Towards a resilient digital Europe

Roberto Cascella

The 2nd ECSCI Workshop on Critical Infrastructure Protection

28 April 2022
Created in 2016 as the contractual counterpart to the European Commission for implementing Europe's unique Public-Private Partnership in Cybersecurity.

Today, ECSO positions itself as the obvious partner to the European Cybersecurity Competence Centre in driving the European Cybersecurity Community with more than 260 members across 29 countries, connecting more than 2000 organisations in Europe.

Vision To achieve a Cyber resilient digital Europe and increase European Digital Sovereignty & Strategic Autonomy through the establishment of trusted & resilient supply chains for cybersecurity solutions and services.
ECOSYSMTEMS DEVELOPMENT: local, regional, national and beyond

MARKET, INVESTMENTS & COMPETITIVENESS
SKILLS: Human factors, Education, Training, Ranges, Awareness, Jobs

COMPETENCE: Research & Innovation

USERS & VERTICALS: Infrastructure, Services, CTI

SUPPLY CHAINS: Trusted and Resilient

APPROACH: Public – Private cooperation with a European cybersecurity industrial policy for an increased European Digital Sovereignty & Strategic Autonomy

FEDERATE COMMUNITIES

IMPLEMENT ACTIONS

SUPPORT POLICIES

ETHICS: EUROPEAN FUNDAMENTAL RIGHTS, VALUES, IDENTITY and INTERESTS

EUROPEAN CYBERSECURITY COMPETENCE COMMUNITY
Digital Economy and Digital transformation

• Growing digitalisation of the Society and of the EU Industry / Economy

• Digital transformation and increase reliance on new technologies
  ➔ IoT, AI, cloud, 5G and beyond...

• Data driven society

• Cyber threats evolving very quickly: approaches and organisations should be very flexible
Cybersecurity policies

- The EU Security Union Strategy (July 2020)
- The EU Cybersecurity Strategy (December 2020)
  - resilience, technological sovereignty and leadership;
  - operational capacity to prevent, deter and respond;
  - cooperation to advance a global and open cyberspace.
- Legislations and certification
  - Revision of the NIS Directive
  - Cybersecurity Act and EU cybersecurity certification framework
  - ....
- European Cyber Resilience Act (ongoing consultation)

Source: EU website
https://ec.europa.eu/info/policy-topics/security/eu-security-union_en
Legislation protecting European Critical Infrastructures (ECI)

- Directive 2008/114 EC
- Network and Information Security Directive (NIS) • 06/07/2016
- Proposal of Critical Entities Resilience Directive (CER) • 16/12/2020
- Network and Information Security (NIS2) Directive • 16/12/2020

- Member States would be required to adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments in order to identify critical entities.
- Critical entities would have to carry out risk assessments of their own and to take technical and organizational measures to ensure their resilience, as well as to report disruptive incidents.
- A Critical Entities Resilience Group, gathering Member States and the Commission, will evaluate national strategies and facilitate cooperation and exchange of best practices.
- To enforce rules, Member States should enable national authorities to conduct on-site inspections of critical entities and introduce penalties in case of non-compliance.
- The Commission would provide support to Member States and critical entities, for instance by developing a Union-level overview of cross-border and cross-sectoral risks, best practices, methodologies, cross-border training activities and exercises to test the resilience of critical entities.

Energy
Transport
Space
Banking
Financial Markets
Health
Drinking water
Waste water
Digital infrastructure
Public administration
Goal of the proposed NIS 2 expected to be enforced by the end of 2022: boost national cybersecurity capabilities and ensure higher levels of cyber resilience

- Security requirements will be strengthened with a list of focused measures, including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and effective use of encryption.
- The cybersecurity of the supply chain of key information and communication technologies will be strengthened.
- Management responsibility for compliance with cybersecurity risk management measures.
- Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timing.
Expanding the scope of NIS Directive

NIS Directive
- Healthcare
- Transport
- Banking
- Digital Infrastructure
- Water Supply
- Digital Service Providers

NIS 2 Directive
- Food
- Postal & Courier
- Electronic Communications Providers
- Space
- Public Administrations
- Digital Services
- Water Management

Digital Services Providers

28/04/2022
Need to develop capability and capacity in Europe

- Foster a resilient society by developing digital capabilities with reliable strategic technologies, solutions and skills (increase of strategic autonomy)

- Develop trusted supply chains, with solutions assessed as trusted by national agencies (digital sovereignty)

Latest digital (/data) strategic priorities for the EC as in the “State of the Union”:
- High performing computers
- Connectivity
- Cloud

Are these the only key strategic technologies for EU?
Path to the Digital Decade

On September 2021 the Commission proposed a Path to the Digital Decade to achieve the digital transformation of our society and economy by 2030.

Areas targeted for Europe's digital transformation by 2030... data infrastructure, low-power processors, 5G communication, high-performance computing, secure quantum communication, public administration, blockchain, digital innovation hubs, and people's digital skills.

Europe’s Digital compass - objectives

- Digitally skilled citizens and highly skilled digital professionals (80% adults with basic digital skills – more women)
- Secure, performant and sustainable digital infrastructures (full 5G coverage, production of 20% semiconductors in EU, first quantum computer)
- Digital transformation of businesses (75% using cloud, big data, AI - >90% SMEs)
- Digitalisation of public services (available online and 80% citizens using eID solutions)

Digitalisation offers many new opportunities on the European marketplace, where more than 500,000 vacancies for cybersecurity and data experts remained unfilled in 2020.
Strategic autonomy as an enabler of sovereignty ... some challenges ahead

Strong links with Digital sovereignty

Opportunities for EU's autonomy

80% of all generated data is expected to be processed at the edge by 2025, with no current dominant market players

Strong growth in software services is a major opportunity for European providers to leverage their position

5G networks and multi-cloud computing (risk-mitigation tool) constitutes another opportunity

Cloud computing / edge – which role?

It is key to increase assurance that data is secure wherever they are stored or processed

**European cybersecurity certification scheme for cloud services**

Towards a more secure and trusted resilient infrastructures in Europe

- Cloud services meeting high requirements for data protection, security, portability, interoperability, ....
- ICT supply chain complexity
- Interconnection of heterogeneous technologies (including IT, OT, edge / cloud computing, IoT, etc.)
IoT – which role?

It is a central element in the global digitalisation trend that is reaching our industry, our economy, and our society.

**General purpose vs. intended use**

**Challenges ahead**

- Interplay between regulation, certification and technology
- Developing and maturing IoT cybersecurity technologies
- A pervasive cyber-insecure IoT calls for generous multi-stakeholder effort
Artificial Intelligence – which role?

…. but creates new challenges

A risk-based approach to regulation

A resilient AI is a key enabler for the digitisation of the industry

Challenges ahead

➢ Use of AI for improving cybersecurity
➢ Security of AI systems
➢ Use of AI by attackers and resilience against AI-powered cyberattacks

AI and European digital autonomy & sovereignty

IRIS Motivation

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, novel and complex dimensions to the threat intelligence landscape are introduced. These, are linked with identifying, responding and sharing data related to attack vectors, based on emerging IoT and AI technologies, whose architecture and behaviour are not currently well understood by security practitioners, such as CERTs and CSIRTs.

This lack of experience as well as of tools, for detecting and reporting IoT & AI attack vectors is further aggravated by potentially greater safety risks caused by such attacks.
IRIS Vision

The **H2020 IRIS project** aims to deliver a framework that will support European CERT and CSIRT networks **detecting, sharing, responding and recovering from cybersecurity threats and vulnerabilities of IoT and AI-driven ICT systems**, in order to **minimize the impact of cybersecurity and privacy risks**.

The IRIS platform will be made available, **free of charge**, to the European national CERT and CSIRTs, by the end of the project.
Digital transformation and Cybersecurity

- Not a simple transformation, need to ensure integration with existing infrastructure/products
- Digital transformation is bringing a paradigm shift in business operations and changing cybersecurity requirements
- A forward thinking cybersecurity strategy is necessary to meet forthcoming digital challenges and solutions to face threats (known and unknown – hence, resiliency)

At stake business continuity and resilient digital services and infrastructures

Cybersecurity is critical in the digital transformation era
ECSO cybersecurity priorities for Horizon Europe and Digital Europe Programme

- Risks / Threat management
- Data & AI (including privacy)
- Cyber secure HW & SW (including crypto) supply chains
- Infrastructure resilience
- Skills
- Support to European competitiveness

APPLICATION DOMAINS AND INFRASTRUCTURE

ECOSYSTEM, SOCIAL GOOD AND CITIZENS

BASIC AND DISRUPTIVE TECHNOLOGIES

DATA AND ECONOMY

28/04/2022
ECSO cybersecurity priorities for Horizon Europe and Digital Europe Programme

- Cyber resilient digitised infrastructures
- Secure Quantum Infrastructures
- Cyber secure future communication systems and networks

Vertical sectors cyber challenges: Industry 4.0 and ICS; Energy (oil, gas, electricity) and smart grids; Transportation (road, rail, air; sea, space); Financial Services, e-payments and insurance; Public services, e-government, digital citizenship; Healthcare; Smart cities and smart buildings (convergence of digital services for citizens) and other utilities; Robotics; Agrifood

Deploying resilient digital infrastructures in the field
Areas for possible investments to capabilities under RRF: a ECSO analysis

- Cybersecurity for the **digital transformation of strategic sectors**: cyber resilient critical infrastructures and essential services
- Cyber secure **communication systems / networks and secure connectivity** of products and associated services including secure digital services for B2C
- Secure **data** (end-to-end data protection and secure data management) and protection from manipulation (fake news)
- Secure and trusted **digital identity** management – self-sovereign identity
- Cyber security **aware citizens / decision makers** and highly **skilled workforce**
Cybersecurity for the digital transformation of strategic sectors

Resilience in infrastructures and services means being able to prevent, detect and respond to disruptions

• **Threat intelligence and risk management** to ensure safe, secure and resilient European societies and economies with improved capabilities to cope with known and unknown cascading infrastructure failures

• **Integrity and trustworthiness of interconnected physical-digital EU infrastructures:** resilient cross-vertical platforms to exchange information

• **Securing integrity and availability of the global DNS root system**
System Security and Certification Considerations

*Systems are mission specific, and the risk is managed for its full dimension crossing all life cycle stages from design, procurement, testing, integration, implementation, operation, maintenance, retrofit and decommissioning.*

Aspects to consider

- High-level risk assessment defining a cyber security risk perimeter and providing important risk comprehension for all subsequent actions in a coherent framework
- Interoperability is a point of importance for secure operations as systems are often composed of a very large number of subsystems and products
- Lots of actors with a very variable background are involved
- Different standards and certification schemes can be used, each one adapted to the specific needs from the lifecycle
- Supply chain must be adapted to cover the needs of the system lifecycle

Waters systems (Source: Schneider Electric)

Webinar available

https://www.youtube.com/watch?v=mXiytFIOxI
System lifecycle and stakeholders’ roles

- Full life cycle of the system
- Importance of high-level risk assessment & secure architecture
- Governance
- Secure operation is key all during the operational life of the system, including decommissioning
- Different needs and stakeholders at each phase

- Various stakeholders: End user, system owner, service provider, manufacturer,…
- Evolving of stakeholders at each phase, all along the lifetime of the system
- Evolving of perimeter according to the area of responsibility of each stakeholder

It leads to a formal transfer of risk and responsibilities
The way forward

A comprehensive approach to security is needed...

...technology, people, processes, ... innovation for a trustworthy and resilient cybersecurity ecosystem

"Being prepared is half of the victory"

Miguel de Cervantes

Slide adapted and courtesy of Ana Ayerbe (TECNALIA)
European Cyber Security Organisation (ECSO)
29, Rue Ducale
1000 - Brussels
BELGIUM

secretariat@ecs-org.eu

www.ecs-org.eu

@ecso_eu

ecko-cyber-security

Join the Community
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

Project at a Glance

**Call Identifier:** 2020-SU-DS-2020

**Topic:** SU-DS02-2020 Intelligent security and privacy management

**EC Funding:** 4 918 790.00

**Duration:** 36 months (Sept 2021-Aug 2024)

**Consortium:** 19 partners

**Coordinator:** INOV - Instituto de Engenharia de Sistemas e Computadores, Inovacão, (INOV), Portugal

**Learn More:** www.iris-h2020.eu

**Join us:** @iris-h2020

IRIS H2020 Project

6 Public organizations
3 SMEs
4 Large ICT industries
6 Research institutions & Universities