To what extent is the EU's cybersecurity framework coherent? Coherence, defined as a shared understanding of security and institutional cooperation in the scope of this paper, has been a vital objective in developing European cybersecurity. Even though the EU has placed significant emphasis on the development of coherence in its cyber domain to ensure a consistent response between national actors during cross-border attacks, few studies have attempted to evaluate the coherence of the policy area. Moreover, few to none have focused on the Directive on security of network and information systems (NIS Directive), the first and only EU-level legislation intended to improve national capabilities and enhance cross-border collaboration. In light of this, the purpose of this study is to fill a gap in the academic literature by focusing on the implementation of the NIS Directive by the Member States and studying its effect on the coherence of European cybersecurity. To do so, it employs qualitative content analysis to examine the impact of national cybersecurity strategies and operators of essential services as part of the Directive's implementation on the shared understanding of security and institutional cooperation. The research finds that while most Member States tend to have a shared understanding of cybersecurity, the flexibility of the Directive has led to inconsistencies between the Member States, weakening institutional cooperation and coherence of European cybersecurity. In light of the ongoing development of the NIS2 Directive, this paper urges policymakers to address the flexibility in the new version to ensure institutional cooperation between Member States in the protection of networks and information systems.