The application of RED Article 3.3 to address cyber/privacy risks

Input document for TCAM WG on 14 May 2018
Source: The Netherlands
Date: 14 May 2018

Summary

The instruments of the RED article 3.3 seem to fit well in the overall Dutch national cyber security policy. This regards network integrity, privacy as well as fraud.
The RED is an established and already available regulation and has the potential to prevent, in the short term, a large part of the cybersecurity problems for consumers by setting basic radio equipment requirements. We suggest to use this potential on the short term and work to fine tuning (by modifications of the RED and/or new regulations) on the longer term.

To take a more precise position on the RED, it should be more clear which security areas can be covered by the RED and to which extent, vis-a-vis other EU legislation. Also has to become more clear in which stages of the product life cycle the protection against security risks applies and where the responsibility lies. The mapping which have been provided by the EC is a very useful compilation of existing and foreseen regulation and should be further elaborated with an analysis of possible gaps and doubles across the different existing and foreseen EU legislative instruments. The Netherlands proposes to use for this task the structured framework as given in Annex 1 of this document.
This framework can also be used in the development of (law related) cyber security regulation by helping to identify and develop the most suitable legislation which is able to offer proportionate instruments which adequately address the security risks related to specific equipment or services.

With respect to software updates, the Netherlands invites the Commission to investigate the potential of art 7 of the RED. Article 7[1] of the RED seems to provide a basis for assuring that software updates shall be provided as radio equipment may not be put into service or be used when they cannot properly be maintained in order to stay compliant with the RED. One could conclude that proper maintenance in certain cases is not possible without the availability of regular security updates and that for this reason the putting into service of equipment without software updates could be restricted

1. Introduction

On 7 February 2018 a special TCAM meeting was organized by the EC with a view on the possible extent of the applicability of Article 3(3) of the RED to (cyber)security issues related to radio equipment, which we greatly appreciated. The Netherlands has been one of the Member States inviting the European Commission to explore ways in which this part of the RED could be utilized to combat cyber security in the context of internet connected devices (IoT).

[1] RED at7. :" *Member States shall allow the putting into service and use of radio equipment if it complies with this Directive when it is properly installed, maintained and used for its intended purpose……*"

The result of the meeting was a commitment of the Commission to conduct a gap analysis of the RED vis-a-vis other existing and foreseen EU legislation relevant for cyber security, as well as to come up with a proposal for elaborating possible delegated acts under Article 3.3 of the RED. Member States were asked to give their views, comprising priorities, with reference to problems occurring on the national level, as well as their views on how to utilize RED article 3.3 in this regard.

2. National policy framework for cyber security

The government of the Netherlands has initiated a process involving all relevant stakeholders in order to develop a coherent and effective cyber security policy for connected devices. Such policy will be based on the following main principles:

- Product Life Cycle-approach (PLC): all phases of the life cycle of a product are to be considered, from the design phase, use phase and phase where the product phases out and reaches its end of life;
- Portfolio-approach: a mix of instruments will be necessary to establish an effective policy;
- Stakeholders, such as manufacturers, end-users and telecom providers have different roles and should have corresponding responsibilities.

The foreseen mix of instruments comprises the following:

- Stimulation of the use of voluntary technical standards and certification
- Basic product safety requirements and surveillance (including the RED approach)
- Application of formal product liability
- Protective measures by internet access providers
- Promotion/facilitation of cybersecurity research and testing
- Establishing a public monitor of products with appeared vulnerabilities
- Creating awareness and user empowerment

With respect to some areas it is clear that creating an optimal cyber security environment needs the implementation of multiple measures and this is certainly the case for user-critical applications.

3. Using proportionate instruments based on security risks

We note that product security risk depends on the impact of a vulnerability (on a certain user or others) and the number of users affected (or the probability that a user will be affected); products with high risks may have a large impact on a small number of users or low impact on many users. It is also important to recognize a vulnerability in the system of a certain user may that affect multiple other users so external effects may play an important role. Measures should address both situations; but the optimal mix of the above mentioned measures could be different for different risk areas. E.g. in the latter case the instrument of awareness and user empowerment could be relatively more important.

In the development of (law related) cyber security regulation we propose to use a structured framework (like the framework stated in figure 1 in the annex of this document) to help to identify

and develop the most suitable legislation that can offer proportionate instruments which adequately address the security risks related to specific equipment or services.

With regard to (law-related) regulation for products or services, the concerned instruments in these domains should be well distinguished but are also related to each other:
- *Essential requirements* in product legislation with which products have to comply obligatory;
- *Technical standards*, which can be both voluntary or obligatory;
- *Conformity assessment, by third or first party*. Third party conformity assessment is done by an independent body (certification). First party conformity assessment means that the manufacturer performs the conformity assessment himself (self-certification). Both can be voluntary or obligatory, and are based on legal requirements and/or technical standards.

Generally, measures in the area of conformity assessment should be founded on a risk based approach and should be specific for certain products or groups of products. Depending on the risk involved, the characteristics of the market and type of products a choice should be made between voluntary or obligatory conformity assessment. And when obligatory conformity assessment is used a clear choice between first or third party should be made.

4. RED features for addressing security of equipment

Flexible conformity assessment under the RED

The RED system incorporates obligatory conformity assessment procedures. Depending on whether the manufacturer uses harmonized standards or not this can be first party conformity assessment or third party conformity assessment. This relation between the use of harmonised standards and the choice between first or third party conformity assessment is specific for the RED.

Broad Scope, short implementation time, effective market enforcement

The RED can be regarded in the context of 'wireless internet connected devices' de facto as a horizontal (non-sectoral) approach because many kinds of equipment are (or will be) internet connected in a wireless way. It has the advantage of being able to be implemented in relative short time. It also has the advantage that its point of action within the product life cycle is the making available on the market of products, where surveillance and enforcing can be much more effective compared to measures that apply merely to the use phase of the product.

Broad coverage of ICT security requirements

The implementation of the RED article 3.3 fits well in the overall Dutch national cyber security policy. This regards network integrity, privacy as well as fraud. Conformity assessment of requirements to be defined under article 3.3 can be either first party or third party. This degree of freedom gives an opportunity (from the viewpoint of industry costs) to create generic basic product requirements that may apply to a wide range of products that potentially generate security risks (which may extend to all public internet connected devices), and set specific requirements only in cases where needed.

General basic requirements should include the support of adequate levels of encryption, authentication and protection against the loading of malicious software. It is also important that

software which is loaded in the devices is developed in a safe (under quality control) development process, which prevents a lot of potential security flaws.

Software updates under the RED framework

Where there is a need for basic (minimum) product requirements, related software updates shall be supported by manufacturers. Software updates are essential for maintaining an adequate level of security for many types of products during their use in their expected life time. On the basis of the RED (article 3.3 e and 3.3 f) certain types of radio equipment should be designed in such a way that they support 1. the possibility to be updated and 2. a secure connection for applying updates.

Article 7[2] of the RED seems to provide a basis for assuring that software updates shall be provided as radio equipment may not be put into service or be used when they cannot properly be maintained in order to stay compliant with the RED. One could argue that this is in certain cases not possible without the availability of regular security updates.
A measure for assuring that the provided updates will be installed by the end user could be a technical feature in the radio equipment which turns the radio function (or the specific function generating potential security risks) on or off at the hardware and/or software level depending on if the updates have been installed or not.
Art 3.3(i) can be used to assure that the manufacturer will provide, and the user can load only software updates that are compliant with the RED.
We invite the Commission to investigate the potential of this clause (art 7. RED) .

Furthermore we refer to EU legislation about product liability and its evaluation process. We understand that a specific issue in this evaluation is the relation between product liability and software.

Conclusion RED features

The instruments of the RED article 3.3 seem to fit well in the overall Dutch national cyber security policy. This regards network integrity, privacy as well as fraud.
The RED is an established and already available regulation and has the potential to prevent, in the short term, a large part of the cybersecurity problems for consumers by setting basic radio equipment requirements. We suggest to use this potential on the short term and work to fine tuning (by modifications of the RED and/or new regulations) on the longer term.

5. Comments on cyber related RED art 3.3 articles

Article 3.3 (d):
Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service

This article has a special relationship with the EU Directive 2008/63. This directive aims to stimulate competition in the market for terminal equipment – basically all IoT devices. It frames a free choice of terminal equipment to the condition that terminal equipment is suited for the network interface

[2] RED at7. :" *Member States shall allow the putting into service and use of radio equipment if it complies with this Directive when it is properly installed, maintained and used for its intended purpose……*"

concerned and complies with essential product requirements under the RED or EMC-directive whichever is applicable.
Implementation of the RED article 3.3 (d) requirements may well support that aim and have a complementary role, e.g. in order to combat impacts of DDoS attacks on public networks. On the basis of 3.3 (d) the obligation should be there to e.g. prevent the installation of malware and if the prevention to illegally install malware fails it should be required that the manufacturer provides for a software update so that this failure is corrected. In that way the equipment is protected to be part of a DDoS attacks.
The Netherlands is of the opinion that secure behavior of terminal equipment related to network functionality in the design phase of the product is mainly a responsibility of the manufacturer - not of the provider of the public network.
In order to be able to assess product categories where article 3.3 (d) requirements should apply a mapping is necessary of specific risks of network dysfunctionality.

Article 3.3 (e)
Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected

Radio equipment should be designed in such a way that data stored on the device and/or transmitted with the device is well protected. Following this principle, the complementary role of the RED is beneficial to reach the aim of the GPDR and the implementation of article 3.3 (e) may have a broad scope. In addition one basic requirement could be the possibility to turn the radio function or the specific function generating potential security risks on or off at the hardware and/or software level.

Article 3.3 (f)
Radio equipment supports certain features ensuring protection from fraud

Implementation of this requirement will be beneficial in a significant number of cases. A mapping of different forms of fraud is needed in order to assess the content of such requirements and the product categories on which these should be applied. There are many forms of fraud and it may be useful to look at measures preventing the use of common background techniques like identify theft.

Article 3.3 (i)
Radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated

The potential of this requirement in relationship with the previous requirements should carefully be assessed.

ANNEX 1

Table 1: Concept: A framework to be used for mapping cyber security regulation/initiatives as well as for determining the proportionate regimes for certain products and services

Characteristics of cyber security related regulation		Radio Equipment Directive 2014/53/EU (GROW.C3)	General Data Protection Regulation 2016/679 (JUST.C3)	ePrivacy Directive 2002/58/EC (CNECT.H1)	ENISA prospective Regulation (CNECT.H1	Directive 2008/63 (COMP.C1)	Machinery Directive 2006/42/EC (GROW.C3)	Medical Devices (GROW.D4)	GPSD (JUST.E3), The General Product Safety Directive (GPSD)	NIS Directive 2016/1148 (CNECT.H1)	Payment Services Directive (PSD2, Directive 2015/2366/EU) (FISMA.D3)	ITS directive?
Type of ICT security	Misuse of network or network components	Yes										
	Privacy and protection of personal data	Yes										
	Fraude	Yes										
	Loading of non compliant software during the phase of “use”.	Yes										
	Other	n.a.										
Scope	Products (kind, horizontal, sectorial)	Radio equipment (including combined equipment radio + non radio)										
	Services (commercial/ vital, national safety/other)	n.a.										

Geographic applicability	European/National/World Wide	European												
Voluntary/obligatory requirements	Voluntary	No												
	Obligatory	Yes (Obligatory in Europe)												
Conformity assessment	First party assessment (self assessment)	Yes, voluntary but only if HS are used												
	Third Party assessment	Yes, obligatory if no HS are used, voluntary if HS are used												
(For products) Stage in time in product life cycle where <u>protection</u> is applicable /and who is <u>responsible</u>	Placing on the market	Yes	Responsible: Manufacturer											
	Making available on the market	Yes	Responsible: Manufacturer/ Distributer											
	Putting into service	Yes	Responsible: Manufacturer/ First user											
	Use	Possible? if taken into account at the moment of placing on the market	Responsible: User/ manufacturer?											
	Phase out (end of life)	Possible?, see above at “use”	Responsible: User/ manufacturer?											
(For services) Stage in time in service life cycle where requirements are applicable /and who is responsible	During service	n.a.												
	Other													

Conformity assessment	Intended use by user	Yes										
	Reasonable foreseeable (mis)use by user	No										
	Misuse by user	No										
	Other	n.a.										
Enforcement measures in case of non-compliances	Equipment withdrawal from the market	Yes										
	Equipment recall at end user	Yes										
	Equipment prohibition of use	Yes										
	For Service: Correcting measures at provider of a service	n.a.										
	Other	n.a.										