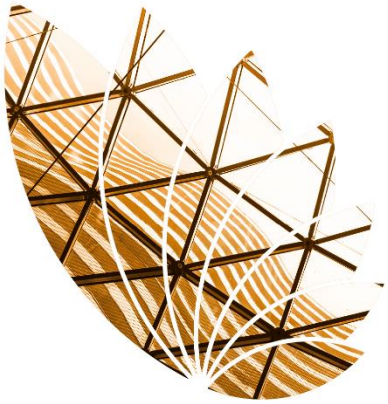
IDEAS IN FOCUS



HARMONISED APPROACH TO CYBERSECURITY – THE HOLY GRAIL OF THE EUROPEAN UNION

Joanna Świątkowska[*]
December 2019

"We are as strong as the weakest link." It is probably one of the most overused phrases in cybersecurity-related debates. This obvious statement, however, takes on special significance in the EU where harmonisation of national policies is a driving approach. But is it feasible, given the 28 different institutional structures, cultures, interests and threat perceptions? A closer look at the experiences with the implementation of the NIS Directive and the ongoing discussions to develop joint standpoints regarding 5G deployment in the EU offer some preliminary answers.

NIS Directive

The harmonisation of the Directive's implementation can be assessed on the basis of experiences and existing data. Among the most crucial elements of the first EU regulation on cybersecurity was the identification of operators of essential services (OES) – entities which play a critical role in Member States' economies and security systems. As these operators often provide services internationally, their business continuity has cross-border significance.

In October 2019, the European Commission published a report that assessed the consistency of the Member States' approaches in OES identification. Even though the Directive assumes a minimum harmonisation approach and allows the Member States to take some liberties while implementing it, significant discrepancies in applying key provisions may impede the main goals of the Directive.

The report's conclusions bring some alarming news. Methods applied by various countries often differed and led to significant inconsistencies. According to the report, the main areas of inconsistency included: different approaches in drawing up lists of essential services, different application of the thresholds and different application of the *lex specialis* principle.

Proper and internationally harmonised OES identification serves as a foundation for further actions that decide the success of the Directive. Once identified, operators are obliged to introduce appropriate security measurements and report incidents. Additionally, a consistent, EU-wide approach increases the chance of a proper and effective reaction to a crisis. It is also important for internal market unity.

Significant differences in the OES identification processes occur despite the existence of mechanisms that are supposed to help coordinate the approaches. The above-mentioned report proposes certain solutions to the problem, pointing out that the NIS Cooperation Group and consultancy mechanisms included in the Directive must be used more. Before applying the cure, however, one must give the proper diagnosis. We need to learn lessons from the difficulties identified at this stage. More practical solutions, such as supporting guidance, should also be offered to the Member States. For instance, the incorrect application of the *lex specialis* is worth looking into. The frequency of this error may suggest that the application of sector-specific rules should be revised - or perhaps existing sectoral security solutions are insufficient.

As for their reluctance to use the cross-border consultation procedure, some countries expressed reluctance to share information due to uncertainties with communication channel security. While that may be true, the question remains whether trust issues are

[*] This paper is produced in the framework of the EU Cyber Direct project funded by the European Union. The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author.

not another problem that discourages entities from exchanging information.

All of these aspects must be analysed in the context of future iterations in OES identification processes, as well as in the context of a possible extension of the Directive into other sectors. It is important to better tune the existing mechanisms, i.e. consultations, NIS Cooperation Group engagement and guidelines. But the core of the solution is to increase Member States' awareness that it is in their own interest to coordinate their actions better and that they must do so in the best way possible. The task for EU decision-makers is to hone all tools that may make the NIS Directive implementation process more effective.

5G – cybersecurity litmus test

5G rollout-related issues seem to be one of the most stirring elements of public, political and media debate today. In order to analyse, understand and minimise multidimensional risks that the next-generation network development process poses, the European Commission decided to mobilise efforts to unite mitigation strategies. The first step in the process was to aggregate national risk assessments that cover analyses of the 5G-related status quo and considerations on the threat landscape. A high-level report published in October 2019 summarises the most important outcomes. Based on this report, the NIS Cooperation Group is engaged in the preparation of a toolbox that will contain possible risk mitigation measures.

An analysis of the EU report's conclusions allows us to make some assumptions regarding the direction in which the toolbox measures might be headed. It is clear that the mobile network operators that "have a central, decision-making role" in the context of overall network security will *de facto* become the front line for the implementation of cybersecurity obligations. It is expected that operators will be tasked with special responsibilities related to security measures, for instance, to make sure their subcontractors meet relevant security criteria. Another set of proposals will probably be oriented at actions to assure supplier diversity at the national and EU level. Both of those obligations may cause severe difficulties for countries' bilateral economic and political relations.

Of course, it remains to be seen which mitigation strategies will be included in the toolbox. Nevertheless, it is obvious that their success depends on whether they are implemented cohesively across the entire bloc. Lack of harmonisation may lead not only to significant market fragmentation but also a decrease in security measures' effectiveness. It would also weaken the whole Union politically and would raise questions about the credibility of the whole organisation.

Similar to the NIS Directive's implementation, the second aspect that must be analysed is the choice of concrete measures for implementing the toolbox. Here, some serious questions arise. The NIS Cooperation Group is the platform for joint action on security, though at the moment it mainly pertains to areas covered by the NIS Directive. Meanwhile, the discussion about the telecom sector falls out of the NIS Directive's scope. The question remains as to whether the EU should start debating the activation of other possible tools, such as a regulatory framework for electronic communications networks and services.

However, this may be difficult for larger aspects related to cybersecurity like telecommunications law. Regulations, if designed properly, can bring positive and necessary changes not only to the security environment but also to the market. There will be no fully functional Digital Single Market without trusted "end to end" digital infrastructure.

All for one, one for all?

Harmonisation of practical steps, procedures, and finding suitable tools for common problems is an ambitious goal. In the context of cybersecurity, the foundation of success is to understand that acting in silos or without a basic common approach will waste the efforts of all. No Member State can achieve its goals if the strategic security foundations of the EU on the whole are shaky. As the case of the NIS Directive shows, decision-makers must invest in learning and trust-building mechanisms as a precondition for effective outcomes.

Similar conclusions apply to the debate over 5G. The way the EU manages the risks related to the next-generation network development will determine its security and economic prosperity for years to come. As the preparation of the EU coordinated risk assessment report showed, there is a general understanding that threats pose multidimensional challenges. Yet the key question is whether countries are able to agree not only on the diagnosis but also on the remedy, perhaps putting certain bilateral deals at risk and exposing themselves to further difficult decisions. The upcoming toolbox needs to propose concrete actions to achieve coherence across the EU. This will be a true test of unity and a clear signal of the EU's importance in the cybersecurity ecosystem.

Dr. Joanna Świątkowska *is the Programme Director of the European Cybersecurity Forum and Senior Research Fellow of the Kosciuszko Institute.*