Funded by
the European Union

KINAITICS

KINAITICS & SAFE4SOC projects Standardization

HSBooster – 11/07/2024

The KINAITICS project has received funding from Horizon Europe under Grant Agreement 101070176

Funded by
the European Union

General context

Impact of artificial intelligence on products and services

Artificial intelligence (AI) is profoundly modifying **products** and **systems** in various sectors. On the one hand, its adoption creates new risks for systems and on the other hand, it has an impact on cyber-physical security practices, both on the attack and defense sides.

Convergence of physical and cyber security in presence of artificial intelligence

It is well-known that attacks or malfunctions in the cyber world can **have critical impacts on the physical world,** especially in critical infrastructures. Conversely, intentional perturbations of physical systems, through e.g., attacks on sensor measurements, can have disastrous consequences on digital control mechanisms, and consequently on physical processes.

Protecting systems when artificial intelligence and humans are involved

Protection of systems must take into account:

- Physical attack surface
- Cyber attack surface
- Artificial intelligence flaws
- Humans flaws and humans interactions with systems

Funded by
the European Union

KINAITICS vision

Artificial Intelligence – a **blessing** and a **curse** for cybersecurity

- Impact of AI on cybersecurity - attack side
  - Expand the threat landscape
  - Introduce new threats
  - Alter threats typical characteristics
- Impact of AI on cybersecurity - defence side
  - Exploit behavioural monitoring to detect and respond to threats / attacks
  - Proactively anticipate threats
  - Automatically respond to AI-driven cyber-attacks

"In our interconnected cyber-physical world, the advent of AI opens the door to various new kinds of attacks and offers numerous defence capabilities "

Funded by
the European Union

Funded by
the European Union

Key facts

36 months

4M € EU Grant

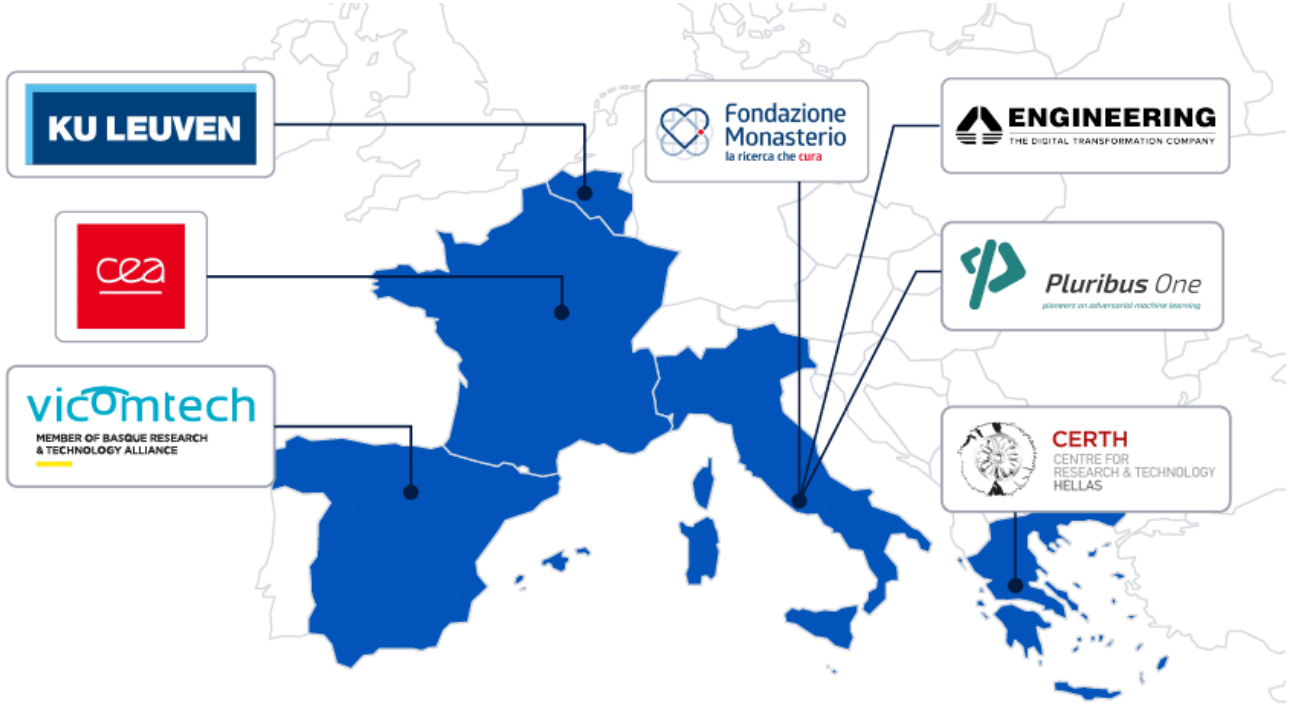
7 partners

5 nationalities

- Coordinator: CEA (France)
- Start date: October 2022
- Call: HORIZON-CL3-2021 – CS-01-03

AI for cybersecurity reinforcement

- Type: Research and Innovation



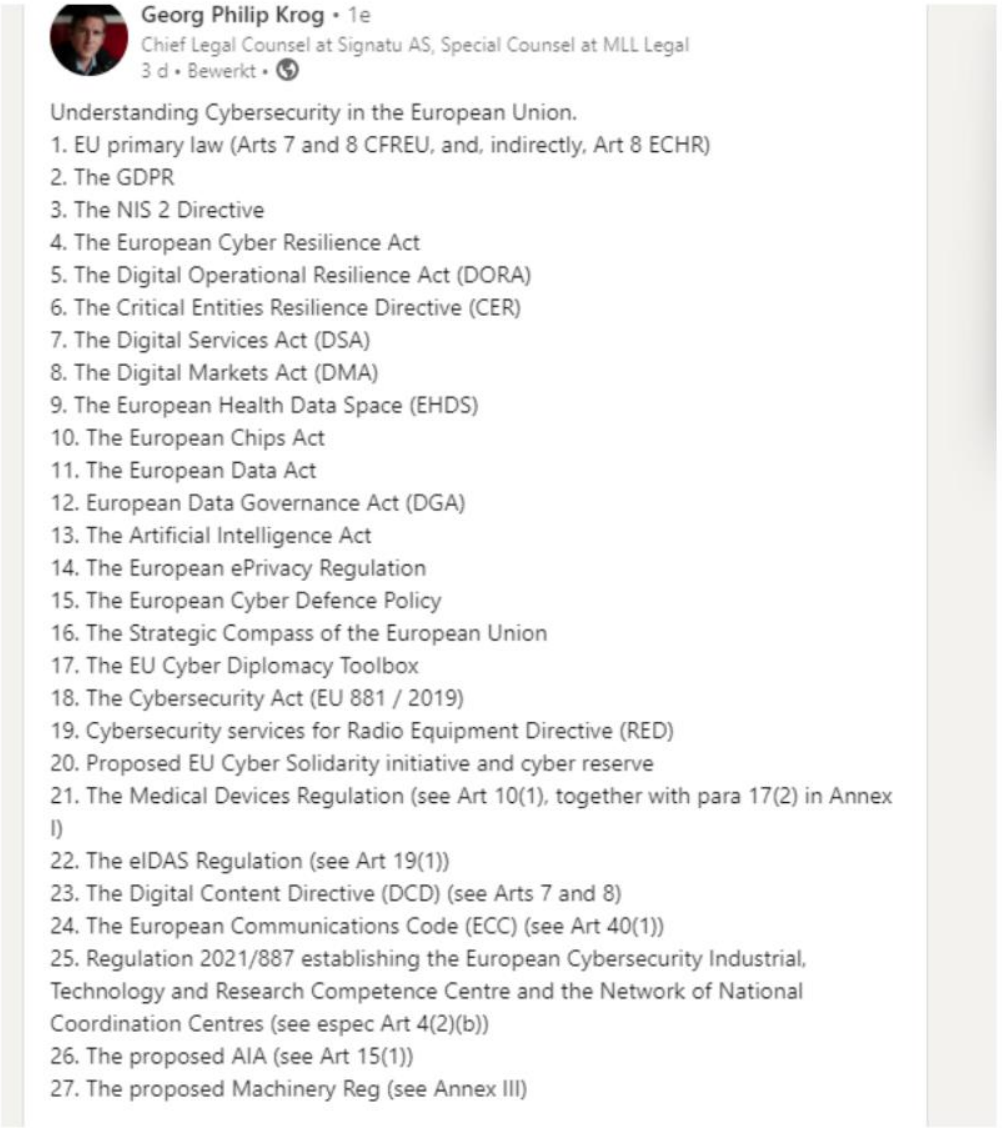
Funded by
the European Union

Very active legislator

Patchwork of cybersecurity regulations

Different applicable laws, often the same principles

How do we go beyond legislation?



Georg Philip Krog • 1e
Chief Legal Counsel at Signatu AS, Special Counsel at MLL Legal
3 d • Bewerkt •

Understanding Cybersecurity in the European Union.
1. EU primary law (Arts 7 and 8 CFREU, and, indirectly, Art 8 ECHR)
2. The GDPR
3. The NIS 2 Directive
4. The European Cyber Resilience Act
5. The Digital Operational Resilience Act (DORA)
6. The Critical Entities Resilience Directive (CER)
7. The Digital Services Act (DSA)
8. The Digital Markets Act (DMA)
9. The European Health Data Space (EHDS)
10. The European Chips Act
11. The European Data Act
12. European Data Governance Act (DGA)
13. The Artificial Intelligence Act
14. The European ePrivacy Regulation
15. The European Cyber Defence Policy
16. The Strategic Compass of the European Union
17. The EU Cyber Diplomacy Toolbox
18. The Cybersecurity Act (EU 881 / 2019)
19. Cybersecurity services for Radio Equipment Directive (RED)
20. Proposed EU Cyber Solidarity initiative and cyber reserve
21. The Medical Devices Regulation (see Art 10(1), together with para 17(2) in Annex I)
22. The eIDAS Regulation (see Art 19(1))
23. The Digital Content Directive (DCD) (see Arts 7 and 8)
24. The European Communications Code (ECC) (see Art 40(1))
25. Regulation 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (see espec Art 4(2)(b))
26. The proposed AIA (see Art 15(1))
27. The proposed Machinery Reg (see Annex III)

Funded by
the European Union

HSBooster's help required

The question: how can HSBooster help in identifying potential actions for the KINAITICS project

- Generic actions:
  - Standardization committees
- Domain-specific actions
  - Healthcare-related actions
  - Railway actions (critical infrastructure)

- Timeline
  - Beginning of february 2024
  - First meeting end of february 2024
  - Second meeting end of March 2024
  - Minutes as well as supporting documents after each meetings exchanged
  - Reports and recommendations

Funded by
the European Union

Consulting results (1/2)

- CEN/CENELEC:
  - CEN-CLC JTC 21 **'Artificial Intelligence'**, where a **Working Group 5** had been recently lunched for "**Joint standardization on Cybersecurity for AI systems**";
  - CEN-CLC/JTC 13 **'Cybersecurity and data protection'**;
  - CLC/TC 65X **'Industrial-process measurement, control and automation'**, which is one main provider of cybersecurity-related standards in the Operational Technology (OT) domain;
- ISO/IEC:
  - ISO/IEC JTC 1/SC 42 **'Artificial Intelligence'**, and
- ISO/IEC JTC 1/SC 27 **"Information security, cybersecurity and privacy protection"**

Funded by
the European Union

Consulting results (2/2)

SAFE4SOC connection on contributing to standards

- IDMEFv2 full success would be IETF Standardization (and adoption)
- Application to KINAITICS use case

Standard Alert Format Exchange
FOR SOC
DIGITAL-ECCC-2022-CYBER-B-03-SOC