cecimo

European Association of the Machine Tool Industries
and related Manufacturing Technologies

POSITION PAPER

Directive on Security of Network and Information Systems across the EU

Brussels, 17 May 2021

INTRODUCTION

Network and Information Security Directives (NIS1 and NIS2)

The 2016 Network and Information Security Directive (NIS1) was the first European piece of legislation in the field of cybersecurity. The specific aim of this legislation was to achieve a high common level of cybersecurity across all Member States, by increasing their capabilities to protect critical infrastructure. Nevertheless, its implementation proved difficult over time, leading to fragmentation at the national, legislative, and supervisory level across Europe's internal market.

In response to the growing regulatory fragmentation within the European Union (EU), and the increasing threats posed by the surge in cyber-attacks experienced in recent years, a revised proposal of the Directive (NIS2) was submitted, on 16 December 2020, by the European Commission to expand the regulatory scope of the NIS1 Directive. The NIS2 Directive was proposed under the EU Cybersecurity Package, which is an important part of the EU's digital transformation and recovery efforts. The scope of the NIS1 Directive was expanded to strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce stricter supervisory and enforcement measures, with the aim of increasing the level of security throughout Europe in the longer term.

CECIMO, representing the machine tool industry and related manufacturing technologies, believes that the NIS2 appropriately addresses the need for harmonization at the European level and for an EU-wide uniform approach. Most importantly, the proposed Directive correctly integrates the suitable and appropriate measures needed to increase cyber resilience in industrial supply chains, given their criticality for Europe's economy and society. In this regard, CECIMO fully supports the overall policy approach and security objective of the NIS2 proposal, particularly as it seeks to tackle cybersecurity risks in supply chains.

Regulatory Scope of NIS2 Directive: Impact on Manufacturing SMEs

Despite CECIMO welcoming the NIS2 Directive's overall policy approach and security objective, we believe that its regulatory scope could negatively affect more than 1,500 machine tool manufacturers operating in Europe, over 80% of which are small and medium-sized enterprises (SMEs). Under the NIS2's provisions, manufacturing SMEs would become subject to measures that were originally targeting a limited group of critical business entities (Essential Entities), which were independently selected by the Member States. Adhering to these measures would require considerable efforts and resources, particularly for the smaller manufacturers, whom would have to bear a significant regulatory burden that could potentially stifle their growth.

Compliance Costs

By expanding the scope of the 2016 Directive (NIS1) to include "Important Entities" (IEs) as well, the NIS2 could potentially create a significant economic burden for machine tool manufacturers, as these would be subjected to additional measures that were previously strictly assigned to "Essential Entities" (EEs). The resulting additional measures would undoubtedly raise compliance costs considerably, especially for companies situated at the lower half of the size spectrum (< 250 employees), which would hardly be able to withstand the additional costs arising from the payroll of the compliance experts, the regulatory reporting costs, and the implementation of internal cybersecurity measures at the firm level.

Aside from the cost-related aspects of compliance, the scarcity of cybersecurity experts on the labour market combined with their rising demand would pose another major compliance challenge as it would intensify the competition among manufacturers to access a very limited pool of specialists. This would largely go to the detriment of SMEs, considering the limited economic resources at their disposal and their lower capacity to attract human capital, relative to the larger manufacturers.

Henceforth, based on the increased compliance requirements and the resource constraints of manufacturing SMEs, CECIMO questions the proportionality and feasibility of the NIS2 proposal given that its "breadth and depth" of intervention is maintained. As a matter of fact, CECIMO expresses a strong desire to restrict the proposal's regulatory scope to exclude SMEs (< 250 employees) altogether, which in our view would not compromise the overall security level of the European machine tool manufacturing sector.

Essential vs. Important Entities

The most critical aspect regarding the scope of NIS2 is the lack of differentiation in the measures applicable to "essential" and "important" entities. The current proposal applies the same requirements to all companies without distinction, whether these are essential, such as key energy suppliers, or important, such as small-scale machine tool manufacturers. As the foreseen criteria to determine companies' classifications remains highly unclear, it can be argued that NIS2's scope could ultimately cover many manufacturing companies that are neither fundamental parts of essential supply chains nor potential security risks for others. Such ambiguity is undesirable for our sector since it does not guarantee legal certainty and thus would make compliance difficult for the manufacturers concerned, with a disproportionate effect towards the smaller ones.

The NIS2 proposal seeks to compensate for this lack of differentiation by adopting a "risk-based approach," according to which the measures adopted for any specific case must be "appropriate and proportional" to the risk presented (Art 17 and 18).[1] Nonetheless, the extent to which this risk-based approach can ensure the necessary case-specific differentiation is highly questionable for the following reasons. First of all, the analysis required to estimate the risks would be too difficult to perform for most SMEs, primarily because of the lack of in-house specialists, experts, and tools available to them. Secondly, determining measures that are appropriate to the risk presented would require close cooperation with the authorities, which is hardly conceivable considering the multitude of manufacturers covered by the NIS2 Directive. Lastly, the notification and reporting obligations (Art 20)[2] foreseen under the NIS2 are far-reaching and entail a significant bureaucratic effort that is unrealistic for the vast majority of manufacturing SMEs.

CECIMO believes that the risk-based approach outlined in the NIS2 proposal does not guarantee a sufficient level of legal and compliance certainty for our manufacturers. A more detailed analysis of what types of manufacturing entities should be considered important is necessary. For these reasons, CECIMO would welcome the establishment of a clearer demarcation line between the definition of essential entities and important entities, thereby ensuring legal and compliance certainty in the application of the NIS2's provisions.

Territoriality

In terms of regulatory scope, the NIS2 should also provide further clarification with regards to its territorial jurisdiction, as we believe that the Directive should strictly apply to all entities that operate within the EU. Particularly in the case of manufacturers, regardless of whether these are classified as "important entities" (IEs) or "essential entities" (EEs), it should be clear that NIS2 obligations should apply to all entities that have manufacturing facilities in the EU. Besides this being a fundamental element of legal certainty, a clear EU-wide territorial jurisdiction also ensures that the internal market does not get distorted by the provisions of the proposed Directive.

[1] Article 17 ("Governance") and Article 18 ("Cybersecurity risk management measures") of the Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.
[2] Article 20 ("Notification of a cybersecurity incident to consumers") of the Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

In addition, the territorial jurisdiction between Member States within the EU should also be subject to further clarifications. The current NIS2 proposal leaves Member States the discretion to define which SMEs are essential or important to their respective economy and society, thereby leading to a high level of legal ambiguity for the SMEs operating across multiple Member States. To improve legal clarity and predictability, CECIMO urges the introduction of clear jurisdiction rules for enforcement, possibly through the main establishment criterion as outlined in the GDPR regulation

Review of the NIS2 Directive: Recommendations

Overall, CECIMO recognizes the guiding principle behind the NIS2 proposal as a suitable and essential step towards achieving a more complete legislative framework on cybersecurity. We fully support the approach of increasing cybersecurity through a collective effort at the European level, also aimed at strengthening the Digital Single Market (DSM).

Nevertheless, we disagree with the horizontal approach outlined in the NIS2 Directive, which applies the same compliance obligations to all companies without distinction. The lack of differentiation in the measures applicable to "essential" and "important" entities could ultimately affect many manufacturing companies that are neither fundamental parts of essential supply chains nor potential security risks for others. In addition, complying with these obligations would require significant resources and efforts, with a disproportionate effect towards SMEs with less than 250 employees. Therefore, we believe that major changes are necessary in order to reduce the burden on SMEs and ensure a correct application of NIS2.

Reducing Compliance Obligations for SMEs

In our view, by including companies with less than 250 employees under its scope, the current version of the NIS2 proposal places a significant compliance burden on a vast number of small manufacturers. Taking into consideration the direct compliance costs, and the challenge of attracting a limited number of cybersecurity expects, the proposed Directive demands sizeable compliance efforts from all companies without distinction. Instead, the compliance obligations contained in the proposal and their depth of intervention must focus on those companies that have "overarching significance for the security of supply chains," in pursuit of a better balance between the cybersecurity measures adopted and the risk presented.

In order to achieve this, the "size cap" for important entities should be based on the EU SME criteria of 250 employees or more. We believe it would be highly feasible to exclude the smaller manufacturers from the NIS2's regulatory scope while guaranteeing the overall security of the machine tool manufacturing sector. This is because manufacturers that fulfil a critical function could still fall within the Directive's scope by applying the criteria listed in Art. 2, regardless of the number of employees. Meanwhile, SMEs classified as "important" would no longer be obligated to comply with the same requirements as large-scale manufacturers operating on a global scale. Henceforth, we strongly advocate for an upward revision of the "size cap" for important entities in the current NIS2 proposal, so that it no longer affects small-scale manufacturers (< 250 employees).

Establishing Legal Certainty

As previously mentioned in this position paper, we deem it inappropriate that the proposal makes no distinction – in terms of obligations – between important and essential entities. The risk-based approach contained in the NIS2 only tackles this problem partially, since the risk assessment outlined in Art 18 ("Cybersecurity risk management measures") and the minimum compliance obligations listed do not eliminate the margin for legal uncertainty. Thus, changes will need to be made to reduce the burden on non-essential entities, particularly the SMEs that do not serve a critical function, so that the Directive exerts an adequate level of proportionality, and most importantly, legal certainty.

In this regard, we encourage the introduction of a new classification method based on a narrower definition of "important entities" that focuses strictly on the "manufacturing of critical products." The current method classifies companies according to the EU's Statistical Classification of Economic Activities (NACE Code), which does not accurately reflect the risks that a company poses to the general public, neither in the sense of cybersecurity, nor in the sense of overall economic resilience. The obligations outlined in the proposal should focus on manufacturers that have an "overarching significance" for the functioning and security of supply chains. To achieve this, there would need to be in-depth supply chain risk assessments that carefully examine the role of manufacturers in their respective supply chains, and ultimately determine whether these affect the cybersecurity and resilience of any essential entities. In our opinion, this would lead to significant relief for all the entities that are not involved in the manufacturing of critical products, most of which are small-scale manufacturers, while ensuring greater proportionality and legal certainty in the application of NIS2.

Along with reducing the obligations of non-essential entities, we believe that the Directive should also provide a set of corresponding support measures to facilitate compliance. To begin with, it is vital that the NIS2's increased compliance obligations are matched by the "timely" creation of sufficient capacity on the side of public authorities and service providers. The necessary investigations are hardly feasible for SMEs without adequate financial and human support, and thus should be sustained by the competent authorities, especially in cases of "significant threats." On top of this, we strongly call for the development of EU-wide harmonized methodologies to carry out risk assessments, with the hope that this can provide guidance for all companies, and finally guarantee proportionality and legal certainty in the application of the proposed Directive.

Conclusion

In conclusion, CECIMO believes that the objectives and principles of the NIS2 Directive are fundamentally correct, but the proposed measures require considerable resources and efforts that would inevitably penalize smaller manufacturers. By restricting the regulatory scope of the NIS2 Directive and easing the obligations for important entities, the regulatory burden for SMEs could be reduced without compromising the overall security level of the European machine tool manufacturing sector.

About CECIMO

CECIMO is the European Association of the Machine Tool Industries and related Manufacturing Technologies. We bring together 15 national associations of machine tool builders, which represent approximately 1500 industrial enterprises in Europe (EU + UK+ EFTA + Turkey), over 80% of which are SMEs. CECIMO covers 98% of the total machine tool production in Europe and about 33% worldwide. It accounts for more than 150,000 employees and a turnover of 19,7 billion euros in 2020. More than three quarters of CECIMO production is shipped abroad, whereas half of it is exported outside Europe.

Contact

Damir GLAS, Head of EU Affairs and Communications, damir.glas@cecimo.eu

Stefano RAMUNDO ORLANDO, Policy and Project Assistant, intern@cecimo.eu