Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Understanding the rule of prevalence in the NIS directive: C-ITS as a case study

Charlotte Ducuing

Katholieke Universiteit Leuven Centre for IT and IP Law (CiTiP), Sint-Michielsstraat 6, box 3443, 3000 Leuven, Belgium

ARTICLE INFO

Keywords:
NIS directive
Cooperative intelligent transport systems (C-ITS)
ITS directive
Cybersecurity
Rule of prevalence
Information security
Network and information systems

ABSTRACT

The paper discusses the interpretation of the rule of prevalence of Article 1 (7) NIS Directive, which has not been the subject of any academic debate 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. Based on the case study of the recent proposal from the European Commission to regulate Cooperative Intelligent Transport Systems ('C-ITS'), the paper unravels a number of issues and unclarities. Recommendations are made with respect to the interpretation and application of the rule of prevalence of Article 1 (7) NIS Directive. In anticipation of a potential future C-ITS regulation and in the context of a possible upcoming revision of the NIS Directive, the paper also makes suggestions to ease the regulation of the interface between the NIS Directive and other (cyber-)security regulation, particularly in the field of C-ITS.

1. Introduction

The European Directive on the security of Network and Information Systems (the 'NIS Directive')[1] 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.[2] Described as the EU's first cyber-security law, the Directive covers a broad scope, including both "operators of essential services",[3] such as airports or financial market infrastructures, and "digital service providers",[4] referring to cloud computing services, online marketplaces and online search engines.[5] The NIS Directive is viewed as a baseline set of security standards[6] for the protection of network and information systems of services constituting the backbone of

E-mail address: charlotte.ducuing@kuleuven.be

[1] 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.

[2] 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>.

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

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

[5] NIS Directive, Annex III.

[6] '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=wluk> accessed 6 November 2019.

https://doi.org/10.1016/j.clsr.2020.105514
0267-3649/

social and economic prosperity in the European Union.[7] In that respect, the NIS Directive can be conceived of as a *lex generalis* with respect to the security of network and information systems (otherwise called 'cybersecurity'). For that reason, Article 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 electronic communications networks and services and trust services, excluded from the scope of the NIS Directive (Art. 1 (3)).

In contrast to the exception of Article 1(3) which targets specific types of operators and is operationalised by the NIS Directive itself, Article 1(7) is more of a 'catch-all' provision and requires operationalisation by the member States. Article 1(7) can be understood as a rule of prevalence in case of regulatory overlap.[8] Provisions of a sector-specific EU legal act which require 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.[9] In other words, the NIS Directive describes itself as a minimum security legal standard *lex generalis*. In this context, how to assess whether sector-specific requirements are "at least equivalent in effect" to the obligations laid down in the NIS Directive? What is the ensuing security-related legal regime and for which operators?

There is no legal literature specifically dedicated to this provision.[10] Yet, moving from the law in the books to its application to real-life cases proves difficult, as investigated in this paper through a case study. The paper analyses the relationship between the NIS Directive and an EU sector-specific proposed legislation dealing with security obligations: The delegated regulation proposed by the European Commission ('EC') to regulate Cooperative Intelligent Transport System ('C-ITS') communications ('the proposed C-ITS regulation'). The paper conducts an in-depth analysis of Article 1 (7) NIS Directive as complemented by related provisions in the Directive and as interpreted in the Communication from the European Commission 'Making the Most of NIS'.

Two objectives are thereby pursued. The first objective is to contribute the legal scholarship on the NIS Directive, yet rather scarce, in particular regarding the *lex specialis* rule set forth in Art. 1 (7). The second objective is to inform on-going political debates on both the NIS Directive and C-ITS regulation. On the on hand, the EC has indeed launched a public consultation on the implementation of the NIS Directive,[11] which could lead to a revision of the Directive. On the other hand, 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 EC,[12] 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.

The first section introduces the proposed C-ITS Regulation, namely its history, the security obligations that were laid down and how the interface with the NIS Directive was anticipated. The second section turns to the NIS Directive as applicable to the (C-)ITS sector. This section also wraps up the understanding of Article 1(7) NIS Directive as interpreted by the EC in its Communication 'Making the most of NIS'. Against this background, the third section brings to light the challenges and inconsistencies of Article 1(7) NIS Directive. This section is informed by the case study of the proposed C-ITS regulation. The paper concludes with recommendations in order to ease the interface between the NIS Directive and EU sector-specific regulation imposing (cyber-)security obligations.

2. The proposed C-ITS regulation

This section introduces C-ITS communications and the regulation that the EC proposed in 2019 to regulate such communications, including the security of the so-called C-ITS network.

2.1. *A brief history of the stillborn proposed regulation*

'C-ITS' stands for cooperative intelligent transport systems. C-ITS communications are a specific kind (namely, cooperative) of 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.[13] However, given their cooperative character, C-ITS communications cannot deliver such benefits without a coordinated,

[7] 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.

[8] 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.

[9] NIS Directive, Art. 1 (7).

[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.

[11] See the public consultation here: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-commission-launches-public-consultation-nis-directive (last visited 5th October 2020).

[12] 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/5 g/news/commission-remains-committed-to-connected-car-plans-despite-council-blocking/?_ga=2.134080332.374840531.1569337114-1050189813.1569337114 (last visited 24th September 2019).

[13] 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.

trustworthy and interoperable deployment, which is the rationale for the proposed C-ITS regulation.[14] With this instrument, the EC pursued the goal to ensure compatibility, interoperability and continuity of C-ITS services in the deployment and operational use of EU-wide C-ITS services based on trusted and secure communication.[15]

In January 2019, the EC made publicly available a draft delegated regulation on C-ITS services based on the Intelligent Transport Systems Directive ('ITS Directive').[16] Following a public consultation,[17] the EC notified a revised proposal on the 13th of March[18] to the European Parliament ('EP') and to the Council. The C-ITS regulation proposed by the EC did however not see the light of day. It was objected to by the Council on the 8th of July 2019.[19] As a result, the proposed regulation was *not adopted*.[20] In other words, from the perspective of the EC, it is now back to square one.

With the procedure of delegated acts laid down in the TFEU,[21] the EC 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 EC, as a draft delegated act may be objected to by the EP 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 EC 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. The EC was particularly blamed by Member States' delegations in the Council for exceeding its mandate, i.e. by self-conferring upon itself extensive powers and by creation new concepts such as the "C-ITS station operator" (further discussed in this section).[22] It remains therefore debated whether a full-fledged regulation of C-ITS communications could be adopted based on the ITS Directive in the future, or whether a legislative proposal should be made by the EC. In any event, the EC remains committed to making progress on the regulatory front of C-ITS.[23]

The following sub-section looks into the C-ITS regulation proposed by the EC in March 2019 and particularly into the security-related provisions thereto.

2.2. *Security obligations*

The proposed C-ITS regulation was aimed at ensuring the security of C-ITS communications and of the C-ITS network environment. In an open network that enables a many-to-many or peer-to-peer relationship between C-ITS stations, all C-ITS stations need to securely exchange messages with each other precisely because they are not limited to exchanging messages with (a single) pre-defined station(s).[24] One of the objectives of the proposed C-ITS regulation is to "ensure the authenticity and integrity of messages exchanged between C-ITS stations, in order to assess the trustworthiness of such information".[25] The level of security and trust should be the same for all C-ITS Stations,[26] which derives directly from the peer-to-peer characteristic of C-ITS communications. The present sub-section outlines the security provisions in 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.[27] They should especially check that the C-ITS station is certified and, before it is put in service, that it is "enrolled in the EU C-ITS security credential management system, to be set up based on the proposed C-ITS regulation. To do so, the C-ITS station shall be registered in a register 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 C-ITS regulation.[28] The proposed C-ITS regulation also lays down obligations explicitly labelled as 'security obligations' incumbent on the C-ITS station operators. In essence,

[14] 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}.

[15] 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 EC, p. 3.

[16] 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').

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

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

[19] 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. 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.

[20] ITS Directive, Art. 14 (3).

[21] Consolidated version of the Treaty on the Functioning of the European Union, OJ 115/0172 ('TFEU'), Art. 290.

[22] 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.

[23] See https://www.euractiv.com/section/5 g/news/commission-remains-committed-to-connected-car-plans-despite-council-blocking/ (last visited 5th October 2020).

[24] Proposed C-ITS regulation, Rec. 2.

[25] Proposed C-ITS regulation, Explanatory Memorandum, 3.

[26] Proposed C-ITS regulation, Rec. 15.

[27] Proposed C-ITS regulation, Art. 22 (1).

[28] Proposed C-ITS regulation, Art. 5 and 22.

they shall set up an information security management system ('ISMS')[29] in compliance with the C-ITS security policy.[30]

Additionally, the whole EU C-ITS security credential management system to be put in place by the proposed C-ITS regulation and in 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)",[31] and planned to be set up "for the provision of trusted and secure communication between C-ITS stations".[32] 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.[33] 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 for the management of information security in C-ITS on the other.[34]

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 public key infrastructure authorization system.[35] The "trust list manager" would be responsible for generating and updating the European Certificate Trust List ('ECTL').[36] 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.[37] 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.[38] In the preparatory phase of the proposed C-ITS regulation,[39] the need for centralised *governance* bodies was identified for the common European C-ITS trust model.[40] As part of the "implementation of the C-ITS network" consisting of all operational C-ITS stations in the EU,[41] the proposed C-ITS regulation 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.[42] "Pending the establishment of central entities", the EC (controversially) proposed to appoint itself to be in charge of these tasks.[43]

The outline of the security obligations laid down by the proposed C-ITS regulation shows the crucial role played by the C-ITS station operators (as defined in the proposed C-ITS regulation) therein. This being said, the entirety of the provisions laid down in the proposed C-ITS regulation were somehow aiming for the security of the C-ITS network overall. In this respect, the proposal to set up new centralised bodies was directly aiming to secure the C-ITS network. These bodies should therefore also be considered as security-relevant bodies. Before turning to the NIS Directive, the following subsection looks into how the proposed C-ITS regulation considered its interface with the NIS Directive, with respect to the regulation of the security of C-ITS communications.

2.3. *The regulation of the interface with the NIS directive*

The first draft of the proposed C-ITS regulation, issued by the EC in January 2019, simply overlooked the interface with the NIS Directive.

A new Recital (6) was included in the second issue of the proposed C-ITS regulation published by the EC 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).[44] It is, however, unclear how to interpret this sentence. What does "complementary" concretely translate into in terms of legal obligations? Does it refer to the 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 accordance with the proposed C-ITS regulation.[45] However, and as outlined in this section, the C-ITS station operator is not the only entity bearing security obligations. Especially, the new centralised bodies to be set up are core to the security of the C-ITS network.

This section introduced C-ITS communications and the regulation that the EC (unsuccessfully) proposed to regulate them, including to regulate the security of the C-ITS network. While the EC anticipated an interface with the NIS Directive,

[29] Proposed C-ITS regulation, Art. 27 "Information security management system".
[30] The C-ITS security policy is laid down in Annex IV of the proposed C-ITS regulation.
[31] Proposed C-ITS regulation, Ar. 2 (27).
[32] Proposed C-ITS regulation, Art. 23 (1).
[33] Proposed C-ITS regulation, Art. 23 (3).
[34] Proposed C-ITS regulation, Art. 23 (2).
[35] Proposed C-ITS regulation, Art. 24 (1).
[36] Proposed C-ITS regulation, Art. 25 (1).
[37] Proposed C-ITS regulation, Art. 26 (1).
[38] See for instance the proposed C-ITS regulation, Rec. (17).
[39] 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).
[40] Proposed C-ITS regulation, Rec. 27.
[41] Proposed C-ITS regulation, Art. 2 (29).
[42] Proposed C-ITS regulation, Art. 29.
[43] Proposed C-ITS regulation, Rec. (22), Art. 24 (2), 25 (2) and 26 (2). This self-conferral of power from and to the EC was blamed by some national delegations in the Council for exceeding the mandate of the EC. It makes part of the legal questions asked by the General Secretariat of the Council to its legal department (see 15 above).
[44] Proposed C-ITS regulation, Rec. 6.
[45] Proposed C-ITS regulation, Art. 2 (16).

how to regulate such interface remained very unclear. The following section now turns to the NIS Directive.

3. The NIS directive

The NIS Directive encompasses (C-)ITS services in its scope of application. This section describes security and notification obligations falling on such service operators according to the Directive. How the Directive regulates the interface between the NIS Directive and other EU sector-specific cybersecurity legislations, based on Article 1(7), is discussed at the end of the section.

3.1. *The NIS directive and (C-)ITS service providers*

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.[46] 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".[47] The NIS Directive applies to two categories of entities: digital service providers[48] and operators of essential services.[49] 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.[50] Essential services are services which cumulatively pass a three-criteria test. (a) They have to be considered as essential for the maintenance of critical societal and economic activities. (b) They are dependent upon information and network systems and (c) an incident would have significant disruptive effects on the provision of that service.[51] Annex II of the Directive provides for the scope *rationae materiae* with a list of sectors and sub-sectors.

Operators of Intelligent Transport Systems ('ITS') are included in the Annex II of the NIS Directive.[52] As a specific category of ITS, C-ITS (operators) can be subject to NIS Directive obligations, depending on the designation by the respective Member States. In light of the three-criteria test, C-ITS are expected to be particularly security-sensitive because of their peer-to-peer character. As a result, operators active in the field of C-ITS could be simultaneously subject to security obligations arising from both the NIS Directive (as implemented by the respective Member States) and the proposed C-ITS regulation (or any future EU regulation of C-ITS).

This regulatory overlap is further analysed in section four as a specific application of Art. 1(7) NIS Directive, in order to unravel the challenges arising from the interpretation of such provision. Before that, the following sub-section outlines the obligations borne by operators of essential services (such as operators of (C-)ITS) as laid down by the NIS Directive.

3.2. *Security and notification obligations incumbent on operators 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".[53] Risk is defined as "any reasonable identifiable circumstance or event having a potential adverse effect on the security of network and information systems".[54] 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".[55]

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 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.[56] The NIS Directive is the first EU legal instrument focusing on incident notification and information sharing as core requirement, based on research showing the criticality of such information for cyber defense.[57] Incident notification is viewed as a form of cooperation between private and public entities.[58] 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.[59] Subsequently, the shared information are further processed within the CSIRTs network (the EU network of national CSIRTs) to promote swift and effective operational cooperation.[60] Finally, same information are spread to the general public and business, in an aggregated and anonymised man-

[46] NIS Directive, Art. 1 (1).
[47] NIS Directive, Art. 4 (2).
[48] NIS Directive, Art. 4 (6).
[49] As defined in NIS Directive, Art. 4 (4).
[50] NIS Directive, Art. 4 (4) and 5 and Annex II.
[51] NIS Directive, Art. 5 (2).
[52] ITS Directive, Art. 4 (1).
[53] NIS Directive, Art. 14 (1).
[54] NIS Directive, Art. 4 (9).
[55] NIS Directive, Art. 4 (7).
[56] NIS Directive, Art. 14 (3).
[57] Guiseppe Settanni and 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.
[58] NIS Directive, Rec. 35.
[59] NIS Directive, Art. 14 (5).
[60] NIS Directive, Art. 12 (1).

ner.[61] 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.[62] 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 carried out for security purposes might issue "binding instructions […] to remedy the deficiencies identified".[63]

To complete the overview of the NIS Directive, the remainder of this section provides a state of affairs of the (scarce) discussion on the interpretation of Article 1(7) NIS Directive. This constitutes a necessary building block before applying Article 1(7) to the specific case of the proposed C-ITS regulation in the following section.

3.3. *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 Article 1 (7) NIS Directive, which shall be read together with other related provisions of the Directive and in particular with the related recitals. To date, this rule of prevalence has not been discussed in the legal scholarship. Only the EC has provided its own interpretation in its Communication 'Making the Most of NIS', which will therefore be part of our analysis. Although the interpretation of EU legislation by the EC in communications, guidelines and other *soft law* documents has no legally binding value, it does often have a strong impact.[64]

Article 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 EC 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". In the Communication, the EC conducts its own 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 EC 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 EC concludes that the Payment Service Directive 2 ('PSD2')[65] 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 EC concludes that sector-specific EU legislation contains provisions on security requirements "which can be regarded as *lex specialis*." The EC therein highlights the *level of details of the PSD2* – higher than the security obligations as laid down in the NIS Directive - as a relevant criterion for the application of Article 1(7). Contrary to the case of credit institutions (above), no mention is made of notification requirements.[66] The EC also disregards notification requirements when it comes to trading venues. *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 does surpris-

[61] NIS Directive, Rec. 40.
[62] NIS Directive, Art. 15 (2).
[63] 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).
[64] 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.
[65] 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.
[66] NIS Directive, Art. 14 (3).

ingly not even mention it. 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 the rule of prevalence. 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 EC itself does not discuss notification obligations in its analysis of the EU sector-specific legislation of the banking and financial market infrastructure sector, except for the credit institutions (where the EC takes into account the cross-border impact of security incidents notification).

While recital (9) considers the "application in the Member States" of the NIS Directive provisions to make part of the comparison exercise, such a mention cannot be found in the body of the Directive. In particular, Article 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 EC 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 EC 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 EC from drawing conclusions as for the application of the *lex specialis* rule.

The first sections outlined, in turn, the proposed C-ITS regulation and the NIS Directive with respect to security obligations potentially applicable to C-ITS communications. In such a case of regulatory overlap, Article 1(7) NIS Directive shall be applied in order to determine which legal framework(s) shall apply and to what extent. While this section described this rule of prevalence as interpreted by the EC, especially in banking and in financial markets, the following section applies Article 1(7) NIS Directive to the interface with the proposed C-ITS regulation. This analysis serves as a case study to reveal the challenges associated with this provision.

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

The application of Article 1(7) to the proposed C-ITS regulation reveals a few issues, which are analysed in turn: 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 of application. Second, the analysis shows an internal inconsistency in the NIS Directive, which results in uncertainty when a EU sector-specific legislation is found to qualify as *lex specialis*. Finally, 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.

4.1. *The lack of a uniform terminology and misalignments in the scope of application*

At first sight, the material scope (*rationae materiae*) of security obligations in respectively both legal frameworks could seem 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".[67] On the other hand, Annex IV of the proposed C-ITS regulation dedicated to security refers only to "information security" with regard to the mandatory establishment of the CSMS of the C-ITS station operators.[68] Information security is defined as the preservation of the confidentiality, integrity and availability of information, based on the ISO standard 27000.[69] 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.[70] The proposed C-ITS regulation could therefore seem to be narrower in scope.

The general lack of a consistent terminology with reference to security in the digital environment has already been underlined. It is associated with a lack of a consistent conceptual framework, in particular the references to both information security, security of network and information systems and cybersecurity.[71] 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 encompasses somehow also network and information systems. Annex IV 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.[72] 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 C-ITS 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 can be said to cover "interconnected information systems", in this case the C-ITS network.[73] Whether it can consequently be concluded that the respective scopes *rationae materiae* of the legal regimes would be *aligned* remains, however,

[67] NIS Directive, Article 14 (1).
[68] Proposed C-ITS regulation, Annex IV, Point 1.3.
[69] Proposed C-ITS regulation, Annex IV, Point 1.2.
[70] NIS Directive, Art. 4 (1).
[71] Kasper and Antonov (n 11) 12.
[72] Proposed C-ITS regulation, Annex IV, Point 1.5.2.1.
[73] Kasper and Antonov (n 11) 21.

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 proposed C-ITS regulation reaches beyond (cyber-) security, a similar question arises regarding *which provisions* should be considered relevant for the gap analysis between the two legal instruments. 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, C-ITS stations are subject to harmonised technical requirements or conformity assessment procedure,[74] which are *not 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 C-ITS regulation, these tasks would be conducted by the EC in the short term,[75] and 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 provided for in Article 1(7) NIS Directive. Yet, such difficulty is not anticipated in the NIS Directive, which does not provide for guiding principles in such a situation.

4.2. *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 a *lex specialis vis-à-vis* the NIS Directive provisions, 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 [respectively] apply", which suggests that the *remaining* NIS Directive provisions would still be applicable. Both legal frameworks could therefore happen to apply concurrently and complementarily. Concretely, where security requirements of EU sector-specific legislation would apply *in lieu of* NIS *security* provisions, remaining NIS *notifications obligations* would still be applicable, 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 EC,[76] the *lex specialis* rule of Article 1(7) NIS Directive was introduced in the text during the phase of interinstitutional discussions between the EP 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).[77] The initial version was clear in that *only* the "corresponding provisions" of the NIS Directive (security requirements *or* incident notification obligation) 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 obligation) 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 obligations to the operators of essential services, whether security or notification obligations. As a result, the prevalence of, for instance, *security requirements* 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 incident 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 EC in this regard. Having concluded that *both* security and notification obligations in sector-specific legislation shall be considered as *lex specialis* provisions for credit institutions, the EC 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 EC as for the applicable legal regime of central CCPs and trading venues, where only security obligations were discussed (and not incident notification obligations). The EC 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' notification obligation remains applicable.

The very same questioning arises with the proposed C-ITS regulation, which sets forth security obligations *but no notification obligations*. Should the security requirements be deemed

[74] Proposed C-ITS regulation, Art. 5 and Annex V.
[75] Proposed C-ITS regulation, Art. 29 (1) (b).
[76] 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) */.
[77] 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.

"at least equivalent" to the NIS Directive security requirements, would incident notification obligations laid down by the NIS Directive apply "complementarily" to them (as suggested by recital 6 of the proposed C-ITS 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 uncertainty would have had to be borne by the Member States, according to recital 9 NIS Directive.

4.3. *Comparing apples and oranges?*

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

One could initially think of the level of details of the legal provisions. What is indeed immediately visible from the above outline 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. For instance, a detailed Annex is dedicated to the "ISMI" in the proposed C-ITS regulation, while security requirements laid down in the NIS Directive could seem quite '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" . In this context, can the higher *level of details* of security provisions in the proposed C-ITS regulation be considered as a relevant factor? 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 EC 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 EC 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 details. It does more generally not clarify *which criteria* should be taken into account when conducting the gap 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 invite one to go beyond a mere *legal* assessment, 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 EC does not clarify it.

In the case of the proposed C-ITS regulation, the different level of details between the two legal frameworks points 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. 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". Such a regulatory approach is based on the observation that most 'essential services' are operated by businesses, who are considered to be well-placed to handle cybersecurity risks and threats. As identified by M. Storm Jensen, the shift to complex societies has turned the focus "from a central approach […] to neoliberal, dynamic and self-regulating approaches […]. In this paradigm the government's role is no longer to control events during crises, but to establish conditions that give the involved actors the abilities and incentives to react in an optimal manner".[78] The NIS Directive is as an illustration of such an approach.

From a regulatory perspective, these provisions could best be described as "principle-based", as opposed to "rule-based".[79] While rule-based regulation "prescribes or prohibits specific behaviours, principle-based regulation 'emphasises general and abstract guiding principles for desired regulatory outcomes'".[80] 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 'responsibilises' the regulated entities, who can and shall design their internal regulation. One could argued 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).[81] 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 by the fact that, for digital service providers, the NIS Directive provisions (together with the EC's implementing act), which lay down a similar regime to this applicable to operators of es-

[78] Mikkel Storm Jensen, 'Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle' (2018) 1 Scandinavian Journal of Military Studies 1, 5.

[79] 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).

[80] 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).

[81] NIS Directive, Art. 3.

sential service providers,[82] constitute 'maximum harmonisation'.[83]

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.,[84] as further discussed by Renaud and al. in the field of (cyber)security and resilience regulation.[85] The categorisation is based on the respective roles of individuals and governments in the risk management process.[86] "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".[87] 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.[88]

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 law-maker 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.[89] The hierarchist approach is visible in the proposed C-ITS regulation, with the significant (and disputed) involvement of public authorities (and especially the EC) 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 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 a similar 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*. 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 take* a normative perspective neither on the level of details nor on the regulatory approach chosen by the legislator. Instead, it is contended that the relevant 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*. In this paradigm, the level of details should not be considered *as such* as a relevant element. The reading of the Communication from the EC 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 EC would seem to consider implicitly as a relevant criterion.

Coming back to our case study, 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 unclear situation of incident notification obligations highlighted in the previous sub-section).

[82] 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.

[83] NIS Directive, Art. 16 (10).

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

[85] Karen Renaud and and al., 'Is the Responsibilisation of the Cyber Security Risk Reasonable and Judicious? - ScienceDirect' (2018) 78 Computer & Security 198.

[86] Four categories are laid down: "fatalist", "hierarchist", "individualistic" and "egalitarian", ibid.

[87] ibid 5, quoting Yan (2015).

[88] Carrapico and Farrand (n 7) 251.

[89] 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.

5. Conclusion and recommendations

In a future-looking perspective, the paper analysed the interface between the regulation proposed by the EC to regulate C-ITS and the NIS Directive, as a case study to better understand and interpret the rule of prevalence of Article 1(7) NIS Directive. The first objective in doing so is to contribute to the (yet scarce) legal scholarship on the NIS Directive, particularly on the interpretation of its Article 1(7). The second objective is to contribute to the policy discussion on the future of C-ITS regulation on the one hand, and on the evaluation (and possible revision) of the NIS Directive on the other.

The paper finds that the NIS Directive is unclear on a number of aspects related to its interface with other EU legal frameworks. Article 1(7) NIS Directive, as complemented by related recitals, was 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. Besides, the absence of consideration by the EU law-maker for a consistent vocabulary in the field of (cyber-)security constitutes another challenge in comparing two EU legal frameworks, for lack of a common reference.

Thirdly, 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, as illustrated by the case study of the proposed C-ITS regulation. While the EC, 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 seems to constitute rather a proxy for the more *specific* way in which a particular EU sector-specific legal framework would regulate (cyber-)security. By 'specific', we mean that a 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 regulation of C-ITS, several recommendations can be made, which are equally valid for any future EU sector-specific legislation involving (cyber-)security requirements which could overlap with the NIS Directive. The law-maker would better acknowledge and anticipate the existence of an interface between the two legal frameworks. The vocabulary used should be consistent, as much as possible, with this of the NIS Directive or could alternatively use legal fictions to link both legal frameworks. In light of the on-going assessment of the implementation of the NIS Directive and of its possible revision, the study unravelled an internal lack of clarity and even inconsistency in the NIS Directive. This concerns the ensuing legal regime when some *lex specialis* applies, *e.g.* whether incident notification obligations in the NIS Directive would remain applicable or not where no such requirement is laid down in sector-specific EU legislation. This issue could be clarified during a revision of the NIS Directive or, failing that, would have to be specifically considered in every EU sector-specific legislation involving (cyber-)security provisions, such as any potential regulation of C-ITS in the future. Finally, the fact that the NIS Directive entrusts the Member States to apply Article 1(7) NIS Directive may not constitute a practical and fair solution when the EU sector-specific legislation at stake is directly and uniformly applicable, such as with the proposed C-ITS regulation.

Acknowledgment

The present study benefited from the experience gathered in the work conducted as part of the CONCORDA project (Connected Corridor for Driving Automation) which has received funding from the European Union's Connecting Europe Facility (CEF) programme Transport Sector under grant agreement No INEA/CEF/TRAN/M2016/1364071. The author would like to thank Ivo Emanuilov and Alessandro Bruni for their insightful comments. All potential errors are these of the author.

References

Andone C and Greco S, '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

Carrapico H and Farrand B, '"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

Crane D, Logue K and Pilz B, 'A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles' (2017) 23 Michigan Technology Law Review 191

Ducuing C, Oneto L and Petralli S, 'Fairness and Accountability of Machine Learning Models in Railway Market: Are Applicable Railway Laws Up to Regulate Them?' (2018) ⟨https://lirias.kuleuven.be/retrieve/526441⟩ accessed 24 September 2019

Fenwick M, Kaal WA and Vermeulen EPM, '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)

Holzleitner M-T and Reichl J, 'European Provisions for Cyber Security in the Smart Grid – an Overview of the NIS-Directive' (2017) 134 e & i Elektrotechnik und Informationstechnik 14

Hood C, Rothstein H and Baldwin R, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press 2001)

Jensen MS, 'Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle' (2018) 1 Scandinavian Journal of Military Studies 1

Kasper A and Antonov A, 'Towards Conceptualizing EU Cybersecurity Law' (University of Bonn; centre for European Integration Studies 2019) Discussion Paper C253 2019 ⟨http://aei.pitt.edu/100365/1/DP-C253-Kasper_Antonov.pdf⟩

Markopoulou D, Papakonstantinou V and de Hert P, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' [2019] Computer Law & Security Review 105,336

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

Settanni G and al., 'A Collaborative Cyber Incident Management System for European Interconnected Critical Infrastructures - ScienceDirect' (2017) 34 Journal of Information Security and Applications 166

'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=wluk⟩ accessed 6 November 2019

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.