CENTRE FOR IT & IP LAW

CiTiP Working Paper Series

On the edge of the NIS Directive: the proposed C-ITS Delegated Regulation, friend or foe?

Charlotte Ducuing

CiTiP Working Paper 2019

KU Leuven Centre for IT & IP Law - imec

14 November 2019

Title

Charlotte Ducuing¹

Table of Contents

Abstract	3
Keywords	3
1. Introduction.....	4
2. The proposed Regulation and its overlooked interface with the NIS Directive	6
2.1. A brief history of the stillborn proposed Regulation.....	6
2.2. An introduction to the regulatory overlap in security regulation of C-ITS.....	7
3. The legal regimes imposing security obligations in the field of C-ITS	9
3.1. NIS Directive regulating providers of essential services	9
3.2. Who is the “Operator of (Cooperative) Intelligent Transport Systems”?	10
3.3. Security obligations related to C-ITS Station Operators in the proposed Regulation.....	13
4. NIS vs. C-ITS? Towards an interpretation of Article 1 (7) of the NIS Directive	14
4.1. The not-as-straightforward-as-it-seems Article 1 (7) NIS Directive	15
4.2. C-ITS as a case study to understand Article 1 (7) of the NIS Directive	17
4.2.1. The scope <i>rationae materiae</i> and the lack of a uniform terminology	17
4.2.2. Security vs. notification obligations: The NIS Directive’s internal inconsistency	19
4.2.3. Comparing apples and oranges?	20
5. Conclusion	23
Acknowledgement.....	24

¹ Charlotte Ducuing is a doctoral researcher at CITIP (KU Leuven). The author can be contacted at charlotte.ducuing@kuleuven.be.

Abstract

The paper discusses the interpretation of the *lex specialis* rule of Article 1 (7) of the NIS Directive, which has deserved little scholarly attention so far. Article 1 (7) NIS Directive organises the interface between the NIS Directive regime and other European Union sector-specific legislations imposing (cyber)security obligations, by laying down the conditions according to which such obligations would prevail over the NIS Directive regime. To do so, the recent proposal from the European Commission to regulate Cooperative Intelligent Transport Systems ('C-ITS') serves as a practical case study. Even though the proposal was eventually turned down by the Council, the regulation of C-ITS remains top on the agenda of the European Commission. Its relevance for the present study also detracts from the fact that, while obviously dealing with (cyber)security, the Proposed C-ITS Regulation barely envisaged the interface with the NIS Directive.

The paper finds that the NIS Directive is unclear on a number of aspects related to its interface with other EU legal frameworks, and notably in the field of ITS. In anticipation of a potential future C-ITS regulation, the paper makes suggestions to smoothly regulate the interface with the NIS Directive and eventually bring legal certainty to the actors involved. Finally, recommendations are made with respect to the interpretation and application of the *lex specialis* rule of Article 1 (7) NIS Directive.

Keywords

NIS Directive, Cooperative Intelligent Transport Systems (C-ITS), ITS Directive, cybersecurity, security management regulation

This paper is a work-in-progress. Any constructive comments made to the author are very much welcome.

1. Introduction

The European Directive on the security of Network and Information Systems (the ‘NIS Directive’)² adopted in 2016 lays down measures to achieve a “high common level of security of network and information systems”, for the purpose of completing the internal market.³ Described as the “EU’s first cybersecurity law”, the Directive covers a broad scope, including both “operators of essential services”,⁴ such as airports or financial market infrastructures, and “digital service providers”,⁵ referring to cloud computing services, online marketplaces and online search engines.⁶ The NIS Directive is viewed as a baseline set of security standards⁷ for the protection of network and information systems of services constituting the “backbone of social and economic prosperity” in the European Union.⁸ In that respect, the NIS Directive can be conceived of as a *lex generalis*. For that reason, Art. 1 also regulates the interface of the Directive with *other* legal instruments which may happen to overlap with the provisions of the NIS Directive. Indeed, security of network and information systems may be *already* subject to sector-specific requirements at EU level, such as the electronic communications networks and services, thereby subject to an exemption to the NIS Directive provisions (Art. 1 3)). Additionally, EU legislation may enact sector-specific security requirements *after* the entry into force of the NIS Directive, which may cause overlap and legal uncertainty as for the applicable legal regime. The EU legislator anticipated such a situation⁹ in Art. 1 (7) NIS Directive, which lays down the conditions according to which EU sector-specific legal provisions would prevail over these of the NIS Directive. The NIS Directive demonstrably constitutes *lex generalis*, over which *lex specialis* provisions may therefore prevail, subject to the conditions laid down in Art. 1 (7).

At first sight, the *lex specialis* rule stated in Art. 1 (7) NIS Directive would seem straightforward. As a matter of fact, there is no legal literature specifically dedicated to its interpretation.¹⁰ Yet, moving from the law in the books to its application to real-life cases may prove more difficult. The present working paper investigates the relationship between the NIS Directive and an EU sector-specific proposed legislation dealing with security obligations: The Delegated Regulation proposed by the European

² Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194/1 (the ‘NIS Directive’). In that personal data are created and processed in C-ITS communications, the proposed Regulation also has an interface with data protection law, and especially the GDPR. This issue is however not discussed in the present paper.

³ NIS Directive, Art. 1 (1). On the internal market as a rationale for the extension of the involvement of the European Union in security in the digital environment, see Agnes Kasper and Alexandr Antonov, ‘Towards Conceptualizing EU Cybersecurity Law’ (University of Bonn; Center for European Integration Studies 2019) Discussion Paper C253 2019 24–26 <http://aei.pitt.edu/100365/1/DP-C253-Kasper_Antonov.pdf>.

⁴ Within the meaning of NIS Directive, Art. 4 (4).

⁵ Within the meaning of NIS Directive, Art. 4 (5).

⁶ NIS Directive, Annex III.

⁷ ‘The NIS Directive – a Practical Perspective’ (*Practical Law*) <<http://uk.practicallaw.thomsonreuters.com/Document/I1B2E1220C62211E5BEE8A79E11D00157/View/FullText.html?originationContext=document&transitionType=DocumentItem&contextData=%28sc.Default%29&comp=wlu>> accessed 6 November 2019.

⁸ Helena Carrapico and Benjamin Farrand, “Dialogue, Partnership and Empowerment for Network and Information Security”: The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers’ (2017) 67 *Crime, Law and Social Change* 245.

⁹ Marie-Theres Holzleitner and Johannes Reichl, ‘European Provisions for Cyber Security in the Smart Grid – an Overview of the NIS-Directive’ (2017) 134 *e & i Elektrotechnik und Informationstechnik* 14, 15.

¹⁰ Markopoulou and al. introduce the interface between the NIS Directive and other legislative frameworks, but they do not discuss the interpretation, while they discuss the relationship with the GDPR, see Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, ‘The New EU Cybersecurity Framework: The NIS Directive, ENISA’s Role and the General Data Protection Regulation’ [2019] *Computer Law & Security Review* 105336.

Commission to regulate C-ITS services and communications ('the proposed C-ITS Regulation'). C-ITS services are covered by security requirements both in the NIS Directive (as potential "essential services") and in the Proposed C-ITS Regulation.

C-ITS stands for "cooperative intelligent transport systems". C-ITS communications are a specific kind (namely, cooperative) or ITS communications. They are expected to enable road vehicles to exchange messages in a peer-to-peer fashion, with one another and with other participants in their environment, such as the road infrastructure (e.g. traffic signals) or even pedestrians. C-ITS communications are expected to increase road safety, traffic efficiency and driving comfort. They also constitute a building block towards safe automated driving.¹¹ However, given their cooperative character, C-ITS communications cannot deliver such benefits without a coordinated, trustworthy and interoperable deployment.¹² The proposal from the Commission aimed mainly to prevent a "fragmentation of the internal market in the field of C-ITS" and to "ensure their coordinated and coherent deployment". With this instrument, the Commission pursued the goal to "ensure compatibility, interoperability and continuity of C-ITS services in the deployment and operational use of Union-wide C-ITS services based on trusted and secure communication".¹³ As a result, security is one of the core objectives of the Proposed C-ITS Regulation.

The paper pursues two objectives. First, it aims to contribute to the on-going debate on the regulation of C-ITS. The proposed C-ITS Regulation was quashed in the Council in July 2019. However, the deployment of C-ITS remains high on the political agenda of the European Commission,¹⁴ so that a new text is likely to be proposed in the near future. In this case, the interface of the new text with the NIS Directive will have to be tackled and could benefit from the present study and recommendations. Second, the paper aims to contribute the legal analysis of the NIS Directive, which remains rather scarce, in particular regarding the *lex specialis* rule set forth in Art. 1 (7). To do so, the Proposed C-ITS Regulation is studied as a practical case study. The analysis mainly focuses on the figure of the "C-ITS Station Operator", as the European Commission proposed to define and regulate it, without prejudice to other actors which may be concerned. The present study is without prejudice to the analysis of other aspects of this controversial proposal. It should be viewed as a forward-looking paper, as C-ITS services are barely on the market yet.

The first section briefly presents the proposed (and abandoned) Proposed C-ITS Regulation and uncovers the overlooked interface with the NIS Directive. The second section introduces the regulation of security in, respectively, the NIS Directive and the proposed Regulation, with a focus on the "C-ITS

¹¹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility, COM(2016) 766 final.

¹² Commission Staff Working Document Impact Assessment, Accompanying the document Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems [C(2019) 1789 final] - {SEC(2019) 100 final} - {SWD(2019) 95 final}.

¹³ Proposed C-ITS Regulation, Rec. (3). The Proposed C-ITS Regulation did not lay down an *obligation to equip* road vehicles and/or road infrastructure with C-ITS Stations. However, C-ITS stations and services could be deployed and made available on the market only provided they would comply with the proposed Regulation, see Art. 3 and 6 of the Proposed C-ITS Regulation and the explanatory memorandum of the European Commission, p. 3.

¹⁴ See Samuel Stolton, 'Commission 'remains committed' to connected car plans, despite Council blocking', on Euractiv dated 19th September 2019, available here: https://www.euractiv.com/section/5g/news/commission-remains-committed-to-connected-car-plans-despite-council-blocking/?_ga=2.134080332.374840531.1569337114-1050189813.1569337114 (last visited 24th September 2019).

Station Operator” as the central actor in this environment. Third, the last section analyses the legal conditions for and consequences of the qualification of this sector-specific legal framework as *lex specialis* to the NIS Directive.

2. The proposed Regulation and its overlooked interface with the NIS Directive

2.1.A brief history of the stillborn proposed Regulation

In January 2019, the European Commission (EC) made publicly available a draft delegated regulation on C-ITS services based on the Intelligent Transport Systems Directive (‘ITS Directive’).¹⁵ Following a public consultation,¹⁶ the Commission notified a revised proposal on the 13th of March¹⁷ to the European Parliament (EP) and to the Council (the ‘Proposed C-ITS Regulation’). The C-ITS Regulation proposed by the European Commission did not see the light of day. It was objected to by the Council on the 8th of July 2019.¹⁸ As a result, the proposed Regulation was *not adopted*.¹⁹ In other words, from the perspective of the European Commission, it is now back to square one.

With the procedure of delegated acts laid down in the TFEU,²⁰ the European Commission is granted the power to “supplement or amend certain non-essential elements” of the legislative acts with “non-legislative acts of general application”, subject to legislative delegation. This procedure grants far-reaching competence to the European Commission, as a draft delegated act may be objected to by the European Parliament and / or the Council only provided they reach respectively a majority and a qualified majority *against* the proposal, within a limited period of time (in this case 2 months, subject to extension). It is therefore very rare for the Commission to face such criticism against a draft delegated act. This gives an idea of the turmoil triggered by the Proposed C-ITS Regulation within the EU institutions. As of the time of writing, the reasons for the objections have not been made public by the Council.²¹ Following legal concerns of several national delegations, the Council commissioned a legal opinion from its legal department concerning the proposal’s compatibility with the ITS Directive, the conferral of implementing powers, procedural questions as well as the potential existence (and breach) of the technology neutrality principle.²² The legal opinion of the legal department was issued

¹⁵ Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJ L 207/1 (the ‘ITS Directive’).

¹⁶ See here: https://ec.europa.eu/info/consultations/public-consultation-specifications-cooperative-intelligent-transport-systems_en.

¹⁷ The revised proposal is accessible here: [http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/actes_delegues/2019/01789/COM_AD\(2019\)01789_EN.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/actes_delegues/2019/01789/COM_AD(2019)01789_EN.pdf).

¹⁸ 2019/2651(DEA) Deployment and operational use of cooperative intelligent transport systems in the European Parliament’s Legislative observatory, see [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2019/2651\(DEA\)&l=en](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2019/2651(DEA)&l=en). The objection took place after the time period for raising objections was renewed, see Decision to extend the time-limit for raising objections to a delegated act, ‘I/A’ ITEM NOTE, 8169/19, TRANS 257 DELACT 110 see here: <https://data.consilium.europa.eu/doc/document/ST-8169-2019-INIT/en/pdf>.

¹⁹ ITS Directive, Art. 14 (3).

²⁰ Consolidated version of the Treaty on the Functioning of the European Union, OJ 115/0172 (‘TFEU’), Art. 290.

²¹ This is an obligation set forth in the ITS Directive, Art. 14 (3).

²² See the note from the General Secretariat of the Council of 19 June 2018, 0292/18, available in the repository of the Council: <https://data.consilium.europa.eu/doc/document/ST-10292-2018-INIT/en/pdf>, last visited 28th August 2019.

on the 14th June 2019, but its content was not made public.²³ Yet, earlier documents from the European Parliament and the Council, as well as a large number of reports issued by large industry players' lobbying associations,²⁴ point to a few challenging issues.

Regarding the content of the proposal, several national delegations in the Council accused the drafters of the text for unduly exceeding the mandated conferred onto the Commission by the TFEU and the ITS Directive on several points (e.g. for creating and regulating new concepts such as the "C-ITS station operator" discussed below and for self-conferring upon itself extensive powers such as enforcement powers).²⁵ The criticism that garnered most attention concerns the technological choices made by the Commission regarding the telecommunications network, deemed to run against "technology-neutrality",²⁶ to the detriment of the upcoming 5G technology. The criticism essentially lies in the misalignment between EU electronic communications law – which refers to technology-neutrality as a regulatory objective – and the Proposed C-ITS Regulation. More broadly, questions have also touch upon the interface between electronic communications law and the ITS respective legal frameworks.²⁷

2.2. An introduction to the regulatory overlap in security regulation of C-ITS

The proposed C-ITS Regulation had interfaces with the NIS Directive, in that it regulated the security of C-ITS communications and environment. In an "open network that enables a many-to-many or peer-to-peer relationship between C-ITS stations", all C-ITS stations within the meaning of the proposed Regulation need to "securely exchange messages with each other" precisely because they are not "limited to exchanging messages with (a single) pre-defined station(s)".²⁸ In this context, the Proposed C-ITS Regulation aimed to ensure "the authenticity and integrity of C-ITS messages containing information, such as position, velocity and heading".²⁹ "The level of security and trust should be the same for all C-ITS Stations",³⁰ which derives directly from the peer-to-peer characteristic of C-ITS

²³ Opinion of the Legal Service to the Working Party on Transport - Intermodal Questions and Networks on the Commission Delegated Regulation (EU) .../... of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems, 10357/19, available in the repository of the Council: <https://data.consilium.europa.eu/doc/document/ST-10357-2019-INIT/en/pdf>, last visited 28th August 2019.

²⁴ See the large amount of feedback received by the Commission during the phase of the consultation phase, see here: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-2592333/feedback_en?p_id=351850, last visited 28th August 2019.

²⁵ See for instance the position of Finland, document 8213/19 in the repository of the Council, available here: <https://data.consilium.europa.eu/doc/document/ST-8213-2019-INIT/en/pdf>, last visited 28th August 2019.

²⁶ Among others, the lobbying association representing telecom operators (GSMA) was especially loud, see the "GSMA letter to the European Parliament on Delegated Act C-ITS" issued on the 9th of April 2019 and available on their website: <https://www.gsma.com/gsmadeurope/news/gsma-letter-to-the-ep-on-delegated-act-c-its/>, last visited 28th August 2019.

²⁷ In an earlier blog post of April 2019, "Legal principles behind technical complexities: the proposal from the Commission for a C-ITS Delegated Regulation", the author concluded that no *legal* principle of technology-neutrality is applicable in this context. It suggests that legal scrutiny should rather be focused on two other related principles, without prejudice to other legal issues related to the proposal. First, this of non-discrimination which constitutes a general principle of EU law and, second, this of consistency set forth in Article 7 TFEU. The blog post is available here: <https://www.law.kuleuven.be/citip/blog/legal-principles-behind-technical-complexities-the-proposal-from-the-commission-for-a-c-its-delegated-regulation/>, last visited 28th August 2019. The obligation to respect "coherence" and therefore to "take into account existing Union rules, policies and activities which are relevant in the field of ITS, in particular in the field of standardisation" is also included in the body of the ITS Directive, Annex II.

²⁸ Proposed C-ITS Regulation, Rec. 2.

²⁹ Proposed C-ITS Regulation, Rec. 17.

³⁰ Proposed C-ITS Regulation, Rec. 15.

communications. In this context, the entirety of the provisions laid down in the Proposed C-ITS Regulation were somehow aiming for the security of the C-ITS network.

The NIS Directive “lays down measures with a view to achieving a high common level of security of network and information systems within the Union”.³¹ Security of network and information systems is defined as “the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems”.³² The NIS Directive applies to two categories of entities: digital service providers³³ and operators of essential services.³⁴ Unlike digital service providers, bound by the NIS Directive regime upon sole transposition of the Directive in national law, essential services are only covered by the scope of the NIS Directive regime upon their designation as such by the respective Member States.³⁵ Essential services are services which cumulatively pass a three-criteria test. They “have to be considered as essential for the maintenance of critical societal and economic activities”. They are “dependent upon information and network systems” and “an incident would have significant disruptive effects on the provision of that service”.³⁶ Annex II of the Directive provides for the scope *rationae materiae* with a list of sectors and sub-sectors.

Concerning the transport sector, particularly road transport, Annex II of the NIS Directive includes “road authorities [...] responsible for traffic management control” and “Operators of Intelligent Transport Systems [as referred to in the ITS Directive]”. Intelligent Transport Systems (ITS) are described in the ITS Directive as “systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport”.³⁷ Within the meaning of the NIS Directive, ITS seems to meet the criteria for being an essential service(s). As a specific category of ITS, C-ITS are in principle subject to the NIS Directive. They are even particularly security-sensitive because of their peer-to-peer character. It means that operators active in the field of C-ITS could be potentially subject to security obligations arising from both the NIS Directive and the Proposed C-ITS Regulation, whenever the latter is formally adopted. The potential regulatory overlap begs several questions, such as how the two regimes would interact, whether operators should comply with both legal regimes, wholly or partly, or whether one legal framework should prevail and, if so, to what extent. The first draft of the proposed C-ITS regulation, issued by the European Commission in January 2019, simply overlooked these questions. A new Recital (6) was then included in the Proposed C-ITS Regulation issued by the European Commission in March 2019, with the purpose to clarify the interface with the NIS Directive. The recital sets forth that “as the NIS Directive listed operators of Intelligent Transport Systems as defined in paragraph 1 of Art. 4 of [the ITS Directive] as potential operators of essential services, the application of the NIS Directive and of the requirements imposed pursuant to the present Regulation *may be in certain cases complementary*” (emphasis added).³⁸ It is, however, unclear how to interpret this sentence. What does

³¹ NIS Directive, Art. 1 (1).

³² NIS Directive, Art. 4 (2).

³³ NIS Directive, Art. 4 (6).

³⁴ As defined in NIS Directive, Art. 4 (4).

³⁵ NIS Directive, Art. 4 (4) and 5 and Annex II.

³⁶ NIS Directive, Art. 5 (2).

³⁷ ITS Directive, Art. 4 (1).

³⁸ Proposed C-ITS Regulation, Rec. 6.

“complementary” concretely translate into in terms of legal obligations? Does it refer to concurrent application of both legal regimes or to the application of the (proposed) Regulation as a *lex specialis* to the NIS Directive and, if so, to what extent concretely? Besides, *what* are the services – and thus *who* are the operators - concerned? One would spontaneously think of the prominent figure of the “C-ITS Station operator” in the Proposed C-ITS Regulation, defined in the text as the person “responsible for the putting in service and the operation of C-ITS stations in according with the Regulation”.³⁹

On its side, the NIS Directive regulates interfaces with other legal frameworks as follows. Provisions of a sector-specific EU legal act which requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents should take precedence, provided such requirements are at least equivalent in effect to the obligations laid down in the NIS Directive.⁴⁰ Recital 9 further clarifies that, in such a case, Member States should “apply the provisions of such sector-specific Union legal acts, including those relating to jurisdiction, *and should not carry out the identification process for operators of essential services as defined by the [NIS] Directive*. In this context, Member States should provide information to the Commission on the application of such *lex specialis* provisions” (emphasis added). In other words, the NIS Directive describes itself as a minimum security legal standard *lex generalis*. In this context, how to assess whether the “requirements [e.g. of the proposed Regulation] are at least equivalent in effect to the obligations laid down in [the NIS] Directive”? What is then the ensuing security-related legal regime and for which operators?

3. The legal regimes imposing security obligations in the field of C-ITS

3.1. NIS Directive regulating providers of essential services

The NIS Directive lays down security obligations incumbent on operators of essential services, such as operators of ITS, upon their identification and subject to national transposition.

First, providers of essential services shall “take appropriate and proportionate technical or organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed”.⁴¹ Risk is defined as “any reasonable identifiable circumstance or event having a potential adverse effect on the security of network and information systems”.⁴² In addition to the risk management obligation, operators of essential services shall also “take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services”. An “incident” is defined broadly as encompassing “any event having an actual adverse effect on the security of network and information systems”.⁴³

Secondly, the operators shall “notify, without undue delay, the competent authority or the CSIRT [computer security incident response teams] of incidents having a *significant impact* on the continuity

³⁹ Proposed C-ITS Regulation, Art. 2 (16).

⁴⁰ NIS Directive, Art. 1 (7).

⁴¹ NIS Directive, Art. 14 (1).

⁴² NIS Directive, Art. 4 (9).

⁴³ NIS Directive, Art. 4 (7).

of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident” (emphasis added).⁴⁴ The NIS Directive is the first EU legal instrument focusing on incident notification and information sharing as core requirements, based on research showing the criticality of such information for cyber defense.⁴⁵ Incident notification is viewed as a form of cooperation between private and public entities.⁴⁶ Information concerning incidents from operators are useful for national public authorities to investigate and respond to such events, but also for other Member States to tackle security incidents when they have a cross-border effect.⁴⁷ Subsequently, the shared information are further processed within the CSIRTs network (the EU network of national CSIRTs) to “promote swift and effective operational cooperation”.⁴⁸ Finally, same information are spread to the general public and business, in an aggregated and anonymised manner.⁴⁹ All in all, security information and especially incident information notified by providers are considered precious input to respond incidents and to raise awareness and preparedness to further security incidents.

Finally, the NIS Directive regulates enforcement and regulatory monitoring of operators of essential services. The operators shall provide the competent authorities, upon prior request stating its purpose and which information is required, with “the information necessary to assess the security of their network and information systems, including documented security policies” on the one hand and “evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority [...]”, on the other.⁵⁰ In this context, the operators of essential services may be subjected to further-reaching security obligations issued by national authorities. Indeed, national authorities, taking into account the results of security audits, can carry out for security purposes might issue “binding instructions [...] to remedy the deficiencies identified”.⁵¹

While the field of ITS is covered by the NIS Directive, *who* is concretely concerned in the specific case of C-ITS remains quite unclear.

3.2. Who is the “Operator of (Cooperative) Intelligent Transport Systems”?

To understand the interplay between the NIS Directive regime and the proposed C-ITS Regulation, their respective personal scope of application (*rationae personae*) need to be clearly identified.

The NIS Directive refers to Art. 4 (1) ITS Directive for the purpose of defining “operators of Intelligent Transport Systems” as potential operators of essential services. Such provision does however not identify *categories of operators*, but defines Intelligent Transport Systems (ITS). The Communication from the European Commission “Making the Most of NIS”,⁵² aimed to clarify the NIS Directive,

⁴⁴ NIS Directive, Art. 14 (3).

⁴⁵ Giuseppe Settanni and al., ‘A Collaborative Cyber Incident Management System for European Interconnected Critical Infrastructures - ScienceDirect’ (2017) 34 Journal of Information Security and Applications 166, 166–167.

⁴⁶ NIS Directive, Rec. 35.

⁴⁷ NIS Directive, Art. 14 (5).

⁴⁸ NIS Directive, Art. 12 (1).

⁴⁹ NIS Directive, Rec. 40.

⁵⁰ NIS Directive, Art. 15 (2).

⁵¹ NIS Directive, Art. 15 (3). For a more thorough explanation of the legal regime applicable to the operators of essential services in the NIS Directive, and particularly on the institutional landscape that is set up, see Markopoulou, Papakonstantinou and de Hert (n 18).

⁵² Communication from the European Commission to the European Parliament and the Council, Making the most of NIS – Towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM/2017/0476 final, 4.10.2017.

observes that “for most of the entities which belong to the ‘traditional sectors’ EU legislation contains well developed definitions to which Annex II makes a reference”,⁵³ such as in the rail transport where “infrastructure managers” and “railway undertakings” are referred to with a link to their legal definition as part of EU legal order.⁵⁴ Yet, this is not true for ITS, where the reference to ITS legislation relates to technological applications (“ITS”) and not to legally-defined entities or functions. On the NIS “side”, neither the Directive nor the Communication “Making the Most of NIS” provide further explanation in this regard.

On the side of ITS legislation, the ITS Directive does also not define or refer to *operators* of ITS (services). The ITS Directive rather refers to the “*ITS service provider*” in what could be called a ‘waterfall definition’. The ITS service provider is defined as “any provider of an ITS service, whether public or private”.⁵⁵ In turn, an ITS service is “*the provision of an ITS application* through a well-defined organisational and operational framework to contribute to user safety, efficiency, comfort and/or to facilitate or support transport and travel operations” (emphasis added).⁵⁶ Finally, an “ITS application” is defined as an “operational instrument for the application of ITS”.⁵⁷

Against this background, it remains unclear whether - and to what extent - the “operator of ITS” within the meaning of the NIS Directive should be read as referring to the same as “ITS service provider” within the meaning of the ITS Directive. Should both terms be read as equivalent? Would one encompass (and be thus broader than) the other? No answer has been provided thus far. This question could seem purely theoretical regarding ITS in general, as both the NIS Directive and the ITS Directives require further measures either at the national level, which could thus bring additional clarity and legal consistency, where appropriate. Yet, it may be different with C-ITS, subject to an EU proposed Regulation (and potential new legal instrument in the near future). Then, does the proposed Regulation bring clarity as for which entities should be deemed as “operators of ITS” within the meaning of the NIS Directive?

Based on the ITS Directive, the Proposed C-ITS Regulation partly adopts its vocabulary. Like the ITS Directive and contrary to the NIS Directive, it does not refer to “operator of ITS”. It does refer to “C-ITS service” like the ITS Directive as “an ITS service provided through C-ITS”⁵⁸ or in other words as a specific kind of ITS service. C-ITS - or Cooperative Intelligent Transport Systems - are defined in the proposed Regulation as “intelligent transport systems that enable ITS users to cooperate by exchanging secured and trusted messages using the EU C-ITS security credential management system”.⁵⁹ C-ITS is defined not only as a specific kind of ITS; it also implies the integration within the EU-centred system. Yet and although the term “service provider” is used in broad terms throughout the Proposed C-ITS Regulation, the latter does neither define nor regulate a ‘C-ITS service provider’. In turn, great emphasis is placed on the “C-ITS station” and on the “C-ITS station operator”. A C-ITS station is defined as “the set of hardware and software components required to collect, store, process, receive and transmit secured and trusted messages *in order to enable the provision of a C-ITS service [...]*” and

⁵³ Annex to the Communication from the Commission to the European Parliament and to the Council, Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, Section 4.1.1.

⁵⁴ NIS Directive, Annex II (2) (b).

⁵⁵ ITS Directive, Art. 4 (5).

⁵⁶ ITS Directive, Art. 4 (4).

⁵⁷ ITS Directive, Art. 4 (3).

⁵⁸ Proposed C-ITS Regulation, Art. 2 (2).

⁵⁹ Proposed C-ITS Regulation, Art. 2 (1).

is therefore instrumental to the provision of the latter. It can consist of “personal, central, vehicle and roadside ITS stations [...]”.⁶⁰ The C-ITS station operator is defined as “any natural or legal person who is responsible for the putting in service and the operation of C-ITS stations in accordance with this Regulation”.⁶¹ The notion should be distinguished from the role of “manufacturer” who “designs and manufactures a C-ITS station or has a C-ITS station designed or manufactured, and markets that C-ITS station under his name or trademark”.⁶² It should also be distinguished from the C-ITS station “owner” referred to in Art. 22 (3) of the proposed Regulation.

Although it would seem intuitively quite *logical* to consider the C-ITS station operator as an “operator of ITS” within the meaning of the NIS Directive, the Proposed C-ITS Regulation does not provide a *legal* answer to this question. A similar consistency issue can also be observed between the C-ITS station operator in the proposed Regulation and the “ITS service provider” in the ITS Directive. Given the instrumental definition of C-ITS station as a means to provide C-ITS services, a C-ITS station could be viewed as a sub-category (namely, a specific “operational instrument”) of “ITS application” within the meaning of the ITS Directive. As a result, “C-ITS station operator” would constitute a sub-category, for the purpose of C-ITS, of “ITS service provider”, within the meaning of the ITS Directive. Such reasoning could bring some clarity to the relationship between the ITS Directive and the Proposed C-ITS Regulation. However, it does not bring clarity and consistency as of the terminology between the Proposed C-ITS Regulation and the NIS Directive.

At this stage of the legal analysis, two intermediary conclusions can be drawn. First, the provisions of the NIS Directive are not clear on its personal scope of application (*rationae personae*) in the field of ITS, and particularly the cross-referencing to the ITS Directive. Secondly, the personal scope of the Proposed C-ITS Regulation seems, in turn, to overlook the need for consistency with other legislative frameworks, notably the ITS Directive and the NIS Directive, which results in legal uncertainty. This overall lack of clarity also detracts from the fact that the technology is not yet deployed in the market and the ecosystem is yet to be set up. The peer-to-peer character of C-ITS communications further blurs the situation. Further research would be welcome to analyse the inconsistency in the terminology between the legal frameworks in the face of the principle of consistency set forth in primary law.⁶³ The first recommendation which can be drawn at this point is that the potential future new C-ITS regulation should bring clarity in this regard.

The remainder of this paper assumes that the C-ITS station operator *is* the (or at least *a*) relevant operator of ITS in the C-ITS environment, for further studying the interplay between the proposed C-ITS Regulation and the NIS Directive. How, then, does the Proposed C-ITS Regulation deal with the security obligations of the C-ITS station operator?

⁶⁰ Proposed C-ITS Regulation, Art. 2 (3).

⁶¹ Proposed C-ITS Regulation, Art. 2 (16).

⁶² Proposed C-ITS Regulation, Art. 2 (15).

⁶³ Consolidated version of the Treaty on the Functioning of the European Union (TFEU), OJ C 326/47, Art. 7, which reads: “The Union shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers”.

3.3. Security obligations related to C-ITS Station Operators in the proposed Regulation

The Proposed C-ITS Regulation is all about bringing trust and security for C-ITS communications, to the extent that an entire chapter (Chapter V) is dedicated to “security”. As stated by the European Commission in the Explanatory Memorandum of the Proposed Regulation, “C-ITS are a category of ITS services, based on an *open network* that enables a *many-to-many* or *peer-to-peer* relationship between C-ITS stations”.⁶⁴ In this context, one of the objectives of the Proposed Regulation is to “ensure the authenticity and integrity of messages exchanged between C-ITS stations, in order to assess the trustworthiness of such information (see also in recital 17).”⁶⁵ The present sub-section outlines the security provisions of the Proposed C-ITS Regulation, with a focus on the C-ITS station operator.

According to the Proposed C-ITS Regulation, C-ITS station operators shall “ensure that all their C-ITS stations are put in service and operated in accordance with [the Regulation]”.⁶⁶ They should especially check that “the C-ITS station is certified [...]” and before it is put in service, that it is “enrol[led] in the EU C-ITS security credential management system [...]”. To do so, the C-ITS station shall be “registered in a C-ITS station register of its enrolment authority together with the identification of its operator [...]”. The C-ITS station operators are then responsible for ensuring that the C-ITS stations, while in use, comply with the technical requirements set forth by the Proposed Regulation. In addition to technical standards, it especially implies what could be called ‘must carry’ obligations with regard to the C-ITS priority services listed in Annex I of the Proposed Regulation as well as compatibility obligations.⁶⁷

The Proposed C-ITS Regulation also lays down *security* obligations incumbent on the C-ITS station operators. In essence, they shall set up an information security management system (ISMS)⁶⁸ in compliance with the C-ITS security policy enshrined in Annex IV of the Proposed Regulation. They are also made responsible for ensuring that the C-ITS stations are certified in compliance with the Proposed Regulation⁶⁹ and that they remain in compliance with it throughout their use.

Finally, the whole “EU C-ITS security credential management system” to be put in place by the Proposed C-ITS Regulation, should it have been enacted, and to which the C-ITS station operator should take part, can be viewed as amounting to security measures. It is defined as “the European Union C-ITS framework for the provision of trusted and secure communication using a public key infrastructure (PKI)”,⁷⁰ and it is planned to be set up “for the provision of trusted and secure communication between C-ITS stations”.⁷¹ All C-ITS stations shall be enrolled in and comply with the system, subject to technical and security requirements laid down in the annexes of the proposed Regulation.⁷² The system itself shall comply with technical security requirements, namely the certificate policy setting out “the requirements for the management of publickey certificates for C-ITS services by issuing entities and their usage by end-entities” on the one hand, and the “security policy” setting out “the requirements

⁶⁴ Proposed C-ITS Regulation, Explanatory Memorandum, 1.

⁶⁵ Proposed C-ITS Regulation, Explanatory Memorandum, 3.

⁶⁶ Proposed C-ITS Regulation, Art. 22 (1).

⁶⁷ Proposed C-ITS Regulation, Art. 5 and 22.

⁶⁸ Proposed C-ITS Regulation, Art. 27 “Information security management system”.

⁶⁹ Proposed C-ITS Regulation, Art. 22 (2).

⁷⁰ Proposed C-ITS Regulation, Art. 2 (27).

⁷¹ Proposed C-ITS Regulation, Art. 23 (1).

⁷² Proposed C-ITS Regulation, Art. 23 (3).

for the management of information security in C-ITS” on the other.⁷³ In this regard, the Proposed C-ITS Regulation plans to create new categories of centralised players in the C-ITS ecosystem in charge of security-related activities. The “C-ITS certificate policy authority” would be responsible for “managing the certificate policy and the PKI authorization [...]”.⁷⁴ The “trust list manager” would be responsible for “generating and updating the European Certificate Trust List (ECTL)”.⁷⁵ Finally the “C-ITS point of contact” would be responsible for “handling all communication with root certification authority managers and publishing the public key certificate of the trust list manager and the ECTL [...]”.⁷⁶ These centralised activities are considered necessary for the governance and the security of C-ITS communications within the C-ITS network. The whole regime is referred to as “one common European C-ITS trust model”, applicable to all C-ITS stations.⁷⁷ In the preparatory phase of the Proposed Regulation and notably as part of the work conducted in the C-ITS platform created by the European Commission,⁷⁸ the need for centralised *governance* bodies was also identified for the common European C-ITS trust model.⁷⁹ As part of the “implementation of the C-ITS network” – consisting of “all operational C-ITS stations in the EU”⁸⁰ – the Proposed Regulation therefore contemplates “governance tasks”, such as preparation of the “updates to the C-ITS governance framework”, and “supervision tasks”, such as the supervision of security incidents management.⁸¹ “Pending the establishment of central entities”, the Proposed Regulation (controversially) proposed to appoint the European Commission to be in charge of these tasks.⁸²

The section outlined the security obligations respectively set forth in the NIS Directive and in the Proposed C-ITS Regulation. The figure of the C-ITS Station Operator in the Proposed Regulation was also introduced as the core debtor of security obligations and potentially subject simultaneously to the two legal frameworks. Against this backdrop, it remains to be seen how both legal frameworks interact, and in particular how the *lex specialis* rule the NIS Directive (Art. 1 (7)) applies in such situation.

4. NIS vs. C-ITS? Towards an interpretation of Article 1 (7) of the NIS Directive

This section discusses the interpretation of Art. 1 (7) NIS Directive governing the interface and interplay with other EU legal frameworks imposing security obligations, with the Proposed C-ITS Regulation as a practical case study. By going into the detailed provisions of the NIS Directive, the first sub-section reveals a number of interpretation questions. The second sub-section confronts the *lex specialis* rule the NIS Directive with the Proposed C-ITS Regulation, in order to determine the applicable security-related legal regime for C-ITS station operators.

⁷³ Proposed C-ITS Regulation, Art. 23 (2).

⁷⁴ Proposed C-ITS Regulation, Art. 24 (1).

⁷⁵ Proposed C-ITS Regulation, Art. 25 (1).

⁷⁶ Proposed C-ITS Regulation, Art. 26 (1).

⁷⁷ See for instance Proposed C-ITS Regulation, Rec. (17).

⁷⁸ The documents issued by the C-ITS Platform are available here: https://ec.europa.eu/transport/themes/its/c-its_en (last visited 3rd September 2019).

⁷⁹ Proposed C-ITS Regulation, Rec. 27.

⁸⁰ Proposed C-ITS Regulation, Art. 2 (29).

⁸¹ Proposed C-ITS Regulation, Art. 29.

⁸² Proposed C-ITS Regulation, Rec. (22), Art. 24 (2), 25 (2) and 26 (2). This self-conferral of power from and to the European Commission was blamed by some national delegations in the Council for exceeding the mandate of the Commission. It makes part of the legal questions asked by the General Secretariat of the Council to its legal department (see 15 above).

4.1. The not-as-straightforward-as-it-seems Article 1 (7) NIS Directive

The interactions between the NIS Directive and other EU legal frameworks imposing security obligations are regulated by Art. 1 (7) NIS Directive, which shall be read together with other related provisions of the Directive and in particular with the related recitals. Barely discussed in the legal scholarship, such provisions were discussed by the European Commission in its Communication ‘Making the Most of NIS’. As a reminder, Art. 1 (7) NIS Directive reads: “Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply”. Next to Art. 1 (7), the NIS Directive also contains a specific provision for the electronic communications sector undertakings and for trust service providers (Art. 1 (3)). They are excluded from the scope of the NIS Directive for they are respectively subject to sector-specific EU legal regimes. Not only does Art. 1 (3) target *specific* sectors and types of operators, as opposed to Art. 1 (7) which is more of a ‘catch-all’ provision. Contrary to the latter, Art. 1 (3) does not require further analysis: the exception is operationalised by the NIS Directive itself, throughout the whole EU.

Art. 1 (7) is supplemented with recitals 9 to 14 of the Directive. Recital 9 states that it is up to Member States to provide information to the European Commission on the application of [...] EU sector-specific *lex specialis* provisions. Should the *lex specialis* provisions prevail, the NIS Directive does consequently *not apply, including the process of identification of the operators of essential services*. Recital 9 further clarifies that, in doing the gap analysis between the NIS Directive and the provisions of EU sector-specific Union legal act, regard should only be had to these provisions and “their application in the Member States”. Recitals 10 and 11 discuss the water transport sector; Recitals 12 to 14 then discuss the banking and financial market infrastructure sectors, having been respectively subject to security obligations with regard to network and information systems as part of sector-specific EU legislation. No other EU sector-specific legislation is discussed in the NIS Directive itself. The Recitals do not provide clear-cut answers, whether such EU sector-specific legislations should be considered as *lex specialis* and therefore whether – and if so to what extent - they should prevail over the NIS Directive provisions. For instance, Recital 10 seems to tip in favour of a positive answer but remains yet equivocal: “In the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations [...]. Part of the mandatory procedures to be followed includes the reporting of all incidents *and should therefore be considered as lex specialis, in so far as those requirements are at least equivalent to the corresponding provisions* of [the NIS] Directive” (emphasis added). The same can be said of the banking and financial market infrastructures sectors. Recitals 12 to 14 provide a catalogue of security- and incident notification-relevant provisions, which again seem to tip in favour of an application of Article 1 (7). Yet, they do not provide a conclusive answer.

The Communication ‘Making the Most of NIS’ includes a section on “the relationship between the NIS Directive and other legislation”. Although the interpretation of EU legislation provided by the European Commission in communications, guidelines and other *soft law* documents has no legally binding value,

it does often have a strong impact.⁸³ In the Communication, the European Commission conducts its analysis of the application of Article 1 (7) to the banking and financial market sectors and appears to be slightly more assertive than the NIS Directive.

The analysis of the European Commission covers three categories of entities: Credit institutions with regard to the provision of payment services, financial market infrastructure (especially central counterparties or 'CCPs') and trading venues in financial instruments markets. The European Commission concludes that the Payment Service Directive 2 (PSD2)⁸⁴ should be considered as a *lex specialis* to the NIS Directive with regard to the provision of payment services by credit institutions and should, therefore "apply instead of the corresponding provisions of Article 14 of the NIS Directive". Regarding central CCPs, the European Commission concludes that sector-specific EU legislation "contains provisions on security requirements [...] which can be regarded as *lex specialis*." The European Commission therein notes that "the legal acts provide for technical and organisation measures related to the security of network and information systems *which in terms of detail* go even beyond the requirements of Article 14 (1) and (2) NIS Directive and *therefore can be regarded as fulfilling the requirements of Article 1 (7) of the NIS Directive as far as the security requirements are concerned*" (emphasis added). Contrary to the case of credit institutions (above), *no mention is made of notification requirements*, be it with regard to the sector-specific legislation or with regard to the ensuing applicability of related provisions in the NIS Directive.⁸⁵ Similarly, the European Commission concludes that EU sector-specific legislation "contain[...] security obligations that are in effect at least equivalent to the corresponding obligations of Article 14 (1) and (2) NIS Directive", with regard to trading venues. No mention is made of notification requirements either. *No conclusion is drawn* either as for the ensuing applicable legal regime on notification, but also more generally on *the applicable legal regime* altogether. Although the water transport sector is touched upon in recitals of the NIS Directive, the Communication surprisingly does not even mention it. With regard to other sectors, the Communication only clarifies that [at the time of writing], "there is no sector-specific legislation for the category of the digital service providers that provides for security and notification requirements comparable to those laid down in Article 16 NIS Directive that can be considered in the applicability of Article 1 (7) NIS Directive", while clarifying in footnote that "this is without prejudice to the Notification of a personal data breach to the supervisory authority covered by Article 33 GDPR".⁸⁶ No other sector is discussed for the sake of interpreting Article 1 (7) NIS Directive.

Generally speaking, the Communication is not prolific in clarifying the methodology to be followed in interpreting Article 1 (7) NIS Directive. It merely states that "as far as notification requirements are concerned, special attention needs to be paid to the obligations of the operator [...] to include in the notification information enabling the competent authority or the CSIRT to determine any cross-border impact of a security incident". Such mention seems paradoxical as the European Commission itself does not discuss notification obligations in its analysis of the EU sector-specific legislation of the

⁸³ Corina Andone and Sara Greco, 'Evading the Burden of Proof in European Union Soft Law Instruments: The Case of Commission Recommendations' (2018) 31 International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique 79.

⁸⁴ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337/35.

⁸⁵ NIS Directive, Art. 14 (3).

⁸⁶ European Commission, Making the Most of NIS, 37.

banking and financial market infrastructure sector, except for the credit institutions (where the European Commission takes into account the cross-border impact of security incidents notification).

While Recital (9) NIS Directive considers the “application in the Member States” of the NIS Directive provisions to make part of the comparison exercise, such provision cannot be found in the body of the text. In particular, Art. 1 (7) NIS Directive does not mention national transposition or implementation, although the need to evaluate the respective legal frameworks “in effect” could somehow suggest to look at national implementation. In its Communication ‘Making the Most of NIS’, the European Commission holds that “Member States need to consider Article 1 (7) in the overall transposition of the Directive”. Yet, when conducting its own assessment regarding banking and financial market respective EU sector-specific legislation, the European Commission does *not* take into consideration any national provisions implementing the NIS Directive. The assessment is limited to a comparison of EU legal frameworks, which does not prevent the European Commission from drawing conclusions as for the application of the *lex specialis* rule. Against this backdrop, the remainder of this paper compares the Proposed C-ITS Regulation and the NIS Directive, within the meaning of Art. 1 (7) NIS Directive, notwithstanding national implementations of the NIS Directive with respect to ‘Operators of C-ITS’.⁸⁷

The following sub-section applies Article 1 (7) NIS Directive to the interface with the Proposed C-ITS Regulation, with specific focus on the legal regime applicable to the C-ITS station operator.

4.2.C-ITS as a case study to understand Article 1 (7) of the NIS Directive

The Proposed C-ITS Regulation is analysed in this sub-section as a practical case study for the analysis of Article 1 (7) NIS Directive. The analysis focuses on a few identified issues: First, the lack of a uniform terminology in both legal instruments and the ensuing difficulty to identify what provisions have to be compared, with a focus on the scope *rationae materiae*. Second, the analysis shows an internal inconsistency in the NIS Directive, which results in legal uncertainty when a EU sector-specific legislation is found to qualify as *lex specialis*. The third sub-section discusses criteria guiding the comparison of both legal frameworks so as to avoid engaging into arbitrary discussion on their respective merits.

4.2.1. The scope *rationae materiae* and the lack of a uniform terminology

First, the material scope (*rationae materiae*) of security obligations in respectively both legal frameworks could seem *prima facie* to be different. According to the NIS Directive, the Member States “shall ensure that operators of essential services take [...] measures to manage the risks posed to the security of network and information systems which they use in their operations”.⁸⁸ On the other hand, Annex IV of the proposed Regulation dedicated to security refers only to “information security” with regard to the mandatory establishment of the CSMS of the C-ITS station operators.⁸⁹ Information

⁸⁷ In its Report to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23 (1) of Directive 2016/1148/EU on security of network and information systems, COM/2019/546 final, the European Commission barely mentions road transport and does not refer at all to (C-)ITS. This should come at no surprise as C-ITS is yet to be developed and commercialised on the market.

⁸⁸ NIS Directive, Article 14 (1).

⁸⁹ Proposed C-ITS Regulation, Annex IV, Point 1.3.

security is defined as the “preservation of the confidentiality, integrity and availability of information (ISO 27000)”.⁹⁰ Information security does thus *not* include “device or group of interconnected devices, one or more of which, pursuant to a program perform automatic processing of digital data” which are components of “network and information systems” within the meaning of the NIS Directive,⁹¹ and could therefore seem to be narrower in scope. The lack of a consistent terminology with reference to security in the digital environment was already underlined and associated with a lack of consistent conceptual framework, in particular the references to both “information security” and “security of network and information systems” (in addition to “cybersecurity” being also commonly referred to).⁹²

Notwithstanding, a closer look at the *substantive content* of security obligations suggests that the Proposed C-ITS Regulation deals with more than information security and also somehow encompasses network and information systems. Annex IV of the Proposed Regulation includes, as part of the risk identification, the category of “supporting assets, including [...] C-ITS stations and their software, configuration data and associated communication channels; central C-ITS control assets; every entity within the EU CCMS”. As a result, threats to these assets and their sources should be identified and managed. Vulnerabilities which could be exploited to harm assets but also the other C-ITS stakeholders should also be identified and further managed.⁹³ C-ITS stations are also subject to technical regulation and prior certification and registration to the CCMS with the purpose to ensure their security before they can be used to exchange C-ITS communications. All in all, the security obligations in the Proposed Regulation seem to extend well beyond sole information security *strictu sensu*. Quite on the contrary, the scope of security management obligations can be viewed as particularly broad, in that it even covers risks to third parties, namely to other C-ITS stakeholders. In the parlance of Kasper and Antonov, the scope of security requirements in the Proposed C-ITS Regulation can be said to cover “interconnected information systems”, in this case to the C-ITS network.⁹⁴ Whether it can consequently be concluded that the respective scopes *rationae materiae* of the legal regimes would be *aligned* remains, however, very unclear. The lack of uniformity in the terminology and the higher technicality of the provisions of the Proposed C-ITS Regulation therein appear to play a significant and detrimental role.

As the scope of the Proposed C-ITS Regulation reaches beyond security, a similar question arises regarding *which provisions* should be considered relevant for the gap analysis between the two legal instruments. In other words, which of the provisions of the proposed C-ITS Regulation shall be considered as related to the security of network and information systems? For instance, the C-ITS stations are subject to harmonised technical requirements or conformity assessment procedure,⁹⁵ which may *not be expressly labelled* as ‘security’ provisions in the text but which are generally aimed at contributing to the overall security of C-ITS communications within the C-ITS network. Similarly, one may wonder about including “supervisory tasks”, namely the supervision of “the management of large-scale and high-severity security incidents that impact the entire C-ITS network (including disaster recovery situations where the cryptographic algorithm is compromised)”. According to the Proposed Regulation, these tasks would be conducted by the European Commission in the short term,⁹⁶ and

⁹⁰ Proposed C-ITS Regulation, Annex IV, Point 1.2.

⁹¹ NIS Directive, Art. 4 (1).

⁹² Kasper and Antonov (n 11) 12.

⁹³ Proposed C-ITS Regulation, Annex IV, Point 1.5.2.1.

⁹⁴ Kasper and Antonov (n 11) 21.

⁹⁵ Proposed C-ITS Regulation, Art. 5 and Annex V.

⁹⁶ Proposed C-ITS Regulation, Art. 29 (1) (b).

anyway by central authorities in the long run, rather than by the C-ITS station operators. These tasks are yet undoubtedly aimed at *securing* the C-ITS network, and the C-ITS station operators should comply with the overall governance regime. It would therefore seem more *logical* to include them in the provisions subject to the gap analysis, although no *legal* clear-cut stance can be taken.

All in all, the lack of uniformity in the vocabulary generally hinders the conduct of the gap analysis. Yet again, the legislator of a future C-ITS regulation would better anticipate such issue.

4.2.2. Security vs. notification obligations: The NIS Directive's internal inconsistency

Another challenge can be found in the level of granularity to evaluate whether the Proposed C-ITS Regulation could qualify as *lex specialis vis-à-vis* the NIS Directive provisions with respect to the C-ITS stations operators, and to conclude on the applicable legal regime.

The wording of Article 1 (7) NIS Directive suggests that the “security requirements” on the one hand and the “incident notification” obligations on the other, should be evaluated separately. As a result, “those provisions of that sector-specific Union legal act shall apply”, which suggests that the *remaining* NIS Directive provisions would still be applicable. Both legal frameworks would therefore apply concurrently and complementarily. Concretely, where security obligations of EU sector-specific legislation would apply *in lieu of* NIS security provisions (a), remaining NIS *notifications obligations* would still be applicable (b), should there no be “at least equivalent” notification obligations in the EU sector-specific legislation.

Such interpretation is supported by the history of the provision. Not included in the original proposal from the European Commission for a directive,⁹⁷ the *lex specialis* rule of Article 1 (7) NIS Directive was introduced in the text during the phase of interinstitutional discussions between the European Parliament and the Council. The provision was barely modified throughout the institutional discussions, except for the last part, which read as follows, when first introduced: “[...] those provisions of that sector specific Union legal act shall apply *instead the corresponding provisions of this Directive*” (emphasis added to highlight the modified part).⁹⁸ The last part of the proposed provision was clear in that *only* the “corresponding provisions” of the NIS Directive would be dismissed by the application of *lex specialis* provisions in the EU sector-specific provisions. The *remaining* provisions in the NIS Directive (e.g. incident notification obligations) were logically meant to remain applicable.

However, Recital 9 of the NIS Directive *expressly supports a different interpretation*: “Whenever those Union legal acts contain provisions imposing requirements concerning the security [...] or notifications of incidents [...], Member States should then apply the provisions of such sector-specific Union legal acts, including those relating to jurisdiction, *and should not carry out the identification process for operators of essential services as defined by the Directive*” (emphasis added). Such recital was introduced in the draft directive (as Recital 10) *together with* the introduction of the *lex specialis* rule. Yet, identification phase is the *sine qua non* obligation for the application of the NIS Directive

⁹⁷ Proposal from the European Commission for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, /* COM/2013/048 final - 2013/0027 (COD) */.

⁹⁸ Approval in committee of the text agreed at 2nd reading interinstitutional negotiations, PE612.044 / PE612.045, 14/01/2016, Art. 1 (7) of the proposal.

obligations to the operators of essential services, whether security or notification obligations. As a result, the prevalence of, for instance, *security provisions* in sector-specific EU legislation would result in the concerned actors *not being identified* as operators of essential services in the first place and thus not subject to *any* NIS obligation, including *no notification obligation* at all. This finding sounds absurd given the ambit of the EU legislator to place the NIS Directive as a minimum security standard.

The Communication ‘Making the Most of NIS’ suggests some discomfort on behalf of the European Commission on that the legal regime applicable as a result of the application of Article 1 (7) NIS Directive. Having concluded that *both* security and notification obligations in sector-specific legislation shall be considered as *lex specialis* provisions for credit institutions, the European Commission does state that, consequently, such sector-specific provisions shall “apply instead of the corresponding provisions of Article 14 of the NIS Directive”. *On the contrary*, no conclusion was made by the European Commission as for the applicable legal regime of central CCPs and trading venues, where only security obligations were discussed (and not notification obligations). The Commission notes that security obligations can be “regarded as *lex specialis*” but *does not clarify the ensuing applicable* legal regime, in particular whether the NIS Directive’s notification obligation is applicable.

The very same questioning arises with the Proposed C-ITS Regulation, which sets forth security obligations *but no notification obligations*. Should the security obligations incumbent on the C-ITS station operator be deemed “at least equivalent” to the NIS Directive security obligations, would notification obligations laid down by the NIS Directive apply “complementarily” to them (as indicated in Recital 6 of the proposed Regulation)? Or, alternatively, would the NIS Directive regime be dropped altogether in favour of the exclusive application of the Proposed C-ITS Regulation? There is no clear answer to this conundrum. Should the Proposed C-ITS Regulation have been adopted, this issue would have been all the more acute that, as a regulation, it would have applied directly to the private actors without national transposition (direct effect). Quite illogically, this legal uncertainty would have had to be borne by the Member States, according to Recital 9 NIS Directive. Should a future C-ITS regulation be proposed, one can only advise to regulate this aspect.

4.2.3. Comparing apples and oranges?

Moving now to the *substance* of security obligations, this sub-section analyses the criterion(a) guiding the gap analysis between the two legal frameworks, within the meaning of Article 1 (7) NIS Directive.

One could first think of the level of detail of the legal provisions. What is indeed immediately visible from the above introduction of the respective security legal regimes, is that the Proposed C-ITS Regulation lays down *way more detailed* security provisions than the NIS Directive, especially with respect to the C-ITS station operators. A full and detailed Annex is dedicated to the “ISMI” in the Proposed C-ITS Regulation on the one hand, while on the other security obligations laid down in the NIS Directive could seem ‘vague’. Operators shall, for instance, take “appropriate and proportional” measures to manage the risks posed. Such measures shall ensure a level of security “appropriate to the risk posed”, as further discussed in section 3.3 above. In this context, when comparing both regimes within the meaning of Article 1 (7) NIS Directive, can the higher *level of details* of security provisions in the Proposed C-ITS Regulation be considered as relevant? In other words, would a higher level of details *per se* substantiate a higher level of security obligations – or a level “at least equivalent” in the parlance of the NIS Directive? The European Commission seems to be of that opinion. In its study of security requirements applying to central CCPs conducted in the Communication ‘Making the Most

of NIS', the European Commission took into account as a relevant factor the fact that sector-specific requirements go further than the NIS Directive provisions "in terms of detail".

The NIS Directive itself does not refer to the level of detail. It does more generally not clarify *which criteria* should be taken into account to conduct the analysis; Article 1(7) NIS Directive merely indicates that the gap analysis should regard the *effect* of the sector-specific legal provisions. Looking at the *effects* of the law seems to imply that making the gap analysis between the two legal frameworks within the meaning of Article 1 (7) NIS Directive would lie partly beyond a legal endeavour, by shifting the focus toward the practical consequences of the application of legal provisions. Yet, this issue remains entirely obscure, and the Communication from the Commission does not clarify it.

The level of details should not be considered *as such* as a relevant element. The reading of the Communication from the European Commission rather implicitly suggests that the level of details of financial sector-specific legislation provisions mirrors the *specificity* of security obligations to the context of the financial activities and actors in question. Such a finding is also in line with the general interpretation of the applicability of a *lex specialis* as opposed to this of a *lex generalis*. The "level of details" should not be confused with the *specificity* of the provisions, which the European Commission would seem to consider as a relevant criterion.

In our case, the different levels of details between the Proposed C-ITS Regulation and the NIS Directive seems to be related to another aspect, namely their different *regulatory approach*. It is therein debatable whether security provisions in the NIS Directive should be best labelled as 'vague' and whether this should be viewed as 'less stringent' than more detailed provisions at all. Recital 44 NIS Directive importantly clarifies that "responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services [...]. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices". From a regulatory perspective, these provisions could best be described as "principle-based", as opposed to "rule-based".⁹⁹ While rule-based regulation "prescribes or prohibits specific behaviours, principle-based regulation 'emphasises general and abstract guiding principles for desired regulatory outcomes'".¹⁰⁰ While a rule-based approach to security could have resulted, for instance in a detailed list of mandatory preventive actions, the NIS Directive lays down general obligations of "risk management". The merit of this regulatory approach is to allow for flexibility, deliberately viewed here as a means to counteract dynamic cyber threats. By doing so, the NIS Directive 'responsibilizes' the regulated entities, who can and shall design their internal regulation. One could argue that the 'vagueness' of the NIS Directive provisions also partly detracts from the need for national transposition and implementation, which could lay down *more specific* and *more stringent* provisions (minimum harmonisation).¹⁰¹ While this is true, national transposition and implementation should however contradict neither the letter nor the spirit of the NIS Directive, and particularly its foundation in the responsabilisation of regulated entities. Such reasoning is confirmed

⁹⁹ Mark Fenwick, Wulf A Kaal and Erik PM Vermeulen, 'Regulation Tomorrow: Strategies for Regulating New Technologies' in Toshiyuki Kono, Mary Hiscock and Arie Reich (eds), *Transnational Commercial and Consumer Law: Current Trends in International Business Law* (Springer Singapore 2018).

¹⁰⁰ Charlotte Ducuing, Luca Oneto and Simone Petralli, 'Fairness and Accountability of Machine Learning Models in Railway Market: Are Applicable Railway Laws Up to Regulate Them?' (2018) 2 <<https://lirias.kuleuven.be/retrieve/526441>> accessed 24 September 2019. The authors therein quote Fenwick et al. (n 98).

¹⁰¹ NIS Directive, Art. 3.

by the fact that, for digital service providers, the NIS Directive provisions (together with the European Commission's implementing act), which lay down a similar regime to this applicable to operators of essential service providers,¹⁰² constitute 'maximum harmonisation'.¹⁰³

Against this backdrop, the NIS Directive regime can be qualified as mainly "individualistic", according to the categorisation of government risk management cultures of Hood and al.,¹⁰⁴ as further discussed by Renaud and al. in the field of (cyber)security and resilience regulation.¹⁰⁵ The categorisation is based on the respective roles of individuals and governments in the risk management process.¹⁰⁶ "Individualistic" hereby refers to the fact that the government "supports markets and underpins informed choice but responsibility is essentially the individual citizen's". Two main elements characterize such "responsibilisation": (a) "Individuals [are required] to take reasonable precautions thereby minimising their risk of becoming victims" and (b) "if they fail to take all the right precautions and fall victim, a certain degree of responsibility for the consequences rests with them".¹⁰⁷ By requesting regulated entities to identify the risks, to determine the acceptable level of security, to identify and take appropriate measures to manage the risks and mitigate the incidents, the NIS Directive undeniably "responsibilises" them, based on the assumption that they do have the expertise and are the best placed to take action.¹⁰⁸

As opposed to that, the anticipated (cyber-)security risk management legislation to be adopted as C-ITS Regulation appears to qualify mainly as "hierarchist", in the same categorisation "Hierarchist" cultures are characterized by two main elements: (a) Based on the observation that managing the risks requires "special skills", such culture firstly involves "expert forecasting and management". (b) Based on the view that "failure to adequately deal with the risk [would] affect the community at large", they secondly consist of "whole-society solutions" at various steps of risk management. For instance, the State may "enact legislation to ensure that preventative measures are taken" or "provide agents to [provide] remediation (such as firemen managing a fire), which includes information gathering. In the case of C-ITS, the cooperative or peer-to-peer nature of the communications obviously makes coordination acutely necessary. The network could for instance not operate without assurance of the authenticate source of C-ITS messages. Similarly, a threat to one peer could endanger the whole C-ITS network and lead to systemic detrimental consequences.¹⁰⁹ The hierarchist approach is visible in the Proposed C-ITS Regulation, with the significant (and disputed) involvement of public authorities (and especially of the European Commission) as centralised expert agents to ensure coordination between the stakeholders as well as enforcement. Stringent standards to bring interoperability can also be viewed as complementary coordination tools in this regard. While the NIS Directive mainly entrusts

¹⁰² Commission implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, OJ L 26/48.

¹⁰³ NIS Directive, Article 16 (10).

¹⁰⁴ Christopher Hood, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press 2001).

¹⁰⁵ Karen Renaud and al., 'Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious? - ScienceDirect' (2018) 78 *Computer & Security* 198.

¹⁰⁶ Four categories are laid down: "fatalist", "hierarchist", "individualistic" and "egalitarian", *ibid*.

¹⁰⁷ *ibid* 5, quoting Yan (2015).

¹⁰⁸ Carrapico and Farrand (n 16) 251.

¹⁰⁹ The discussion over the role of public authorities in C-ITS coordination and implementation has been discussed in the US, under the auspices of NHTSA, see Daniel Crane, Kyle Logue and Bryce Pilz, 'A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles' (2017) 23 *Michigan Technology Law Review* 191.

regulated entities to adopt internal security management system and to operationalise the security principles, the Proposed C-ITS Regulation provides for a detailed legal regime, characterised by an important role played by public authorities to coordinate the whole C-ITS network.

In this context, it could seem generally difficult to *legally* compare the two legal regimes, characterised by different regulatory approaches, without indulging in arbitrary or policy conclusion.

Yet, both the higher level of details and the different regulatory approach to security of the proposed Regulation boil down to the same aspect. The Proposed C-ITS Regulation regulates security of the C-ITS station operators (and more generally of the C-ITS network) in a more *specific* way than the NIS Directive, which takes into consideration the *specificities of the technologies and of the ecosystem of the sector in question*. Yet again, it is in the view of the author a decisive criterion in determining whether a sector-specific EU legislation should prevail over the NIS Directive provisions. The author *does not take* a normative perspective on the level of details or on the regulatory approach chosen by the legislator. Instead, it is claimed in the present paper that the criterion should be *whether the rationale of these regulatory choices reflects the specificities of the sector, technologies, actors in question, with a view to ensuring security*.

Against this background, the security requirements laid down in the Proposed C-ITS Regulation should prevail, in our view, over security obligations set forth in the NIS Directive and also over national transposing law (with the reservation of the notification requirements noted in the previous subsection).

5. Conclusion

In a future-looking perspective, the paper analysed the interface between the Regulation proposed by the European Commission to regulate C-ITS (Proposed C-ITS Regulation) and the NIS Directive. It focussed on the role of the C-ITS station operator, proposed to be created and regulated by the European Commission in the Proposed C-ITS Regulation. Based on the study of such Proposed Regulation as a case study, the paper mainly discussed the interpretation of the *lex specialis* rule of Article 1 (7) NIS Directive, which regulates under which conditions security obligations laid down in other EU sector-specific legislation apply as *lex specialis* and prevail over the application of the NIS Directive. Two objectives were pursued in the present study. First, the paper aims to contribute to the policy discussion on future C-ITS regulation. Even though the proposal from the European Commission was eventually turned down by the Council, the regulation of C-ITS remains top on the agenda of the European Commission. The paper provides legal recommendations for future C-ITS regulation concerning its interface with the NIS Directive, such topic having been overlooked in the initial proposal. Second, the study aims to contribute to the (yet scarce) legal scholarship on the NIS Directive, particularly on the interpretation of its Article 1 (7).

The paper finds that the NIS Directive is unclear on a number of aspects related to its interface with other EU legal frameworks, and notably in the field of ITS. First, *which actors* should be considered as “operators of intelligent transport systems” within the meaning of the NIS Directive remains unclear, for lack of consistent referencing to the ITS Directive. Second, Article 1 (7) NIS Directive, as complemented by related recitals, was also found to suffer from a lack of clarity and even to some extent inconsistency. It is therein especially unclear whether the NIS Directive shall apply to some extent *in excess of lex specialis* provisions found in other EU sector-specific legislation. For instance,

where EU sector-specific legislation lays down security obligations applying to some operators of essential services which are found to qualify as *lex specialis*, should the remaining incident notifications obligations (of the NIS Directive) apply complementarily or not? The study found no clear legal answer to that question and even hinted to internal inconsistencies in the NIS Directive.

Which criterion(a) to apply when making the gap analysis between two EU legal frameworks remains obscure in the NIS Directive. This issue is acute in cases where the regulatory approach adopted in the ‘other’ EU legal framework is very different from the (described here as) principled-based regulatory approach of the NIS Directive. While the European Commission, in its Communication ‘Making the Most of NIS’, considers that the “level of details” of the obligations therein matters, another interpretation grid is suggested. In our view, the “level of details” is not and should not be the determining factor, but instead, seems to constitute a proxy for the more *specific* way in which a particular EU sector-specific legal framework would regulate security. By ‘specific’, we mean that legal framework takes into account the specificities of the sector, actors, technologies and more generally ecosystem at stake. This focus on the specificity of the regulation of security makes it possible to compare legal frameworks *based on different regulatory approaches* (such as the NIS Directive on the one hand, and the Proposed C-ITS Regulation on the other hand) without indulging in arbitrary discussions on their normative merits.

In anticipation of a potential future C-ITS regulation, the paper makes suggestions to smoothly regulate the interface with the NIS Directive and eventually to bring legal certainty to actors involved. First, the law-maker would better acknowledge the existence of an interface between the two legal frameworks. Second, the vocabulary used should be consistent with this of the NIS Directive or could alternatively use legal fictions to link both legal frameworks. For instance, the future C-ITS regulation could refer to the “C-ITS Station Operator” as a function and clarify that actors conducting related activities should be considered as an “Operator of ITS” within the meaning of Annex II of the NIS Directive. Thirdly, the study unravelled the lack of clarity of the NIS Directive concerning the ensuing legal regime when some *lex specialis* applies, e.g. whether incident notification requirements of the NIS Directive would remain applicable or not where no such requirement is laid down in sector-specific EU legislation. In this context, the law-maker would be well advised to consider whether incident notification requirements are needed in the C-ITS context. Given the high level of integration and cooperation of the C-ITS network and in line with the rationales for a ‘hierarchist regulatory approach’ discussed above, one would intuitively answer positively to this question. In such a case, it is advisable to regulate incident notification requirements *in the C-ITS regulation*.

Acknowledgement

The present study benefited from the experience gathered in the work conducted as part of the CONCORDA CEF project (Connected Corridor for Driving Automation).¹¹⁰

The author would like to thank Ivo Emanuilov and Alessandro Bruni for their insightful comments. All potential errors are these of the author.

¹¹⁰ Information on the CONCORDA project is available here: <https://connectedautomateddriving.eu/project/concorda/>, last visited 26th September 2019.