Position Paper –NIS-Review

Bitkom position towards the Revision of the NIS Directive

2 of October 2020

Introduction

The Directive (EU) 2016/1148 concerning measures for implementing an equivalent and commonly high level of security in network and information systems across the Union (hereafter referred to as the NIS Directive) is currently reviewed by the European Commission. By having shared our view and position with the Commission about the combined Evaluation Roadmap / Inception Impact Assessment in August, we already contributed to the first milestone on the way to a revised legislative proposal scheduled for Q4 2020.[1]

As the next leap ahead does not only foresee the submission of a detailed questionnaire but also allows for the provision of further written contributions, we are pleased to provide both and hope likewise that our additional input further assists the Commission in substantially and sustainably strengthen the resilience of networks and systems across Europe. While the questionnaire touches upon significant aspects, we welcome the possibility to provide hereby a more nuanced contribution. As before, our position is guided by the urgent need to create a more coherent and harmonized common level playing field for operators of essential services (OES) as well as for digital service providers (DSP) across the Union. We are convinced that common and harmonized cybersecurity rules at EU level are the most effective way to achieve a higher level of cyber resilience. We see the clear need to deepen the harmonization of the European Digital Single Market and to avoid new forms of fragmentation.

In tangible terms, **we are in favor of targeted regulatory interventions**. While empirical evidence[2] revealed several persisting inconsistencies that are best addressed by legal amendments, we remain cautious about adopting an entirely new legislative act. Although well-intended, the latter would imply a long and time-consuming process that may not keep up with the constantly evolving particularities of the cyber and IT security. Hence, instead we call for an approach that addresses the most pressing issues in the first place through the revision of certain aspects of the NIS Directive. However, this revision shall still offer the private sector the necessary leeway in order to develop its own content-tailored solutions and innovative ideas to significantly strengthen Europe's cyber-resilience. The protection of networks and systems against any form of disruption is in the innermost interest of OES and DSP.

[1] https://www.bitkom.org/Bitkom/Publikationen/Bitkom-views-concerning-the-nis-directive-review-roadmap
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52019DC0546

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Sebastian Artz
IT Security
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Furthermore, the scope of the revised directive should be in accordance with the most serious threats for network and information security. In the case of OES, Member States are allowed to impose stricter security and notification requirements than those enshrined in the current Directive. This does, however, not account for DSP. Bitkom continues to **favor a "light-touch" regulatory approach as the appropriate way forward concerning DSP**, especially in view of their rapidly changing nature and innovative potential.

Complementary information to our answers provided through the consultation questionnaire

First of all, it shall be noted that we filled in the questionnaire through a German-centered lens as this was deemed most useful to provide the Commission with the reliable insights. For example, when we indicate that the level of cybersecurity resilience in a sector is "high", it refers to the high level of protection in Germany. We hope that this approach facilitates the work of aggregating qualitatively high responses across all European Member States for the good of cross-country cyber-resiliencies.

Section 1: General questions on the NIS Directive

Relevance of the NIS Directive & Cyber-threat landscape (1.a. & 1.b.)

We are completely convinced that the overarching objectives of the NIS Directive:

- increase the capabilities of Member States when it comes to mitigating cybersecurity risks and handling incidents,
- improve the level of cooperation amongst Member States in the field of cybersecurity and the protection of essential services, and
- promote a culture of cybersecurity across all sectors vital for our economy and society

They are not only of significant importance but even of greater relevance today when compared to the situation in 2016. In the same vein, Cyber-threats have increased significantly since the adoption of the NIS Directive.

Concerning the level of preparedness of SMEs in the EU, as inquired about in Q2, it is rather difficult to provide an overall response on a scale from 1 to 5. A more precise answer is required at this point. The reason is that, especially in Germany, the landscape of SMEs is highly diverse and you can find highly specialized SMEs or even small companies that do score very well when it comes to cybersecurity. But of course, the majority of SMEs is, indeed, still lagging behind and there is much more room for improvement. That is why

we rated Q2 on level 2. Nevertheless, the differentiation within the category of SMEs had to be made explicitly. Apart from Q2, the crucial question remains unaddressed by the questionnaire: how to nudge the diverse group of SMEs to more cybersecurity? Rather than overburdening them with even more legal obligations and compliance restrictions, SMEs would highly profit from making IT-security a C-level responsibility. That's why raising awareness remains a key priority for making SMEs cyber secure across Europe. In addition, and instead of redundant structures, SMEs need clear guidance – especially in an emergency. So ENISA should make sure that SMEs across Europe have a clear understanding of whom to contact under which circumstances. If a Member State cannot provide such efficient and transparent structures, there should be a last resort point of contact at European level. Cyberattacks that go undetected due to inefficient governmental structures should not pose a risk to other Member States.

Technological advances and new trends (1.c.)

We all know very well that innovation cycles in the field of technology are rather short and that the breakthrough potential of new ideas can hardly be envisioned beforehand. That is why it is crucial to give recent technological advances and new trends enough regulatory leeway. Any update of the EU cybersecurity policy is recommended to not aim too high and to better step back from introducing new forms of regulation before a technology has indeed proven to be of significant economic, political or societal importance.

Added-value of EU cybersecurity rules (1.d.)

We strongly support the Commissions statements that common cybersecurity rules at EU level are more effective than national policies alone and thus contribute to a higher level of cyber resilience at Union level. We also support its position that "all entities of a certain size providing essential services to our society should be subject to similar EU-wide cybersecurity requirements" (Q1). However, we would like to be more precise and point to the unspecified wording "of a certain size". The specification of such critical size must follow scientific recommendations and should not be determined arbitrarily as we would then run the risk of overburdening small companies with a bunch of security requirements that those firms are unable to comply with, simply due to insufficient manpower and a lack of financial resources.

Sectoral scope (1.e.)

We generally support an enlarged definition of what is seen as the European critical infrastructure baseline. However, as already mentioned before, any expansion and harmonization must be guided by scientific reasoning and should not be the outcome of mere political interests.

In the German case, the government is planning to introduce "disposal" as a new sector of the critical infrastructure. From our point of view, the decision to consider "disposal" additionally as a critical sector, is reasonable. However, we would appreciate that any extension of the scope of essential services / critical infrastructure is done at the European level to foster the harmonization of the Digital Single market and to avoid any form of market distortion. At the same time, the harmonization between the Member States based on a cross-border consultation process should give national authorities enough freedom throughout the identification process so that national and sectoral specificities can be taken into account. When it comes to OES, the methodologies to identify operators and thresholds should be clear, transparent and comparable. Irrespective of whether the identification process is carried out by the competent authorities of the member state themselves or as part of a self-identification, OES should be able to verify whether they meet the requirements or not.

Closely linked to the aforementioned point is our recommendation that the discussion should not only focus on the mere extension of what to consider as critical infrastructures, but also what to exclude from it. This also refers to the change in wording during the ongoing Covid-19 pandemic. The public discourse has been marked by a different, sometimes misleading, understanding of critical infrastructures. The term was less seen under the aspect of what is worth protecting but more under the aspect of what has to function and to be maintained. That is why we recommend to stay focused on cyber threats within the scope of the NIS Directive and to not confound the maintenance of supply chains with the criticality of the IT to ensure the supply of a good or a service. The process of the NIS-Review should be viewed and thought through from the latter point of departure. As the Roadmap also touches upon Covid-19, the Commission should stick to clear definitions and avoid any (scientifically) unjustified inflation of what to consider as critical infrastructure. Such impulse-guided scope expansion would only lead to even more fragmentation in the aftermath of the global health crisis.

In tangible terms, we support the inclusion of the following sectors within the scope of the Directive due to their exposure to cyber threats and their importance for the economy and the society as a whole:

- Public administration (first and foremost)
- Chemicals
- Waste Water
- Data centers
- Culture and Media

But again, any extension of the sectoral scope must be guided by the predominant maxim to harmonize the regulatory landscape at the European level. Any redundant security and reporting requirements across legislation at national and European level must be ruled out. With respect to social networks, we would like to add that, from a KRITIS auditor's

point of view, social media has no influence on the critical service of a KRITIS operator. That's why social networks are not covered under §8a BSIG and are neither addressed in any of the B3S nor in the so-called BSI "Grundschutz-Kompendium".

Regulatory treatment of OES and DSPs by the NIS Directive (1.f.)

From our point of view, the current understanding of DSP is sufficient to balance the need for above-average cybersecurity requirements with the necessary 'light-touch' to give enough room for innovation. As recognized by the NIS directive, there are fundamental differences between OES and DSP, which is the reason why DSP are subject to different rules (Recital 57). The security measures for DSP should be lighter than those for OES. DSP should be free to define how they ensure the protection of their network and information systems appropriate to the risks presented. The security measures should be process-oriented and focus on risk management. They should not require that ICT products have to be designed, developed or manufactured in a particular manner (Recital 51). Such distinction should be maintained as the reasons for applying the different rules remain valid. If the Commission would still opt for an extension or a changed definition of what constitutes a DSP, empirical analyses and research with consultations from industry and other relevant stakeholders must be made the prerequisite.

Sub-section 1.g. – Information sharing

In general, we strongly welcome the exchange of the CERTS and consider their dialog as required and desirable for strengthening cyber-resiliencies in the EU. However, we do not see the need to introduce any additional tasks neither for the Cooperation Group nor the CSIRTs network. Instead of extending responsibilities and information duties, the focus should be put on improving the quality of already assigned tasks in the first place. When it comes to the involvement and influence of secret services, we take a critical stance and reject any secret transmission of discovered vulnerabilities without informing manufactures. Such behavior would undermine trust and security on a broader scale and runs counter to the objective of improving the security of information systems as unpatched systems pose a threat to cybercriminals.

Section 2: Functioning of the NIS Directive

In the light of the past experiences of our membership and in line with the findings of the OLS report, we strongly recommend to make the persisting communication bottlenecks the centerpiece of the NIS-Review. Instead of enforcing legal compliance by means of new legal measures, we encourage a closer cooperation between the Commission, the EU Member States and the private sector. To this end, the Commission is asked to consider the broad range of impactful and promising German public-private initiatives that have been already put in place. Most notably, the alliance for cybersecurity, launched by Bitkom

together with the Federal Office for Information Security (BSI) in 2012, and the UP KRITIS may serve as European role models to enhance the cross-border information sharing and to strengthen the cooperation mechanisms of the member states in the area of network and information security.

Resolving communication impasses is not only of utmost importance for addressing shortcomings and inconsistencies of the past. New communication bottlenecks are looming and must be consequently addressed in a proactive manner by the Commission – in close consultation with the member states – already at this stage of the consultation period. If not properly addressed, we run risk of introducing new inconsistencies, negative feedback loops and fragmentation while actually striving for European harmonization. With this, we refer primarily to two core aspects. First, we face the simultaneous revision of the German IT-Security Law and the NIS-Review. Second, the revision of the NIS Directive comes along with an unexpected parallel update of the European Critical Infrastructure (ECI) Directive 2008/114/EC.

National strategies (2.a.), national competent authorities / bodies (2.b.) & level of discretion on transposition and implementation given to Member States (2.g.)

In Accordance with our responses in the first section, we are convinced that common objectives set on EU level are highly relevant for the adoption of national strategies on the security of network and information systems in order to achieve a high level of cybersecurity. As the evolving cybersecurity landscape requires European harmonization at the upper benchmark, additional elements that are so far not listed in the Directive are to be included for all Member States. At the same time, national particularities must still play an important role and any new legislative proposal must follow the principle of subsidiarity. We also call for the strengthening of the neutral advisory function by public institutions, especially for SMEs.

As our responses in subsection 1.b. (Q1-Q10) indicate, any reviewed NIS Directive must tackle the persisting communication bottlenecks**.** A bunch of tasks and responsibilities has already been assigned to national authorities and bodies. Rather than introducing new areas of work, the focus should be on improving the performance of the tasks and responsibilities that are already put in place. A potential way forward could be a closer cooperation between the Commission, the EU Member States and the private sector. Separately worth mentioning is Q10 as two questions are merged into one. While the level of consultation and cooperation between competent authorities and SPOCs works rather well in Germany, the level of consultation and cooperation between relevant national law enforcement authorities and national data protection authorities needs further improvement and streamlining.

Identification of operators of essential services and sectoral scope (2.c.)

With respect to Q2 we would like to highlight that harmonized definitions are necessary to ensure consistent and uniform implementation and application of legislation. Currently there is a lack of clarity regarding the NIS Directive and its transposition. For example, even basic terms such as information system and security of an information system differ between EU directive and national transposition in the BSIG (BSI Gesetz). We cannot overemphasize the importance of European harmonization. Concerning our response provided for Q4 (How has the level of risk of cyber incidents in the different sectors and subsectors covered by the NIS Directive evolved since the Directive entered into force in 2016?), it is worth highlighting that we see a significant increase in risk across all sectors and subsectors, with a very significant increase in the health and banking sectors. This is a remarkable finding. At the same time, however – speaking only for the German case – we also evaluate the cybersecurity resilience as high across all sectors when compared to other European counterparts (Q5). From our point of view, there is a certain correlation between increased risks in the cyberspace and ramping up cyber-resilience across sectors in Germany. Put in a nutshell, higher degrees of connectivity and reliance on networks go – on average – hand in hand with higher cybersecurity resilience. One should always keep in mind that the protection of networks and systems against any form of disruption is in the innermost interest of OES (and DSP).

As before, a differentiation has to be made with respect to small companies and medium-sized companies (Q6), whose cyber resilience and risk-management practices are – on average and of course with several exemptions – worse. The problem is often related to the following circumstance. IT security must not lie uncoordinatedly in the hands of many (or nobody) nor must IT security be considered as purely technical security that only the IT department takes care of. Organizational and personal security in the company must be considered at all times. This requires a central area of responsibility at management level, where IT security priorities are set and budgets are channeled accordingly. In a nutshell: security belongs on the executive floor. This is the only way to promote a holistic security culture throughout the company and to establish robust IT security management. This holds true for all sizes of companies but is even more relevant for SMEs.

Besides, it is always important to have some sort of prioritization in mind when talking about critical infrastructures and start thinking correspondingly. Power failures are the most serious issue as it directly affects communication technology, which can be thought of as the subsequent most important infrastructure that has to be kept running. As these industries are already heavily regulated, one has to think twice before extending the scope of what to consider as critical infrastructure. Otherwise we would run the risk of not only introducing counterproductive double regulations but also losing the track of what our key infrastructures are, that have to be covered by the NIS. If a specific topic is addressed by both the NIS Directive and sector-specific regulation, preference must be given to the

latter. More precisely, for already heavily regulated sectors the "speciality principle" should be applied (special rule > general (NIS) rule).

We are well advised to stay focused on cyber threats within the scope of the NIS Directive and to not confound the maintenance of supply chains with the criticality of the IT to ensure the supply of a good or a service. The Covid-19 Pandemic has blurred the lines to some extent. Our recommendation is to not confuse the criticality of a good (supply) with the criticality of the IT for providing / producing it. The NIS Directive has to keep its focus clearly on IT-security. So the question is: does the degree of connectivity in a sector equal the level of criticality that justifies incorporation within the scope of the NIS Directive?

When it comes to Q7 and the question whether the level of resilience and the risk-management practices applied by companies differ from sector to sector for small and medium-sized companies, we would like to add that SMEs, in particular those with a higher IT affinity or a high need for coordination, such as tax advisors or industrial production, make greater use of IT. As a result, these SMEs are more likely to be sensitive to security issues, as IT security is important for securing their business activities.

Digital service providers and scope (2.d.)

Besides the need to further harmonize security requirements and incident notification requirements at the EU level, we do not see the need that would justify the decision to step back from the “light touch approach” towards a more regulated approach for DSP under the NIS Directive. The reasons are manifold. First of all, due to their cross-border nature, DSP indeed require a much more harmonized regulatory regime than OES do. Furthermore, innovative micro- and small enterprises should not fall under the European jurisdiction as this would overburden them with regulatory compliance requirements. One also has to admit that these enterprises do not unfold a significant impact on the functioning of the economy and society as a whole on a comparable scale as OES do. Most important, is the fact that online marketplaces, online search engines and cloud computing services do score high or very high when it comes to the level of cybersecurity resilience. To give an example, there are numerous security requirements catalogs for the cloud, like the BSI C5, that are embraced by DSP to demonstrate high security standards. For DSPs, IT-security has already become the decisive competitive advantage, nudging entire sectors to higher cyber-resiliencies. All this happens without additional or even punishing legislative measures.

Security requirements (2.e.)

As Q4 correctly highlights, several Member States have enacted very detailed requirements featuring a higher degree of prescriptiveness. While binding commitments can help to achieve a high level of cybersecurity harmonization in the EU, we remain rather cautious with respect to a high degree of prescriptiveness, simply in terms of practicability. Similarly, pouring out detailed security requirements over heterogeneous sectors will not lead to the desired outcome. In any case, and apart from potentially insignificant effects on the security of network and information systems, this can have severe financial consequences for OES and DSP alike. Companies need flexibility to manage their own risk. That's why we are strongly in favor of risk-based approaches as they allow efficient use of resources, depending on the circumstances and needs of an enterprise. Legislation must leave enough space so that each company can follow its own tailored risk assessment. It would be very much appreciated if the ENISA / Commission could specify – in a transparent and precise fashion – its understanding of adequate risk management under a revised NIS Directive. Such guidance would be of particular importance and high value to SMEs. In addition, we recommend introducing some sort of trustworthy feedback-mechanism for SMEs in such a way that SMEs can submit proceedings and proposals of how they intend to comply with respective standards and regulations. ENISA could then provide tailored and risk-based assistance. Such cooperative basis would be much more effective than following a mere penalizing approach. The latter would only increase the uncertainty for SMEs.

At the same time, a reasonable degree of prescriptiveness and certain rigid regulations can help to align security requirements for OES and DSP across Member States. In the German case, the IT Security Law from 2015 introduced reasonable technical and organizational measures for OES to manage the risks posed to the security of their network and information systems. Security-by-design and security-by-default can be thought of as a promising – and not lowest – common denominator on which risks can then be managed on a case by case basis. In order to enable companies, and especially SMEs, to comply with legislation, they need appropriate technical guidance, implementation checklists and easy-to-implement reporting requirements.

Another question in this subsection is whether companies should be required to use certificates in order to demonstrate their compliance with the NIS. While we are clearly in favor of certification, we reject the idea of introducing mandatory certification requirements or prohibiting the general use of uncertified components on a broad scale. There is a distinction between certification and the provision of evidence. Providing evidence may be useful but not in form of a one-dimensional certification obligation. Any form of legally enforced mandatory certification would run counter to the logic of how companies operate on national, European and international markets. That's why national, European and international certification schemes must be valid, usable and recognized by the NIS. From our

point of view, voluntary certification is found to be the best way forward. It gives companies the necessary leeway but also allows different companies to position themselves in various niches on the market.

Incident notification (2.f.), Information exchange (2.i.) & coherence of the NIS Directive with other EU legal instruments (2.k.)

Incident notification should be made a focal point of the NIS review. So far, we face highly inefficient, redundant and non-transparent reporting structures across sectors. Nobody wants to report too much, but too little is punishable. In addition, different entities follow different time constraints. This makes it even more confusing for companies to report the required information to the responsible entity before the respective deadline. Instead of reporting each and every port scan, incident notification requirements should also follow a risk-based and priority-driven approach. More reporting to even more stakeholders will not automatically lead to more security.

Closely related to our demand of improving incident notification procedures, we consider a more coherent European legislative landscape as central for an updated NIS Directive. Legal amendments must overcome the persisting – and partly conflicting – overlaps with the reporting obligations of the GDPR, the eIDAS and the PSD2. Taking the financial sector as an example, we are confident that persisting fragmentation can be overcome by aligning timeframes for reporting, requirements for reported information (common thresholds, formats) as well as addressees for reporting cyber incidents. The Commission should also work further on the development of consistent and clear definitions. The NIS Directive contains some not clearly defined legal concepts such as “significant” or “substantial” impact, “appropriate and proportionate technical and organizational measures” while no references are given to international standards, for instance, for a greater clarity. Overlapping security requirements with the ECI Directive should also be overcome through explicitly stating the differences between both Directives in achieving critical infrastructure protection. Having said all that, we consider the NIS review as the perfect opportunity to streamline the inefficient, redundant and non-transparent reporting structures of the past.

Another crucial – but so far neglected – aspect is the importance of understanding information sharing not as a one-way street. Any type of feedback loop towards the companies – and possibly to the broad public – to showcase what has been achieved with the data, would be appreciated. The more detailed and including qualitative effects of said data-collection, the higher the awareness and the acceptance in the stakeholder groups to contribute. During the past year, many of our members discovered vulnerabilities and reported them to federal authorities. Unfortunately, many OES never received any kind of feedback. Even if it sounds ridiculously simple, a mere “thank you” or a response like: “*Thanks to your reporting we were able to prevent this or that serious emergency from hap-*

pening and it was extremely important that you informed us about your discovery" can do wonders. In the same vein, it is counterproductive when an entity that voluntarily shares information about vulnerabilities with federal institutions is contacted over and over again to provide further details. That does not really incentivize OES nor matches the spirit of the regulation.

Section 3: Approaches to cybersecurity in the European context currently not addressed by the NIS Directive

Although we are well aware of the fact that cyber-related issues are not yet fully congruent with all (physical) threat vectors to critical infrastructures, the division into IT and physical security is becoming increasingly blurred. This development is likely to continue in the years to come. In the context of critical infrastructure protection, we encourage the Commission to understand cybersecurity also as a means to an end for safety. Subdivisions based on the motivation of the attackers are irrelevant in most cases. It makes no difference whether an attack on critical infrastructure is launched by an economically oriented cybercriminal, a governmental organization or a terrorist. They use the same procedures and affect ultimately the same objectives to which we are committed (business continuity, readiness for response / resilience, better prevention). Furthermore, the orientation by sectors and funds is not necessarily appropriate. Attacks are also launched against processes and procedures without any particular technical reference. Future legislation should take this further into account. The security of networks and systems can only be achieved holistically. Technology, organization, and the human factor must be included and also reflected in the laws. What is needed is a European harmonization of the sectors included and of the requirements (general and sectoral). This remains difficult to convey to a regional and sectoral structure of authority.

Provision of cybersecurity information (3.a.)

Building upon our explanations in the previous section, we would like to be more precise at this point and provide more detailed aspects of how the exchange of cybersecurity information may be improved:

1. After having reported cybersecurity information on a voluntarily basis there should be no additional overhead for the reporting company. Although it may be reasonable to ask for further details, the bureaucratic costs have to be limited to a minimum.

2. Breaking rigor and time-consuming hierarchical reporting structures. The responsibility cannot be put in the hands of the reporting entity or person. Authorities must take over the responsibility at an early point of time and trigger well-

defined internal procedures following efficient flows of information. So far, public entities lose valuable time due to long internal reporting mechanisms.

3. Establishing a give & take principle. Reporting must not go one way into a black hole. There has to be a certain feedback culture.

4. Mutual trust is the basis for productive cooperation between the authorities responsible for IT security and the business community. Companies must be able to rely on the fact that their constructive cooperation to achieve the highest possible level of IT security will not be used elsewhere to achieve other security policy goals. This trust can be established if the authorities responsible for IT security act with the greatest possible autonomy.

Vulnerability discovery and coordinated vulnerability disclosure (3.c.)

Unfortunately, European vulnerability disclosure procedures are hardly visible or effective. The lack of functional European vulnerability disclosure policies must be addressed during the review process because the effectiveness of such policies is indisputable. However, the way how the Commission addresses the question leaves too much room for interpretation. In Q4, the wording "national authorities such as CIRTSs" could also refer to secret services and it is left unaddressed to whom the vulnerabilities are reported. Vulnerability discovery and coordinated vulnerability disclosure must be footed on a trustworthy basis. Hence, there can hardly be an active involvement or cooperation with secret services. If the Commission foresees any hacking by governmental agencies, we have to negate such intents. If the Commission seeks to improve trustworthy coordinated vulnerability disclosures, we are clearly in favor of such efforts. In any case, national authorities should not be allowed to take proactive measures. Instead, OES / DSP should submit and share information about discovered vulnerabilities proactively.

Security of connected products (3.d.)

The basic premise for ensuring a high level of cybersecurity across Europe is that all relevant stakeholders – OES / DSP, HW / SW manufacturers as well as regulators and policy-makers – work together on a trustful and cooperative basis, assuming their respective responsibilities within the ecosystem. One hand must reach into the other, because the dangers in cyberspace start at the weakest link in the chain. A fair burden sharing for security and risk management of the digital economy in the EU must be ensured and all actors in the digital value chain should contribute to this. We support a common minimum safety level and see the need to evenly regulate the digital value chain, including basic security requirements such as 'Security by Design' for critical products. We believe

that the New Legislative Framework rather than the NIS Directive is better suited to for connected devices. Networkable products that include Consumer IoT, Enterprise IoT, Healthcare IoT and Manufacturing IoT products would be better regulated following well-established and proven mechanisms for market access using the New Legislative Framework (NLF) approach with CE marking. There is already a bunch of regulation in place so that we have to highlight once more that European harmonization must be the prerequisite of any legal amendments. When asked for common EU cybersecurity rules it remains an open question who will be responsible for monitoring and enforcing such new rules. Legislation should define a horizontal phenomenon directive for cybersecurity specifying mandatory minimal cybersecurity requirements defined by harmonized European standards. In any case, the establishment of legal certainty must be of utmost importance.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.