AmCham EU

SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Cyber Solidarity Act

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.7 trillion in 2022, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Executive summary

Cybersecurity is a global issue that should be addressed through value- and asset-based partnerships, not mere geography. Given that cyber threats are not bound by physical borders between countries or regions, a multistakeholder approach to cybersecurity is highly appropriate. The EU's Cyber Solidarity Act (CYSOL) currently prioritises political interests rather than addressing risk-based security interests, as it refers to politically sensitive definitions such as technological sovereignty. This goes against the initiative's objective: reinforce the European Union's ability to fight against the growing global cybersecurity threats and attacks.

The following document presents a set of recommendations and amendments for the implementation of an effective EU CYSOL. These proposals highlight the importance of building capacity through consolidation, leveraging the expertise of global providers, including essential entities under the scope of the Network and Information Security 2 (NIS2) Directive and applying a risk-based approach to the initiative. On top of these, the EU should prioritise engaging with stakeholders from the private sector and deploying state-of-the-art technology and skills to strengthen its detection and response capabilities against cybersecurity risks.

Introduction

In April 2023, the European Commission proposed the EU CYSOL to enhance the Union's capabilities in the detection, preparedness and response to substantial and expansive cybersecurity threats and assaults. The draft proposal encompasses the establishment of the European Cyber Shield (ECS), which is composed of interconnected Security Operation Centres (SOCs) distributed throughout the EU, along with the implementation of a comprehensive Cyber Emergency Mechanism (CEM) to fortify the EU's cybersecurity posture.

The proposed CYSOL is an important opportunity to enhance EU's cybersecurity policy. However, the introduction of politically sensitive concepts like technological sovereignty ignores the global nature of cyberattacks and risks undermining the initiative's potential to achieve a stronger and safer union. In order to strengthen the proposal, the following paper outlines several recommendations and amendments to **improve and further clarify aspects of the proposed regulation**.

Build capacity through consolidation – not isolation

We must focus on building – not cutting off – strategic partnerships to allow access to key cybersecurity technologies. To avoid potential concerns associated with untrustworthy providers, policymakers should focus on real risks while allowing trusted providers to participate in cybersecurity information-sharing and capacity-building arrangements with the EU. In this way, the European Commission should:

- Conduct a comprehensive impact assessment and market analysis for managed security services in cooperation with the European Union Agency for Cybersecurity (ENISA) and the national authorities.
- Review Article 16 and Article 19 of the CYSOL to allow non-EU providers to participate in initiatives under the Act.
- Establish channels, beyond Article 17 on third-country support, for operational cooperation and information exchange with strategic partners by leveraging providers that operate across jurisdictions.

Proposals for amendments:

Bold: addition
~~**bold strikethrough**~~: deletion

AmCham EU amendments

Recital 2 The magnitude, frequency and impact of cybersecurity incidents are increasing **both in the Union and globally. These include** ~~**including**~~ supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine, and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in critical or highly critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy of the Union, and could even have health or life-threatening consequences. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve within very short periods of time, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries**. Therefore, as demonstrated by the successful joint actions taken in response to Russia's war of aggression against Ukraine, the Union's response must be coordinated with Union like-minded partners and allies, well identified by international cooperation frameworks and agreements, based on the best available tools and resources.**

Recital 9 Specific conditions for participation concerning each action will be provided for in the relevant work programmes, in line with the applicable provisions of Regulation 2021/694. **In order to ensure the swift procurement of 'state of the art' tools and trusted providers, actions will not apply Article 12(5) of Regulation 2021/694 as a condition of participation in calls relevant to Chapters II and III of this Regulation. The terms of tender participation will be evaluated on a case-by-case basis, in line with applicable provisions in this Regulation, Regulation 2021/694, and the specific terms of each tender.**

Article 12 (7) In order to support the Commission in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, after consulting Member States and the Commission **and conducting a comprehensive market analysis**. ENISA shall prepare a similar mapping, after consulting the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, shall consult the High Representative.

Article 16 (3 – NEW) By way of derogation from Article 12(5) of the 2021/694, legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries are eligible to participate in the European Cyber Shield and the EU Cybersecurity Reserve if they contribute to the Specific Objective 3 and, for the purposes of the EU Cybersecurity Reserve, meet the requirements of Article 16 of the Regulation (EU) 2023/XX.

Article 16(2)(c) The provider shall provide sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest **that pose a disproportionate risk contrary to the Union security interests and aims of open strategic autonomy**;

Article 19(4) The following article 16a is added:

(1) In the case of actions implementing the European Cyber Shield established by article 3 of Regulation (EU) 2023/XX, the applicable rules shall be those set out in Articles 4 and 5 of Regulation (EU) 2023/XX. In the case of conflict between the provisions of this Regulation and Articles 4 and 5 of Regulation (EU) 2023/XX, the latter shall prevail and apply to those specific actions.

(2) In the case of actions implementing the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the applicable rules shall be those set out in Articles 13, 14, 15, 16 and 17 of Regulation (EU) 2023/XX. In the case of conflict between the provisions of this Regulation and Articles 13, 14, 15, 16 and 17 of Regulation (EU) 2023/XX, the latter shall prevail and apply to those specific actions.

Leverage the expertise of global providers to build European capabilities

Cyberattacks are not limited by borders. Investing in partnerships with private providers that have a global view and capabilities will enhance EU’s cyber resilience. In particular, it will strengthen prevention and reaction capabilities based on global datasets, as well as provide a cross-border and cross-sectoral view. Global providers can also help build information-sharing platforms between strategic partners. Hence, the European Commission should:

- Create partnerships between local and global providers within the Cyber Solidarity Act for capacity-building facilitated by the European Cybersecurity Competence Centre.
- Provide better legal clarity for participation of private SOCs in Cross-border SOC. Although Recital 14 mentions that data within the Cross-border SOC will be shared both from public and private sources, Article 5 states that only the national SOCs will be participating in the Cross-border SOC.
- Include the Network of Government Cyber Incident Response Teams (CSIRT Network) in Article 12(5) and Article 12 (6) of the Cyber Solidarity Act as the entity responsible for the implementation of the Cyber Reserve.

AmCham EU amendments

Recital 3 It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market **with state of the art tools and trusted providers.** As recommended in three different proposals of the Conference on the Future of Europe4, it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.

Recital 14 As part of the European Cyber Shield, a number of Cross-border Cybersecurity Operations Centres (‘Cross-border SOCs’) should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved**. Private SOCs may join the Cross-border SOCs** as the general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of data from various sources, public or private, as well as through the sharing and joint use of state-of-the-art tools, and jointly developing detection, analysis and prevention capabilities in a trusted environment. They should provide new additional capacity, building upon and complementing existing SOCs and computer incident response teams (CSIRTs) and other relevant actors.

Recital 15 The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities **and competitiveness**~~ and technological sovereignty~~**.**

Recital 20 By collecting, sharing and exchanging data, the European Cyber Shield should enhance the Union's ~~technological sovereignty, security~~ **security and competitiveness in line with open strategic autonomy.** The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European Cyber Shield with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173

Article 1(2)(a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the ~~digital~~ economy~~. and contribute to the Union's technological sovereignty in the area of cybersecurity;~~

Article 5 (1) A Hosting Consortium consisting of at least three Member States, represented by National SOCs **and private SOCs,** committed to working together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC.

Include essential entities (NIS2)

The CYSOL aims to improve the cooperation between the public SOCs, however it seems to ignore the inclusion of SOCs or cyber expertise of entities falling under the scope of the NIS2 Directive, particularly the essential entities. The essential entities are currently on a security journey and must actively invest in further developing their cyber capabilities and coordination among the SOCs of entities in scope, but also with the National Competent Authorities (often the NCSCs or SOCs in scope of CYSOL). Thus, the CYSOL should formally acknowledge that the SOCs within its scope should cooperate with the entities covered by the NIS2 Directive.

Apply risk-based and proportionate approach

While it is important to improve and evaluate the cybersecurity of critical assets in the EU, mandatory preparedness testing should only apply to entities that do not have appropriate regular assessments in place. Thus, preparedness testing should be targeted at entities that do not have appropriate internal or third-party testing in place.

AmCham EU amendments

Article 11(1) For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level. **The primary subject to testing shall be entities that do not have preparedness testing and regular risk assessment policies in place.**

Article 11(2) The NIS Cooperation Group in cooperation with the Commission, ENISA**,** ~~and~~ the High Representative, **and in consultation with relevant entities referred to in Article 10(1), point (a**), shall develop common risk scenarios and methodologies for the coordinated testing exercises.

A platform for feedback between governments and private providers

Trust and transparency are key elements in any successful cybersecurity ecosystem. Indeed, we must ensure that policies are built on evidence, joint decision-making and regular consultations between the public and private partners. Thus, a structured and transparent framework should be established for discussions on the implementation of the initiatives under the Cyber Solidarity Act. This is particularly essential for the effective implementation and deployment of the Cyber Shield and the Cyber Reserve as well as the certification development.

AmCham EU amendments

Article 14a (NEW): EU Cyber Solidarity Group

1.The Commission shall establish, with the support from ENISA, an EU Cyber Solidarity Group as a platform for regular consultations between the public and private partners on the implementation and deployment of the Cross-Border SOC and the Cyber Reserve.

2.The EU Cyber Solidarity Group will consist of the representative of ENISA, the CSIRT Network, the chair of the NIS Cooperation Group and the trusted providers as described in Article 16.

Ensure state-of-the-art technology and skills deployed in SOCs

Human capital is a prerequisite of a workable cybersecurity policy framework. In this context, the volume and velocity of attacks requires us to continually create new technologies that can tip the scales in favour of defenders. Security professionals are scarce and must be empowered to disrupt attackers' traditional advantages and drive organisational innovation. The most effective way to address the existing skills gap in the EU is through partnerships among the private sector, governments, and educational establishments to provide scalable state-of-the-art training framework. Thus, we recommend that the Cyber Solidary Act focuses on ensuring state-of-the-art technology and skills which allow to:

- **Simplify complexity:** given that – in security – minutes count, with state-of-the-art technology, defenders can respond to security incidents within minutes instead of hours or days.
- **Catch what others miss**: as attackers hide behind noise and weak signals, defenders can discover malicious behaviour and threat signals using AI-enabled technologies that could otherwise go undetected.
- **Address the talent gap**: considering that a security team's capacity is limited by the team's size and the natural limits of human attention, AI can enhance the skills of your defenders by providing answers to a wide range of security-related questions – from basic to complex.

Conclusion

In the current geopolitical environment, where a growing number of security challenges derive from the cyberspace, the Commission's efforts to strengthen the Union's detection and response capabilities through the establishment of the ECS, SOCs and the implementation of a CEM, is timely and appropriate. In spite of this, the are some challenges within the CYSOL proposal that must be addressed, especially regarding the inclusion of politically sensitive concepts linked to technological sovereignty. Policymakers should consider industry's recommendations to ameliorate the initiative, especially focusing on the importance of building capacity through consolidation, leveraging the expertise of global providers, including essential entities (NIS2) and applying a risk-based approach.