UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

The role of private SOCs in national cyberdefense

Dr. Csaba Krasznay
Associate professor
Department of Cybersecurity
Ludovika University of Public Service

Introduction

Lessons learnt from Ukraine

GLOBSEC
IDEAS SHAPING THE WORLD

Ukraine's cyber defence: Insights on private sector contributions since the Russian invasion

Anushka Kaushik, Senior Research Fellow & Cyber Lead, GLOBSEC

The following policy brief outlines some key takeaways from the active private sector participation in Ukraine's cyber defences since Russia's invasion in February 2022.

EU approach

The Commission proposed a **regulation on the EU Cyber Solidarity Act** to reinforce the EU's solidarity and coordinated actions to detect, prepare and effectively respond to growing cybersecurity threats and incidents.

The **Cyber Solidarity Act**, funded by € 1.1 billion (of which about 2/3 will come from the EU budget) introduces:

A **European Cyber Shield**, a pan European infrastructure of national and cross border SOCs.

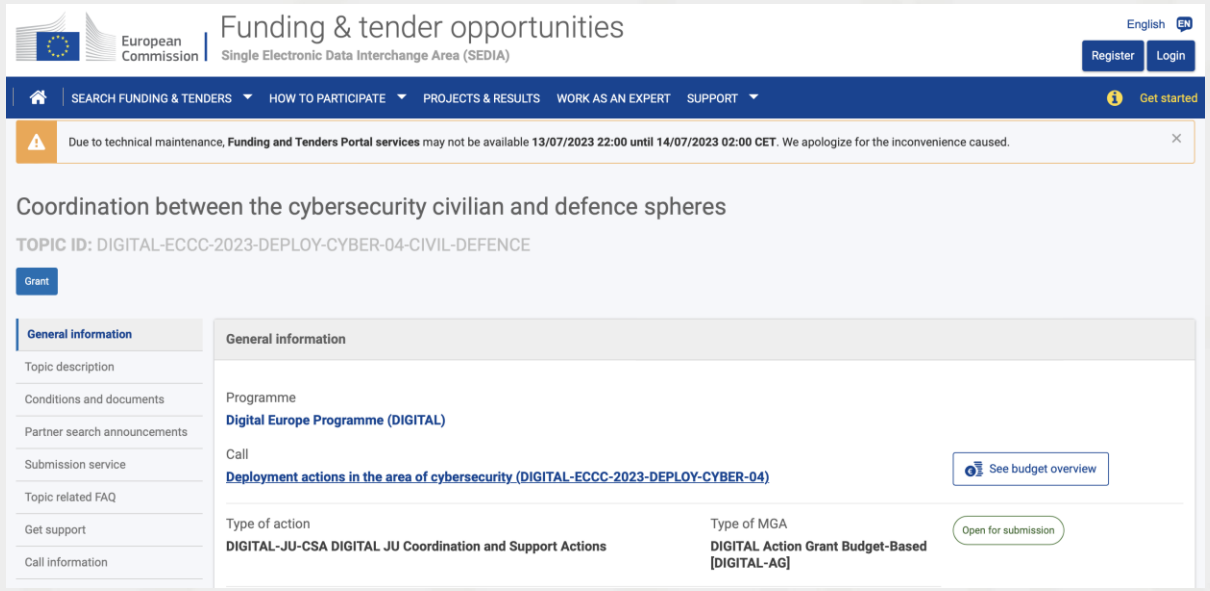
The **Security Operations Centres** (SOCs), are entities that monitor and analyse insights on cyber threats. With the Cyber Shield they will be able to provide timely warnings across borders.

A **Cyber Emergency Mechanism** to:

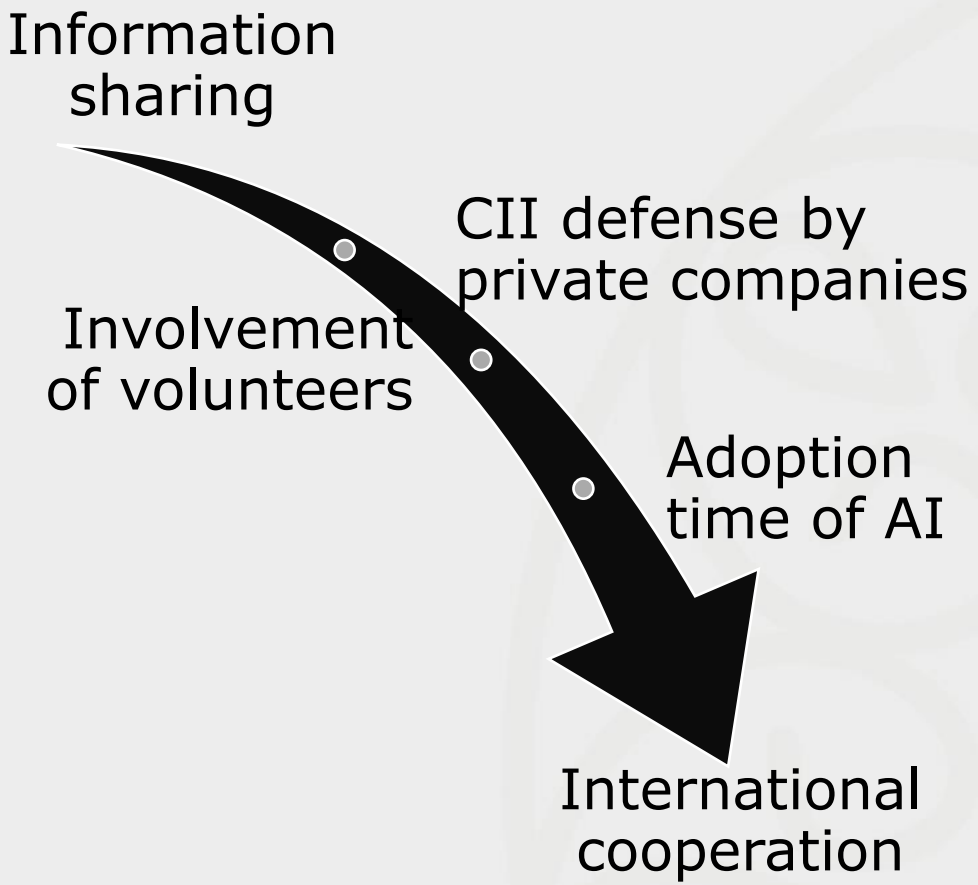
- Strengthen **preparedness** by testing entities in highly critical sectors (healthcare, transport, energy, etc.) for potential vulnerabilities.
- Create an **EU Cybersecurity Reserve** with incident response services from trusted providers ready to intervene, at the request of a Member State, in case of significant and large-scale cybersecurity incidents.
- Provide **financial support for mutual assistance** between Member States' national authorities.

A **Cybersecurity Incident Review Mechanism** to:

- Review and assess significant or large-scale incidents.
- At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA should review the cybersecurity incident and response. ENISA should then deliver a report on lessons learned and recommendations.



Major challenges



Opportunities in NIS2

(86) Among service providers, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and, because of their close integration in the operations of entities pose a particular risk. Essential and important entities should therefore exercise increased diligence in selecting a managed security service provider.

5. By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

THANK YOU!

en.uni-nke.hu