DIGITALEUROPE

11 SEPTEMBER 2023

Paving the way towards a collective response to cybersecurity challenges in Europe

DIGITALEUROPE's views on the proposal for a Cyber Solidarity Act

Executive Summary

DIGITALEUROPE welcomes the **proposal for a Cyber Solidarity Act**, published by the European Commission on 18 April 2023.[1] Cyberattacks targeting the critical infrastructure of all nation-states increased by 20% in 2022,[2] having had serious political, financial, and economic consequences across Europe and beyond. A unified European approach has become an absolute necessity, as emphasised in our press release:[3]

> *Last year, in the wake of Russia's invasion of Ukraine, we called[4] for common European action to strengthen our cyber shield. We need a joint cyber defence to replace the current ineffective bits-and-pieces approach. With this announcement, Europe is delivering. The network of Security Operation Centres (SOCs), the European cyber mechanism with its cyber reserve are vital first steps towards multi-country collaboration on cyber defence.*

In this position paper, DIGITALEUROPE provides a series of recommendations aimed at further consolidating the proposal for a Cyber Solidarity Act. We consider the proposal a vital step towards a collective response to cybersecurity challenges in Europe. However, we

[1] European Commission (2023), *The EU Cyber Solidarity Act*, <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>.

[2] Microsoft (2022), *Microsoft Digital Defence Report 2022*, <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022>.

[3] DIGITALEUROPE (2023), *Solidarity Act and Skills Academy: Vital first steps towards a common European cyber shield, but private sector must play a role*, <https://www.digitaleurope.org/news/solidarity-act-and-skills-academy-vital-first-steps-towards-a-common-european-cyber-shield-but-private-sector-must-play-a-role/>.

[4] DIGITALEUROPE (2022), *DIGITALEUROPE and national associations to EU Council: Ukraine war must be a wake-up call to step up Europe's action on cybersecurity*, <https://www.digitaleurope.org/news/digitaleurope-and-national-associations-to-eu-council-ukraine-war-must-be-a-wake-up-call-to-step-up-europes-action-on-cybersecurity/>.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

urge policymakers to understand that the private sector should be at the forefront of these efforts. The private sector has been leading the charge against cybercriminals for decades through collaboration within various entities e.g., Information Sharing and Analysis Centres (ISACs) while transcending competitive barriers. Our most potent capabilities and solutions emanate from the private sector.

As such, our key recommendations in this position paper are to:

- **Strengthen cooperation and information sharing between cross-border SOCs and Information Sharing and Analysis Centres (ISACs).** The private sector has been sharing relevant information about vulnerabilities and threats as well as insights and best practices within the framework of ISACs. SOCs would greatly benefit from collaborating closely with ISACs. This partnership has the potential to boost the collective defence and resilience of European cybersecurity.
- **Involve private sector in setting up the EU cybersecurity reserve.** The partnership between the European Commission, the European Union Agency for Network and Information Security (ENISA) and the private sector can ensure that the reserve has access to key industry insights and cutting-edge solutions, thus safeguarding European cyber resilience.
- **Include cybersecurity professionals and providers in the EU cybersecurity reserve from NATO allied countries, EU candidate countries and like-minded countries e.g., Switzerland, Israel.** A collaborative approach could boost the collective defence against cyber threats.
- **The use of cloud technology is a pivotal enabler for cross-border SOCs.** Cloud infrastructure enables flexible, scalable, and borderless collaboration for European SOCs.
- **For an efficient cybersecurity ecosystem, procurement processes need to be faster and more agile.** We suggest the European Cybersecurity Competence Centre (ECCC) collaborates with the private sector to simplify procurement for cross-border SOCs in countering evolving threats.

Drawing from these recommendations, our position paper serves to bolster the efficacy of the proposed Cyber Solidarity Act. As we delve into these recommendations, our focus shifts towards concrete strategies that harness collaborative potentials, industry insights, and international expertise. Beyond these initial insights, DIGITALEUROPE

stands poised to share the collective wisdom and expertise of its members, contributing valuable perspectives on the ongoing consolidation of the Cyber Solidarity Act. With a commitment to nurturing a more secure digital future, our engagement extends beyond words to actionable solutions and a shared commitment to fortify European cybersecurity.

Table of contents

Article 7: Cooperation and information sharing with Union entities

DIGITALEUROPE encourages cross-border SOCs to collaborate closely with Information Sharing and Analysis Centres (ISACs). An additional paragraph to Article 7 should emphasise the advantages of this partnership for strengthening the collective defence and resilience of European cybersecurity.

- Efficient sharing of information is crucial for ensuring a well-coordinated response to large-scale cybersecurity incidents. Fostering collaboration among various European Union entities facilitates a unified approach to crisis management and enhances the collective resilience of the European cybersecurity landscape. By pooling the expertise and resources of different entities, the European cybersecurity community can leverage crucial information, enhancing its ability to stay ahead of rapidly evolving cyber threats.

- For decades, a steadfast and proactive collaboration has unfolded, as both private and public entities recognise the urgency of forecasting and combatting the relentless wave of cyberattacks. They willingly share vulnerabilities, thereby reinforcing the collective cybersecurity posture.

This partnership extends beyond the realm of vulnerabilities through shared competencies and capabilities. Cutting-edge technologies collectively contribute to addressing these challenges. The Information Sharing and Analysis Centres (ISACs) illustrate this collaboration.

A strong collaboration between cross-border SOCs and ISACs

- These trusted entities are developed by organisations that are exposed to similar cybersecurity threats and issues, therefore serving as central hubs for aggregating information regarding cyber threats. They are member-driven and are often set up by operators of essential services of critical sectors. ISACs foster the exchange of information and best practices for both physical and cyber threat identification and mitigation. Moreover, they facilitate two-way information-sharing between the private and public sectors about root causes, incidents, and threats as well as the dissemination of experience, knowledge, and analytical insights.

- ISACs address tactical and strategic issues e.g., major or critical disruptions with cross-organisation relevance while enabling trusted information exchange among members through technical solutions. They also conduct analyses on trends and incidents to share insights amongst their members. In addition, they facilitate training and testing of professionals and technical solutions.[5] Another critical aspect of their activity includes the dissemination of relevant policy information at the European level.

- ISACs with a formal structure have a dedicated board and established working groups. They organise regular thematic sessions and publish sectorial trend analysis reports. ISACs with an informal structure are rather focused on trust-based community building. Their members gather several times per year to exchange updates and ideas confidentially about the state of cybersecurity in their specific sectors.[6] Besides operators of essential services as key stakeholders of ISACs, institutions and entities such as the European Union Agency for Network and Information Security (ENISA), Interpol, the European Central Bank and even NATO are collaborating in various forms with

[5] Empowering EU-ISACs Consortium (2021), *Introduction to ISACs*, <https://www.isacs.eu/sites/default/files/flmngr/Empowering%20EU%20ISACs%20information%20package_1.pdf>.

[6] Idem

specific ISACs.7 Therefore, DIGITALEUROPE encourages cross-border SOCs to collaborate closely with sectorial ISACs.

- By harnessing ISACs' expertise and intelligence-sharing mechanisms, cross-border SOCs access crucial insights into emerging threats, vulnerabilities, and mitigation strategies. Collaboration with ISACs could include participation in information-sharing activities, for example, joint training and simulations, thus enhancing SOC teams' skills and best practices while deepening understanding of cross-border threats. Additionally, cross-border SOCs could also contribute by sharing their threat intelligence and incident data, bolstering ISACs' effectiveness through enriched knowledge and broader threat perspectives. Actively engaging with ISACs empowers cross-border SOCs to contribute to European cybersecurity's collective defence and resilience.

- In conclusion, **DIGITALEUROPE recommends adding a third paragraph to Article 7 on "Cooperation and information sharing with Union entities" addressing the cooperation and collaboration between cross-border SOCs and ISACs**. This additional paragraph should reflect the opportunity on the part of cross-border SOCs to have access to ISACs' expertise and intelligence-sharing mechanisms as well as crucial insights into emerging threats, vulnerabilities, and mitigation strategies. A robust collaboration between cross-border SOCs and even national SOCs and ISACs would undoubtedly strengthen the collective defence and resilience of European cybersecurity.

Article 12: Establishment of the EU Cybersecurity Reserve

DIGITALEUROPE welcomes the establishment of the EU Cybersecurity Reserve as a much-needed step towards multi-country collaboration on cyber defence. We recommend that the private sector be included as an active partner in setting up the reserve to strengthen its effectiveness in safeguarding European cyber resilience.

- The EU Cybersecurity Reserve is aimed at supporting national authorities with assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at the national level. Establishing an EU-level cybersecurity reserve is a vital step towards multi-country collaboration on cyber defence. To implement the incident response actions set out in the proposal, the

[7] Computer Weekly (2023), *Global finance firms take part in NATO cyber-attack simulation*, <https://www.computerweekly.com/news/365535419/Global-finance-firms-take-part-in-NATO-cyber-attack-simulation>.

reserve would consist of incident response services from trusted providers.

- Given the deep expertise and pivotal role of the private sector in cybersecurity innovation, it should be included as an active partner in establishing the reserve. **DIGITALEUROPE recommends that ENISA prepares the mapping of needed services in close consultation not only with the Member States and the European Commission but also in partnership with the private sector.** This collaborative effort will ensure that the reserve is fortified with the latest industry insights and cutting-edge solutions, enhancing its effectiveness in safeguarding European cyber resilience.

- At the same time, the EU cyber reserve should create opportunities for well-established companies and smaller businesses alike. Many cyber actors today are smaller firms that house advanced experts in the field. These specialised enterprises can add significant value to cyber defence efforts. Through this initiative, they stand to leverage the support and resources to become European cyber champions. This approach would ensure a dynamic and competitive ecosystem that safeguards our digital future.

- Ensuring effective use of the EU Cybersecurity Reserve necessitates a proactive approach that extends beyond its initial establishment. Regular meetings, training and common exercises involving the experts in the reserve would certainly optimise its efficiency. The management of crises is notably enhanced through robust collaboration and comprehensive preparation. Teams functioning within the reserve, comprising specialised professionals from various sectors, must not only comprehend their individual roles but also harmonise their efforts seamlessly. Through such strategic measures, the EU Cybersecurity Reserve evolves into a dynamic and agile resource, capable of swiftly and effectively countering emerging threats while upholding a unified and well-coordinated front in the face of cyber crises.

Article 14: Implementation of the support from the EU Cybersecurity Reserve

DIGITALEUROPE encourages the European Commission to extend the reach of the EU cybersecurity reserve to include cybersecurity professionals and providers from NATO allied countries, EU candidate countries and like-minded countries e.g., Switzerland, Israel. Such a collaborative approach would strengthen the collective defence against cyber threats.

- The establishment of an EU cybersecurity reserve would provide a dedicated pool of skilled cybersecurity professionals who can be

mobilised swiftly in times of crisis. The reserve would be a valuable asset in bolstering the collective response to cyber threats, augmenting the existing capabilities of Member States and enabling a more coordinated and effective cyber defence. By nurturing and maintaining a reserve of cybersecurity experts, the EU can proactively address the evolving cybersecurity landscape and ensure the availability of specialised expertise when it is most needed. This initiative demonstrates a forward-thinking approach to cybersecurity and reflects the commitment of the European Union to strengthening its cyber defence and protecting critical infrastructure.

- In shaping the EU cybersecurity reserve, it is crucial to recognise that cyber threats transcend national boundaries. **DIGITALEUROPE recommends that the reserve be open to cybersecurity professionals and providers from NATO allied countries, EU candidate countries and like-minded countries e.g., Switzerland, Israel.** Such an approach would bolster the effectiveness and expertise of the reserve.

- By welcoming participation from these nations, the EU can tap into a broader pool of talent and diverse perspectives, fostering international cooperation and the exchange of knowledge. This collaborative endeavour strengthens the collective defence against cyber threats, allowing the dissemination of best practices, pioneering methodologies, and cutting-edge technologies. Such collaboration enhances the collective defence against cyber threats, as it allows for the sharing of best practices, innovative approaches, and cutting-edge technologies. By harnessing the skills and resources of cybersecurity professionals from these nations, the EU cybersecurity reserve can benefit from a global network of expertise, contributing to a stronger, more unified response to cyber incidents and ensuring the resilience of critical infrastructure.

Use of cloud in cross-border SOCs

- **The use of cloud technology is a pivotal enabler for cross-border SOCs.** Cloud-based infrastructure offers the flexibility, scalability, and agility required to transcend geographical boundaries and foster seamless collaboration among European SOCs. By deploying security resources and tools within a cloud environment, cross-border SOCs can efficiently share threat intelligence, conduct joint simulations, and respond collectively to cyber incidents. This integration of cloud technology empowers SOCs to transcend the limitations of physical infrastructure, promoting real-time information exchange and joint decision-making across borders. Moreover, cloud platforms offer advanced analytics capabilities that enhance the ability of cross-border

SOCs to detect, analyse, and mitigate emerging threats with greater speed and accuracy.

Facilitating Faster Procurement

- **For an efficient cybersecurity ecosystem, procurement processes emerges need to be faster and more agile.** The dynamic nature of cyber threats demands rapid access to cutting-edge technologies and solutions. We recommend that the European Cybersecurity Competence Centre (ECCC) works together with the private sector to establish streamlined procurement frameworks that reduce bureaucratic hurdles, ensuring that cross-border SOCs can swiftly acquire the tools and resources needed to counter evolving threats. In the face of rapidly evolving threats, swift procurement is not only a matter of efficiency but also a critical element in maintaining a robust and proactive defence.

Conclusion

DIGITALEUROPE welcomes the proposal for a Cyber Solidarity Act, recognising the pressing need for a joint European approach to address the increasing cyber threats targeting critical infrastructure. We commend the proposal as a significant step forward in fostering cooperation, information-sharing and capacity-building among Member States.

In alignment with the principles outlined above, our recommendations in this position paper directly correspond to the key imperatives identified. These recommendations seek to strengthen collaboration and synergy across multiple fronts in the realm of cybersecurity.

By fostering closer ties between Security Operations Centres (SOCs) and Information Sharing and Analysis Centres (ISACs), as detailed in our first recommendation, we tap into the substantial potential of private sector involvement to enhance collective defence and bolster European cyber resilience.

Moreover, our second recommendation underscores the pivotal role of collaborative engagement between the private sector, the European Commission, and the European Union Agency for Network and Information Security (ENISA) in establishing the EU cybersecurity reserve. This partnership is envisioned to infuse the reserve with industry expertise and state-of-the-art solutions, augmenting our cyber defences.

Lastly, as we advocate for broader participation of cybersecurity professionals and providers from diverse international quarters, our third recommendation aligns seamlessly with our pursuit of a united front against cyber threats.

Therefore, our position paper advocates for a cohesive and collaborative approach that unites various stakeholders, enhances information exchange, and harnesses expertise to fortify the proposed Cyber Solidarity Act. By implementing these recommendations, we aim to build a robust foundation for European cyber defence and resilience, paving the way for a safer and more secure digital future for all.

FOR MORE INFORMATION, PLEASE CONTACT:

Claudia Gherman

Senior Policy Manager for Digital Resilience

claudia.gherman@digitaleurope.org / +32 493 25 40 67

Ray Pinto

Director for Digital Transformation Policy

ray.pinto@digitaleurope.org / +32 472 55 84 02

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT

Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK