Comparison and analysis of definitions and overlap between the NISD and the EECC' security provisions

Discussion paper by the Netherlands

The NISD proposal includes the deletion of article 40 and 41 of the EECC as stipulated in article 40 and explained in recital 48. As a consequence, providers of public electronic communication networks or publicly available electronic communication services would have to fulfill the security and notification requirements of the NISD. We view this as a problem because we fear this will lead to a narrowing of the scope of the security requirements and legal uncertainty for the entities.

This paper is meant to provide a basis for a more substantive discussion on the interplay between the NISD and the EECC. It does not cover all the provisions but focuses on the security provisions as mentioned in art. 40 (1) EECC and art. 18 (1) NIS and relevant definitions and builds upon the BEREC's opinion[1] regarding the effects of the proposed NIS on electronic communications networks and -services.

Our (preliminary) legal analysis gives food for thought regarding two particular topics: (a) the definitions and its consequences and (b) the differences in scope of the security requirements. Additionally, it will also take BEREC's recently published opinion on the revised NIS proposal and its effect on the electronic communications in consideration.

First of all, "the security of networks and services" (EECC) will be replaced by "network and information systems" (NISD). From a first glance this difference appears to be very limited, however when further analyzing these definitions there seem to be unintended, but also undesirable, negative consequences for its application. It is difficult to determine how this would work out in practice, but it will probably lead to a narrowing of the scope of the applicable security requirements, e.g. because 'related services' as stipulated in the EECC for electronic communications services (ECS) & electronic communications networks (ECN) are in our view not covered by the NISD. The ambiguity of definitions and its application would also result in legal uncertainty for competent authorities and entities.

Secondly, the new NISD proposal only revokes art. 40 and 41 of the EECC, while security requirements for ECS and ECN are still regulated under art. 108 and 109 of the EECC. This would lead to overlapping or conflicting requirements for ECS and ECN which would increase the legal uncertainty and does not benefit the overall security of entities. The subject of security is addressed in more articles in the EECC than in articles 40 and 41.

Thirdly, in order to properly assess the relationship between NIS and EECC, it is necessary first to clarify the scope of "services" (article 18.(1)) and the meaning "related services" (article 4 ((2) of the NIS (generic and telecomspecific) because this determines which services are covered by the NIS.

Recalling article 2(6) of the NISD about lex specialis, it is important to guarantee that the NISD only directly regulates sectors when it leads to a higher or at least equivalent level of security. Therefore, issues as described in this discussion paper ought to be resolved because in effect in the current situation it seems that the EECC classifies as lex specialis because it introduces a higher level of cybersecurity for the telecom sector as the NISD is introducing.

All of the above points will be discussed in more detail below:

Attachment 1: Technical analysis overlaps and gaps EECC and NISD

I. Comparison definitions

- The wording of the definitions in both the EECC and NISD as well as the wording of the security requirements appear to be very similar. This could lead to the conclusion that there is no difference in its application and meaning. However, the definitions of 'network and information systems' (NISD) and 'electronic communication network' / 'electronic communication services' (EECC) are actually quite different[2]:

[1] BEREC opinion on the proposed NIS Directive and its effects on Electronic Communications, 19 may 2021.
[2] Although a network and information system can also be an electronic communication network (see art. 4, point 1 (a) NIS).

  - Under the NISD 'provision of their services' (art. 18 (1)) seems to refer to the (essential?) service(s) provided by entities, i.e. the supply of electricity, gas, transport etc. The directive doesn't clarify the scope of "services",. E.g. if a supplier of energy provides various services, such as providing electricity, cleaning services and maintenance, do all these services fall within the scope of NIS or is it limited to providing electricity? Should there be a connection between the way an entity is addressed in the NIS and the service(s) that are regulated?
  - How does this relate to the telecom sector? Is the equivalent in the EECC of "provision of their services", the "(public?) electronic communication services", because these are the essential services in telecom? An electronic communication service is e.g. telephone (fixed and mobile), SMS (mobile), internet access (fixed and mobile) and with the entry into force of the EECC also OTT-services[3] such as Whatsapp[4] and Skype.
  - A provider's electronic communication network is necessary for the provision of its own services, but is also used by other providers of publicly available electronic communications services, such as MVNOs. Do the technical activities and equipment, so the wholesale activities that the MNO's deploys for MVNOs, also fall under the NIS, in other words do these activities fall under the scope of "providing services"?
- In the NIS, the position of the "electronic communication network" is unclear. The definition of "network and information system" (article 4 (1) also refers to the definition of an electronic communication network (article 2(1) of the EECC. Does this mean that electronic communication network components such as RAN, HLR, OSS & BSS etc., fall within this definition? In its opinion BEREC has expressed similar concerns.

II. Comparison between the security requirements

Scope of security requirements

- The definition and the meaning of "security of networks and services" (EECC) is broad, because it encompasses the entire security of an ECN & ECS. This means everything to achieve availability, authenticity, integrity or confidentiality. Although not explicitly stated in the EECC, this also includes the network and information systems required for the ECN and ECS to function and its physical security.
- Article 2 (21) of the EECC makes clear that the "related services" are other services than the ECN or ECS. Therefore in the national implementation[5] of the EECC, NL has interpreted "related services"[6] as a provider's own additional services, such as voicemail service, data storage services or streaming services which it provides to its users (and not e.g. third parties services) which are not a part of the "electronic communications services". The NISD doesn't make exactly clear in article 4 (2) what is meant by "related services". Do they have the same meaning as "their services" in article 18 (1)? "Related services" are both mentioned in the NISD and EECC, but they have a different meaning. In its opinion BEREC has stipulated a similar conclusion.
- Under the NISD, the "provisions of their services" (art. 18 (1) seems to refer to the electronic communications service (and also to the electronic communications network?). This would mean that its scope differs from the EECC actually introduces a narrower scope. The EECC focuses on all security aspects of ECN/ECS and its related services while NISD only focuses on the network and information systems required for the "provision of services", i.e. for ECN/ECS.

III Overlap of security requirements in NIS and EECC

- Security is not solely addressed in articles 40 and 41 in the EECC and is not completely isolated from the other provisions of the EECC. because article 108[7] and article 109 (8) remains in the EECC, the security of ECN & ECS are both regulated in the EECC and in the NISD. Thus there is a significant overlap between art. 108 and art. 109 (8) of EECC and the security requirements as mentioned in the NIS concerning the security of voice communications services and internet access services which are part of ECS. Emergency services are also provided via publicly and non-publicly available ECNs.

[3] NB-ICS & NI-ICS = Number based- & Number independent Interpersonal communication service.
[4] Whatsapp and Skype fall under the definition of number-independent interpersonal communication service, which is part of an electronic communication service.
[5] Telecommunicatiewet.
[6] See definition "security of networks and services"
[7] See p.4 for definition

- As stipulated in art. 108[8] EECC, "*to ensure uninterrupted access to emergency services*" would also require security and continuity of (publicly available) electronic communication networks.
- The same overlap concerns article 109 (8) EECC[9]: "*In order to ensure effective access to emergency services through emergency communications to the single European emergency number '112' in the Member States, the Commission shall, after consulting BEREC, adopt delegated acts in accordance with Article 117 supplementing paragraphs 2, 5 and 6 of this Article on the measures necessary to ensure the compatibility, interoperability, quality, reliability and continuity of emergency communications in the Union with regard to caller location information solutions, access for end-users with disabilities and routing to the most appropriate PSAP. The first such delegated act shall be adopted by 21 December 2022.*"
- BEREC has also pointed out the differences in goals of the EECC (art. 3) and NISD.

IV What are the practical consequences of ambiguity of definitions and the narrowing of the scope of security requirements? Are there alternative solutions?

- Due to changing terminology and the (so far) lacking of a clear interpretation of definitions used in the NIS, there is unclarity of the scope of the NIS. This and the huge overlap between the NIS and EECC will lead to legal uncertainty and confusion among competent authorities and the sector.
- Recital 49 of the NISD states that existing national legislation following the implementation of the EECC should be continued to be used by the competent authorities in charge of supervision and enforcement for the purposes of this directive. However, the question is whether the national measures that have been - or which are currently being - drawn up, such as in the context of 5G security are still fitting the narrowed scope of art. 18 (1) of the NISD. In addition, this recital does not provide sufficient legal basis to apply the broader scope of the EECC.
- Article 2, point 6 NIS states: "*where provisions of sectors-specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive….shall not apply*".
- The justification for the inclusion of ECN and ECS in the NIS 2.0 is stated in consideration nr. 48 NIS: "*In order to streamline the legal obligations imposed on providers of publicly available ecn and ecs and trustservices related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities and bodies to benefit from the legal framework established by this Directive (including CSIRT and Cooperation Group), they should be included in the scope of application of this Directive*."
- A higher telecomsecurity level has been reached since the introduction of security requirements in 2009 with the implementation of art. 13a and 13b of the Framework Directive (now included as Art. 40/41 in the EECC) and good experiences have been gained with this.
- Therefore, to avoid legal uncertainty, duplication of requirements in NISD and EECC and changing the obligations for entities so quickly after the national implementation of the EECC, we would like to suggest to maintain the obligations for providers of public electronic communications networks and services in the EECC (reporting obligations security requirements and supervision). In order to address the lack of governance as mentioned in recital 48, we would like to arrange in the NIS that the governance structure and measures as described in chapters 2 and 3 should also be applicable to the telecomsector. Obligations such as the cybersecurity strategy, the coordinated vulnerability disclosure (CVD), national cybersecurity crisis management frameworks, Single Point of Contacts, CSIRTs, Cooperation Group, EU-Cyclone and peer reviews could also be applied to sectors with existing lex specialis.

Attachment II: Background information legal text EECC and NISD

Comparison EECC and NISD

III. Outline relevant definitions

[8] Article 108 probably requires a higher level of security measures than article 40EECC or article 18(1) NIS, because "Member States shall take all necessary measures to ensure the fullest possible availability of voice communications services and internet access services provided over public electronic communications networks in the event of catastrophic network breakdown or in cases of force majeure". That seems to be a higher level of security than "appropriate and proportionate" measures, but this should be further discussed.
[9] See also recital 316 EECC

a) EECC

- **Article 2 (1)**: '**electronic communications network'** means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;
- **Article 2 (4)**: '**electronic communications service**' means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:
  (a) 'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
  (b) interpersonal communications service; and
  (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;
- **Article 2 (21)**: '**security of networks and services'** means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services;
- The EECC does not contain a definition of network and information systems.

b) NISD

- **Article 4, (1) NIS** says: '**network and information system'** means:
  (a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;
  (b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;
  (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;
- **Article 4, (2)** says: '**security of network and information systems'** means 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;

IV. Outline relevant provisions regarding security requirements

- **EECC**
- **Article 40 (1)**: "Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed **to the security of networks and services.** Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services."
- **Article 108**: "Member States shall take all necessary measures to ensure the fullest possible availability of voice communications services and internet access services provided over public electronic communications networks in the event of catastrophic network breakdown or in cases of force majeure. Member States shall ensure that providers of voice communications services take all necessary measures to ensure uninterrupted access to emergency services and uninterrupted transmission of public warnings[10]."

- **NISD**
  Article 18 (1): "Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to

[10] Article 110 EECC also adresses public warnings

the security of network and information systems which those entities use in the provision of their services. 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 presented."