



Neapolis University Pafos, Cyprus

AI-2-TRACE-CRIME

Jean Monnet Center of Excellence



Co-funded by
the European Union

Policy Brief

Strengthening Cybersecurity:

The EU Cyber Solidarity Act

NUP Jean Monnet / UNESCO Policy Briefs

24/2024



With the support of the
Erasmus+ Programme
of the European Union



UNESCO Chair in Human
Development, Security & the
Fight against Transnational
Crime and Illicit Trafficking in
Cultural Property



The NUP Jean Monnet / UNESCO working papers and policy briefs can be found at:

<https://www.nup.ac.cy>

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP UNESCO/JEAN MONNET WORKING PAPER or POLICY BRIEF NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

© AI-2-TRACE CRIME

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

All rights reserved. No part of this paper may be reproduced in any form without the permission of the author.

Frontpage picture: Generated with AI (Bing Image Creator)

The support of the European Commission and of UNESCO for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors; the European Commission and UNESCO cannot be held responsible for any use which may be made of the information contained therein.

Strengthening Cybersecurity: The EU Cyber Solidarity Act

Executive Summary:

The European Union has taken a significant step towards bolstering its cybersecurity posture with the provisional agreement on the "Cyber Solidarity Act" and a targeted amendment to the Cybersecurity Act (CSA). This policy brief explores the key elements of these agreements, their potential impact, and future challenges in securing the digital landscape.

Keywords

Cybersecurity, Cyber Resilience, Cyber Solidarity Act, Cybersecurity Act, Managed Security Services, Digital Single Market

Background

In April 2023, the European Commission proposed the "Cyber Solidarity Act" alongside an amendment to the existing Cybersecurity Act (CSA) adopted in 2019. These initiatives aim to strengthen the EU's collective ability to detect, prepare for, and respond to cyber threats.

Key Takeaways

- **Enhanced Detection and Awareness:** The Cyber Solidarity Act establishes a "cyber security alert system" with national and cross-border hubs to improve threat detection and information sharing across the EU.
- **Preparedness and Response:** The act also creates a cybersecurity emergency mechanism, including vulnerability testing for critical entities, an EU cybersecurity reserve for incident response services, and provisions for mutual assistance.
- **Strengthening Solidarity:** The EU aims to foster closer cooperation among member states in crisis management and response to large-scale cyber incidents.
- **Secure Digital Landscape:** These measures strive to create a safer digital environment for both citizens and businesses within the EU.
- **Managed Security Services:** The targeted amendment to the CSA enables future European certification schemes for managed security services, promoting their quality and fostering trust in service providers.

Challenges for the Implementation

- **Evolving Threat Landscape:** Cyber threats constantly evolve, requiring continuous adaptation and improvement of detection and response mechanisms.
- **Shortage of Cybersecurity Professionals:** The EU faces a talent gap in the cybersecurity field, requiring significant investment in workforce development.
- **Global Cooperation:** Addressing transnational cybercrime necessitates strong international partnerships and coordinated responses.
- **Balancing Security and Privacy:** Striking a balance between cybersecurity measures and individual privacy rights remains a complex challenge.

Next Steps

- Formal adoption of the Cyber Solidarity Act and CSA amendment by the Council and European Parliament.
- Implementation of the new measures, including establishing cyber hubs and the cybersecurity reserve.
- Developing European certification schemes for managed security services.
- Ongoing monitoring and evaluation of the effectiveness of these initiatives.

Conclusion

The "Cyber Solidarity Act" and the CSA amendment represent a significant step forward for the EU in bolstering its cybersecurity defenses. By fostering collaboration, enhancing preparedness, and improving incident response capabilities, the EU strengthens its collective resilience against cyber threats. However, continuous adaptation, talent development, international cooperation, and a focus on privacy remain crucial to securing the digital landscape in the long run.

Further Reading

- Cyber solidarity package: Council and Parliament strike deals to strengthen cyber security capacities in the EU ([link](#))