directive was transposed), which measures are appropriate and proportionate.

However, the NIS Directive also contains a standardisation provision encouraging Member States to use European or internationally accepted standards and/or specifications for the security of network and information systems, without imposing the use of any particular type of technology.

Obligations of Member States

Under the NIS Directive, Member States have the following three obligations:

(i) Adoption of a national strategy

Each Member State shall adopt a national strategy for the security of network and information systems that sets strategic objectives and appropriate policy and regulatory measures. This strategy shall include the objective, the governance framework, preparedness, response and recovery measures, education, awareness and training programs and research and development. The national strategy shall be communicated to the European Commission. A risk assessment plan must also be drawn up to identify the risks.

(ii) Monitoring and cooperation

Each Member State shall designate one or more competent authorities for the following sectors to monitor the application of the Directive at national level. It must also designate a national contact point for cross-border cooperation with the authorities of other Member States, the cooperation group referred to in Article 11 of the NIS Directive and with the network of national (collective) Computer Security Incident Response Teams (CSIRT's). A CSIRT is a (national) cooperative association with the purpose of ensuring a centralised, specialised and coordinated approach to cyber incidents. A European network of national CSIRTs should contribute to building trust between Member States and facilitate rapid and effective operational cooperation. The cooperation group shall be composed of representatives of the Member States, theCommission and ENISA, and shall deal with the strategic aspects of the cooperation. The EU may conclude international agreements or treaties with third countries or international organisations allowing and organising their participation in some of the activities of the cooperation group.

(iii) Designation of an OES

The NIS Directive requires Member States to designate operators of essential services (OES) for various (sub) sectors. These sectors are energy, transport (including rail), banking, financial market infrastructure, healthcare, supply and distribution of drinking water, and digital infrastructure.

The three criteria for whether an entity qualifies for OES-status are formulated in rather general terms:

(i) the entity provides a service that is essential to the maintenance of critical social and/or economic activities,
(ii) the provision of the service depends on network and information systems, and
(iii) an incident would have significantly disruptive effects on the provision of the service.

Here too, the NIS Directive leaves it to the Member States to determine 'significantly disruptive effects'. The Directive gives general criteria, including the number of users that depend on the service, the consequences that an incident may have, the market share of the service operator, and the geographical extent of the area that may be affected. Sector-specific factors must also be taken into account.

The NIS Directive applies to OES (designated as such). An OES can be a public or private entity and therefore also applies to government organisations providing essential services. Furthermore, the NIS Directive applies to "digital service providers", defined as any legal entity that offers a digital service. Digital service includes entities offering online services such as marketplace and search engines and cloud computing services.
For the rail sector, the NIS Directive identifies infrastructure managers and railway undertakings, as defined in Article 3 of Directive 2012/34/EU, as (to be designated) OES. In the Netherlands, Infrastructure Manager ProRail and railway undertakings providing passenger transport such as the Dutch Railways, will be designated as an OES by the Ministry of Transport.

Level of security requirements

The NIS Directive requires Member States to ensure that an OES takes appropriate and proportionate technical and organisational measures, having regard to the state of the art, to manage the risks to the security of network and information systems used in their activities. The level of security should be appropriate to the risks that are or might be encountered. Furthermore, an OES must take appropriate measures to prevent and minimise the consequences of cyber incidents in order to ensure the continuity of the essential services offered by the OES. This means that the duty of care for an OES is twofold:

(i) preventive management of potential risks, and
(ii) if such a cyber risk occurs, preventing and minimizing its adverse effects.

However, the question is what this duty of care actually involves and how far-reaching it is. This is not always clear. As indicated, the NIS Directive uses a broad definition of network and information systems without giving any further details. Information systems will often involve systems that are dependent on the Internet, but that this is not a requirement. This description does, however, give each OES the opportunity to determine, on the basis of the nature of the data stored, sent and processed by it, the related services and the probability of a disruption and its consequences, whether or not a network and information system usedby it falls within the scope of the NIS Directive.

Because the NIS Directive does not contain any concrete, technical standards that an OES or any other party must comply with, this duty of care must also be determined and fleshed out substantively by the OES, in consultation with the responsible ministry, on the

basis of a threat and risk analysis. The nature of the expected risks, the nature and extent of the possible consequences for the (transport) services to be provided and the (un)feasibility of (technical and organisational) measures to prevent or limit the risks and consequences as much as possible, are important parameters. This therefore requires careful consideration by the OES. Also, this duty of care needs ongoing attention. In the area of ICT and cyber security, technical developments are rapid. A measure may be appropriate and proportionate now in order to prevent a security risk but may no longer be so a year later. It is therefore necessary to constantly keep one's finger on the pulse and consider whether the measures taken are still adequate. National regulations have to provide guidance in this regard.

In the Netherlands, the OES must take in any case the following five measures:

(i) A risk-based approach

The operator has an up-to-date overview of the network and information systems that support its essential service. The operator draws up a risk analysis in which it describes the risks with regard to security and explains how it will reduce the risks to an appropriate level. The operator must justify why it considers this level to be proportional and acceptable. In this justification, it shall in any case take into account the organization-specific and sector-specific risks, the social importance of his essential service and the state of the art. It will record the results of the risk analysis and incorporate them in security and control measures.

(ii) Organization of network and information security management

The operator has an information security policy and strategy and applies them actively. It has invested the tasks, powers and responsibilities for the security and management of its network and information systems in the organization.

(iii) Preventing incidents

The operator has a layered security strategy that is based on the risks that follow from the risk analysis. Defence in depth, lifecycle, asset, patch, identification and access management are at least part of this strategy. When the attention of relevant bodies such as suppliers or relevant government agencies is drawn to security advice and threat information, the operator will assess whether additional measures are necessary on the basis of the state of the art in order to reduce the identified risks to an appropriate level. The operator records the findings of its assessment in writing.

(iv) Detection and response

The operator has organized the security of its network and information systems in such a way that it can detect, analyse and record incidents and

limit the consequences as far as possible. The operator will monitor network and information systems structurally for vulnerabilities and possible compromise, taking into account the available threat information. It will be responsible for logging operations on the network and information systems and will retain this data long enough to be able to analyse incidents. It follows procedures with regard to the response to incidents.

(v) Limiting the consequences of incidents

The operator shall establish a business continuity policy and crisis management policy for the network and information systems. The crisis management policy at least consists of a plan to restore the essential service as soon as possible after an incident. Implementation of the crisis management policy shall therefore be periodically practiced.

These five measures have been elaborated by the Dutch Ministry of Transport saying that an OES in that sector must apply an Information Security Management System (ISMS). This ISMS is a process-oriented and systematic approach to information security that must enable the OES to take, implement and adjust all those measures that are necessary to structurally reduce security risks to an acceptable level and to keep them there. This includes a reasoned description of what levels of risk are acceptable for the essential service that the organisation provides. This must also include the reasonably foreseeable risks within the supply chain. This risk analysis must be updated periodically or as risks increase or decrease. The ISMS must include at least the following topics:

(i) improvement cycle
(ii) a description of the internal organization
(iii) the network and information systems used
(iv) the cyber incident prevention measures (patch management, supply management, design requirements, physical security policies, access security, software security and controlled change management)
(v) the method of detecting, reporting, logging and responding to incidents
(vi) the recovery policy (continuity plans and recovery by backups).

It is therefore a management system in which the risk management process is central. This approach is useful because the ISMS provides the OES with the framework and methodology to quickly respond to the increasing and rapidly changing security risks, as they can also occur in the railway sector. This means that every OES must constantly ask itself which network and information systems, software, data and related services fall within the scope of the NIS Directive, as transposed in national law. Based on a risk analysis, an OES will need to determine the nature, scope and potential consequences of the degradation or failure of these 'crown jewels' (through hacking or otherwise) and the inability or unavailability of certain data essential to the OES or related services offered through those network andinformation systems. In any case, the potential consequences

for the continuity and security of the (transport) processes carried out by the OES will have to be considered. This cannot be entirely new. Sector safety regulations and the internal quality, safety management and control systems will also often prescribe that such risks be inventoried and named and, as far as possible, removed or controlled.

The GDPR contains a similar obligation for parties processing personal data to take appropriate technical or organisational measures to secure information in order to ensure a level of security appropriate to the risk involved, taking into account the stateof the art, the cost of implementation, the nature, scope and context of the processing,the purposes of the processing and the possible risks of data subjects.

The NIS Directive requires OES to report incidents with significant impact on the continuity of essential services they provide immediately ('promptly') to the competent national authority or the CSIRT. This notification must contain sufficient information to allow them to determine any cross-border implications. The NIS Directive stipulates that notification does not lead to increased liability for the notifying party. The directive leaves open which (increased) liability for which damage and vis-à-vis whom could be atissue in the event of an incident.

To determine whether an incident has significant consequences, at least the following criteria are important:

(i) the number of users affected by the disruption,

(ii) the duration of the incident and

(iii) the geographical extent of the affected area.

These criteria will have to be completed and applied by the OES themselves. Other parameters can also be taken into account. For public transport, the dependence of passengers on public transport may be considered. For the transport of goods, the consequences for the surrounding area in the event of an incident involving the transport of hazardous substances and the degree of disruption of the logistics chain, which is often organised on the basis of real time delivery, are relevant. If circumstances permit, the competent authority may inform the OES what has been done with its notification.

In the event of a cyber security incident, personal data relating to natural persons, such as employees and passengers, are often released unintentionally. This will also constitute a breach of personal data. Pursuant to the GDPR, the controller must notify the Regulatory Body within 72 hours of becoming aware of this. If the breach involves a high risk to their rights and freedoms, the controller must also inform the natural persons concerned immediately. A cyber incident may therefore lead to a concurrence of notification obligations: pursuant to the NIS Directive (as transposed) and pursuant to the GDPR.

The NIS Directive requires Member States to designate an entity as the national

competent authority. This provision relates in particular to administrative enforcement.

As regards monitoring and enforcement, the NIS Directive provides in its usual terms that Member States shall lay down rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive. Those penalties must be effective, proportionate and dissuasive.

Cyber Security Act

Another important piece of legislation is the European Cybersecurity Act: Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification.

With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down:

(i) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and

(ii) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

Certification should improve the functioning of the internal market by enhancing cybersecurity and allowing European certification of ICT products, services and processes. In addition, ENISA in cooperation with Member States, provides advice and guidance on standards for cybersecurity.

European developments

The Commission has found that European industry is not sufficiently resilient to the ever-increasing cyber-threats and that existing resilience is unevenly spread among Member States and sectors. The Commission also believes that there is not enough common understanding of the main threats and challenges in the Member States and no common crisis response. Therefore, in December 2020 the Commission launched its EU Cybersecurity Strategy for the Digital Decade. One of the aspects of that strategy contains new legislation: the NIS 2 Directive and regulation on the resilience of infrastructure.

NIS 2 Directive

To improve cyber resilience in the EU, the Commission put forward a comprehensive proposal for a new directive in December 2020 (the NIS 2 Directive). It was approved by

the Council in December 2021 and is now subject to interinstitutional negotiations (trilogues).

The NIS 2 Directive aims to overcome the shortcomings of the current NIS Directive identified by the Commission and to improve cybersecurity in the EU. For example, the scope is extended: new sectors are added, including pharmaceuticals, and the category of digital service provider is modernised and expanded to include data centres, among others. The NIS 2 Directive makes a distinction between essential sectors such as railway transport and important sectors. Regarding rail transport, not only the infrastructure manager and the railway undertaking, but also an operator of a service facility referred to Article 3.12 of Directive (EU) 2012/34 can be designated as an essential entity.

The NIS 2 Directive continues to aim for minimum harmonisation with the possibility of additional regulation at a national level, but no longer differentiates between operators of essential services and digital service providers. In addition, on the basis of a size criterion, all medium and large enterprises - pursuant to Commission Recommendation 2003/361/EC - in the relevant sectors will be covered by the NIS 2 Directive. Member States have discretion to include smaller organisations with a high security riskprofile within the scope of their implementing legislation. The security and reporting requirements for companies will be tightened and streamlined. Instead of the current open norm to take appropriate measures, there will be minimum requirements that must be met. This may also include certification requirements. The Commission also wants to improve the security of supply chains and supplier relations.

At European level, the proposal aims to increase the cybersecurity of the supply chain for key information and communication technologies. Member States, in cooperation with the Commission and ENISA, could carry out coordinated risk assessments of critical supply chains.

An important adjustment to the proposed NIS 2 Directive is enhanced supervision, with the possibility of punitive fees, security audits, preventive supervision and stricter enforcement and harmonisation of sanctions in the Member States for the essential sectors. Furthermore, a far reaching proposal has been made whereby natural persons in key positions within essential entities that fail to comply could be held personally liable.

Finally, the NIS 2 Directive enhances the role of the cooperation group and broadens the exchange of information and cooperation between the authorities of the Member States.

Resilience of infrastructure

Although not directly related to cybersecurity, for the sake of completeness the Commission's proposal for a Directive on the resilience of critical entities should be

mentioned here. This proposal replaces Directive 2008/114/EU on European Critical Infrastructures which, in addition to energy (electricity, oil and gas), includes road,air and rail transport, inland waterway transport and maritime transport (short sea shipping, large sea shipping).

The proposal aims at increasing the resilience of providers of essential services (referredto as "critical entities") which are vital for the preservation of vital societal functions or economic activities. This proposal also covers energy (electricity, heating, oil, gas and hydrogen) and – again - transport (by air, rail, water and road), but adds the following sectors: banking, financial infrastructure, health, drinking and waste water, digital infrastructure,public administration and space.

The proposal is fully consistent with the NIS 2 Directive and contains similar provisions but with a much wider scope. The proposal covers all natural and man-made hazards, such as accidents, natural disasters, hostile threats including terrorist attacks, and pandemics, such as the current COVID 19 pandemic.

Furthermore, on 14 December 2021, the Commission published, among others, a new proposed Regulation on “EU Guidelines for the development of the trans-European transport network (TEN-T Guidelines)”. With this proposal the Commission has aligned the future development of the TEN-T network to the European Green Deal objectives and the climate targets of the EU Climate Law. This includes an increased attention to the resilience aspects of the TEN-T network to natural and human-made disasters via climate-proofing requirements and environmental impact assessments for new infrastructure projects, as well as on the implications of accidents or breakdown (e.g. by enabling alternative route alignments to the main network). In article 46 of the proposed Regulation, cybersecurity and resilience of infrastructure, with particular attention to cross-border infrastructure, are mentioned as one of the aspects to take into consideration when planning new infrastructure projects.

Adrian Hagdorn
Senior In-House-Lawyer, NS