BDI

POSITION | SECURITY POLICY | EU STRATEGY 2025

European Internal Security Strategy

German industry's call for an integrated approach to enhance Europe's resilience by strategically cooperating with industry.

March 12, 2025

The Russian war of aggression against Ukraine as well as other current geopolitical developments require Europe to significantly adapt its security policy. Every day, Europe is the target of digital, hybrid and physical attacks – both from criminal and state actors – without officially being at war. Security cannot be guaranteed by the armed forces and security authorities of EU Member States alone. Rather, security encompasses the entire resilience of the state, economy and society. This also includes securing the supply with critical services and uninterrupted value chains – and therefore, also protecting companies from attacks, whether digital or analogue.

Europe's current security architecture is based on an outdated dual concept: internal and external security, war and peace, digital and physical. The EU's second Network and Information Security (NIS 2) and the Critical Entities Resilience Directive are good examples of this outdated understanding. Rather than providing for an integrated security concept, these directives artificially separate the protection against digital and physical threat vectors. This model does not reflect the hybrid threat situation in which we find ourselves today – and which requires an integrated security strategy. When drafting its European Internal Security Strategy, the EU Commission must overcome this duality and must focus on cooperation. Cooperation between the EU Member States, the EU and its international partners as well as between industry and public institutions – both at EU and national level – is paramount.

Fit for purpose? German industry's six recommendations for a holistic European Internal Security Strategy

BDI very much appreciates the possibility to provide input to the European Commission's consultation. The European Commission should consider the following six recommendations when drafting the European Internal Security Strategy:

1. Enhancing Europe's resilience requires implementation rather than strategies
2. Establishing an effective and lean regulatory framework to protect critical infrastructures and industry
3. Involving Europe's industry as a key pillar of Europe's security architecture
4. Providing up-to-date threat information
5. Strengthening the resilience of Europe's digital networks – on land, under water and in space
6. Promoting the long-term resilience of Europe's critical infrastructures and fostering innovation in Europe

Federation of German Industries (BDI) | www.bdi.eu
German Lobbyregister Number: R000534 | EU Transparency Register: 1771817758-48
Steven Heckler (s.heckler@bdi.eu) | **Kerstin Petretto** (k.petretto@bdi.eu) | **Philipp Schweikle** (p.schweikle@bdi.eu)

Table of Contents

In Detail: German industry's six recommendations for a holistic European Internal Security Strategy

Recent geopolitical developments require a comprehensive review and reorganisation of Europe's internal and external security architecture. They stress that a social consensus is required to defend our values and interests against external and internal threats. The digital transformation and the increasing threats posed by cyber-attacks, disinformation, espionage and acts of sabotage – particularly in the context of hybrid warfare – have dramatically changed the demands on how the EU addresses security policy. Isolated adjustments or the elimination of minor flaws are no longer sufficient – they merely conceal the overarching problems.

Enhancing Europe's resilience requires implementation rather than strategies

The first von-der-Leyen Commission's approach to massively introduce new strategies and laws without ensuring that the necessary pre-conditions for a successful implementation were in place, resulted in a lot of paper but only a meagre improvement of the EU's overall resilience against espionage, sabotage and cybercrime. Take the NIS 2 Directive as a telling example: Companies are now required to provide the national competent authority with three to five reports per incident. However, the national competent authority in Germany, the BSI, has not received any additional personnel or funding to implement these requirements. Hence, the European co-legislators massively increased the bureaucratic burden for companies without ensuring that the necessary preconditions for a successful implementation was in place in all Member States as well as at EU-level.

German industry urges the European Commission, the European Parliament and Member States to always ensure – when adopting new strategies and laws – that the resources required to implement new requirements are available. We strongly encourage the European Commission to reduce the number of newly proposed security-related strategies and legislative acts so that they align with the public administration's own implementation capacities – both at the EU as well as the Member State level. Therefore, the new European Internal Security Strategy must be both bold and realistic in ambition.

Establishing an effective and lean regulatory framework to protect critical infrastructures and industry

To augment Europe's resilience against espionage, sabotage and cybercrime, the EU must adopt a holistic approach. Having two separate resilience-related legislative acts, i.e. the NIS 2 Directive and the CER Directive, artificially separates different attack vectors and does not address the increasingly hybrid attack landscape. When drafting the European Internal Security Strategy, the European Commission must closely intertwine all measures related to the protection against physical, hybrid as well as digital attacks. By continuing the artificial separation of responses to these threat scenarios, the EU will not sufficiently increase its resilience. Henceforth, when revising the directives the next time, the European Commission should propose a legal framework that fuses the currently artificially separated NIS 2 Directive and CER Directive. In addition, the co-legislators should streamline reporting obligations and should reduce the overall bureaucratic burden. Not reporting is paramount to enhanced resilience, rather, the EU should focus on practical requirements for prevention, detection and mitigation of digital, hybrid and physical threats.

Under NIS2, companies are subject to the jurisdiction of every Member State in which they provide their services or in which they operate. Ultimately, this means that they are likely to be subject to 27 national laws transposing the Directive, including registration and supervision by the national authorities, and divergence and multiplication of security and incident reporting requirements. In future,

the European co-legislators should ensure a greater degree of EU-wide harmonisation when adopting security-related legal acts. This would enhance Europe's resilience against external and internal threat vectors while at the same time reducing the implementation costs for companies.

Moreover, we encourage the European Commission to streamline its product-related cybersecurity regulations – the Cyber Security Act (CSA) and the Cyber Resilience Act (CRA) partly overlap. The CSA has proven to be not fit for purpose. In the process of drafting schemes, it does not sufficiently involve all stakeholders and their expertise, and it takes too long to draft and agree on cybersecurity schemes. We encourage the European Commission to rely on the CRA for connected products as it provides for horizontal cybersecurity requirements for all products with digital elements. The revision of the CSA should lead to a harmonised regulatory cybersecurity framework for products with digital elements and ITC services, such as cloud.

Involving Europe's industry as a key pillar of Europe's security architecture

Enhancing Europe's overall resilience towards external digital, hybrid and physical threat vectors requires a holistic approach focusing on the rigorous implementation of strategies and laws. To this end, EU institutions and Member States must closely cooperate with industry. In the past, this co-operation was often neglected, which led to inefficiencies in implementation. In future, the development, implementation and further progression of strategies and measures must involve all relevant stakeholders from industry in a structured manner. Industry is both a provider of security solutions as well as a prime target of security attacks, and therefore, has ample knowledge in the prevention, detection and mitigation of security threats. Henceforth, cooperation between security authorities and industry should be strengthened in the day-to-day operations.

It is of paramount importance that the legally defined mandates of security authorities at EU and Member State level incorporate the protection of businesses. Member States and the EU must adapt the allocation of funding and personnel to the new security environment. Henceforth, implementation-oriented authorities, such as the European cybersecurity agency (ENISA), national cybersecurity agencies (e.g. ANSSI and BSI), intelligence agencies and the police, must be better staffed.

Providing up-to-date threat information

Effective protection against threats in the analogue and digital space requires a systematic, continuous and confidential exchange of information between companies and government agencies. Companies rely on information from the federal and state security authorities to better assess risks and repel threats. European security and intelligence agencies must be legally enabled to provide intel to businesses. Although much has been achieved in the last two years, we must continue to work on understanding security as a joint task and acting accordingly. This also includes an improvement of the exchange of information among European security authorities.

One clear objective should be to establish between security agencies and companies that fall within the scope of the NIS 2 Directive and the CER Directive a systematic two-way exchange of information on risk situations. This is the only way to create an up-to-date, free-of-charge situation report on digital and physical threats. It would be even better to include companies from the second and third tier of suppliers to ensure comprehensive prevention along value chains.

To this end, the EU institutions and Member States should elevate the ENISA Single Reporting Platform, to a reporting mechanism where entities can fulfil all their legal reporting requirements emanating from the CER and the NIS 2 Directive as well as the Cyber Resilience Act and the Cyber Security Act. This would significantly reduce the administrative burden caused by the reporting obligations as

companies no longer have to separately file the same incident report in 27 Member States in 24 different languages. Security authorities across the EU should have access to these reports based on the need-to-know principle. Based on the information generated from reporting as well as other sources, ENISA should provide all entities falling within the scope of the before mentioned EU legislative framework with relevant information about current threats and vulnerabilities.

Strengthening the resilience of Europe's digital networks – on land, under water and in space

Digital networks are the backbone of our modern society and economy. Their importance is destined to massively grow in future. Therefore, the resilience of Europe's digital networks – on land, under water and in space – must be an integral part of the EU's Internal Security Strategy. Respective policy proposals must be closely aligned with the upcoming Digital Networks Act and the already agreed EU 5G Toolbox.

On land, digital networks are, on the one hand, a critical infrastructure themselves and, on the other hand, an essential component of other critical infrastructures, such as the energy, transport, and healthcare sectors. A prioritized energy supply for network operators in crisis and disaster situations is, therefore, urgently required. A reliable power supply is the fundamental prerequisite for resilient telecommunications networks, as they depend on electricity. Additionally, resilient supply chains, effective infrastructure competition, and a high level of cybersecurity – particularly through the protection of sensitive information during and after digital planning and approval procedures – are crucial measures that can make attacks on telecommunication networks more difficult or even prevent them.

The need for greater resilience also applies to the submarine data cable infrastructure. As the backbone of global data traffic, these cables are also exposed to sabotage attempts. The recognition of submarine data cables as strategically relevant security infrastructure in the European Commission's White Paper on digital infrastructure, along with subsequent measures such as a joint EU governance framework for submarine cable infrastructure, should be initial steps at the European level to better protect these cables. Given the significance of submarine data cables, further measures, such as those outlined in the recently proposed EU Cable Security Action Plan, must now follow swiftly. The EU must push for the expansion of maintenance and repair capacities, including an increase in the number of available repair vessels. This is crucial to minimise the impact of accidents or targeted sabotage attempts on submarine data cables. Additionally, investments in submarine data cables must be simplified and promoted at the European level to enhance their resilience through redundancy.

Promoting the long-term resilience of Europe's critical infrastructures and fostering innovation in Europe

To enhance the resilience of Europe's critical infrastructures, German industry proposes that the EU co-legislators establish pan-European access criteria based on harmonised risk-based technical principles for components utilised in such infrastructures. Putting EU-wide rules in place – rather than having a hotchpotch of 27 different approaches – would enable vendors of components to benefit from economies of scale.

Germany and Europe are among the leading regions in technological development. To ensure this remains the case in future, maintaining and expanding German and European production capabilities as well as research and development sites is of critical importance. Compliance with ESG criteria or environmental regulations is not sufficiently valued by customers in competitive markets – procurement decisions remain primarily cost-driven. A proper balance must be found between cost efficiency and resilience. However, this must not lead to mandatory regulations for network operators regarding which hardware or components they are required to use.

To counter state and non-state actors exploiting technological innovation for malicious purposes, the EU and its Member States need to increase funding for disruptive innovation research in security. For example, a breakthrough in quantum computing by one of Europe's competitors could have devastating consequences for the EU's critical infrastructures. The innovation gap identified in last year's Draghi report and addressed in the Commission's Competitiveness Compass, must be closed.

Imprint

Federation of German Industries / Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29
10178 Berlin
www.bdi.eu
T: +49 30 2028-0

German Lobbying Register Number R000534

EU Transparency Register: 1771817758-48

Editorial

Steven Heckler
Deputy Head of Department, Digitalisation and Innovation
T: +49 30 2028-1523
M: s.heckler@bdi.eu

Kerstin Petretto
Senior Manager, Security Policy and Defense
T: +49 30 2028-1710
M: k.petretto@bdi.eu

Philipp Schweikle
Senior Manager, Digitalisation and Innovation
T: +49 30 2028-1632
M: p.schweikle@bdi.eu

BDI Document number: D2059