Cybersecurity programs and collaboration

Vision and opportunities

18.02.2022

Start-up

14 June 2021

Constitution
The National Cybersecurity Agency was established following the adoption of the **Law decree June 14 2021, n.82**.

4 August 2021

Conversion
into law of the Law decree

13-16 September 2021

Prime Minister's **delegation** and **Transfer** of functions to ACN

15 December 2021

Agreement signed for **PNRR** Investment 1.5 Cybersecurity

24-27 December 2021

Approval of the Agency's implementing regulations

26 January 2022

Start of **collaboration** with the Italian Data Protection Authority

Purposes:
➢ sustain the digital development of the national and European **digital autonomy**
➢ coordination and promotion of **public-private initiatives**
➢ develop a national cybersecurity **workforce**
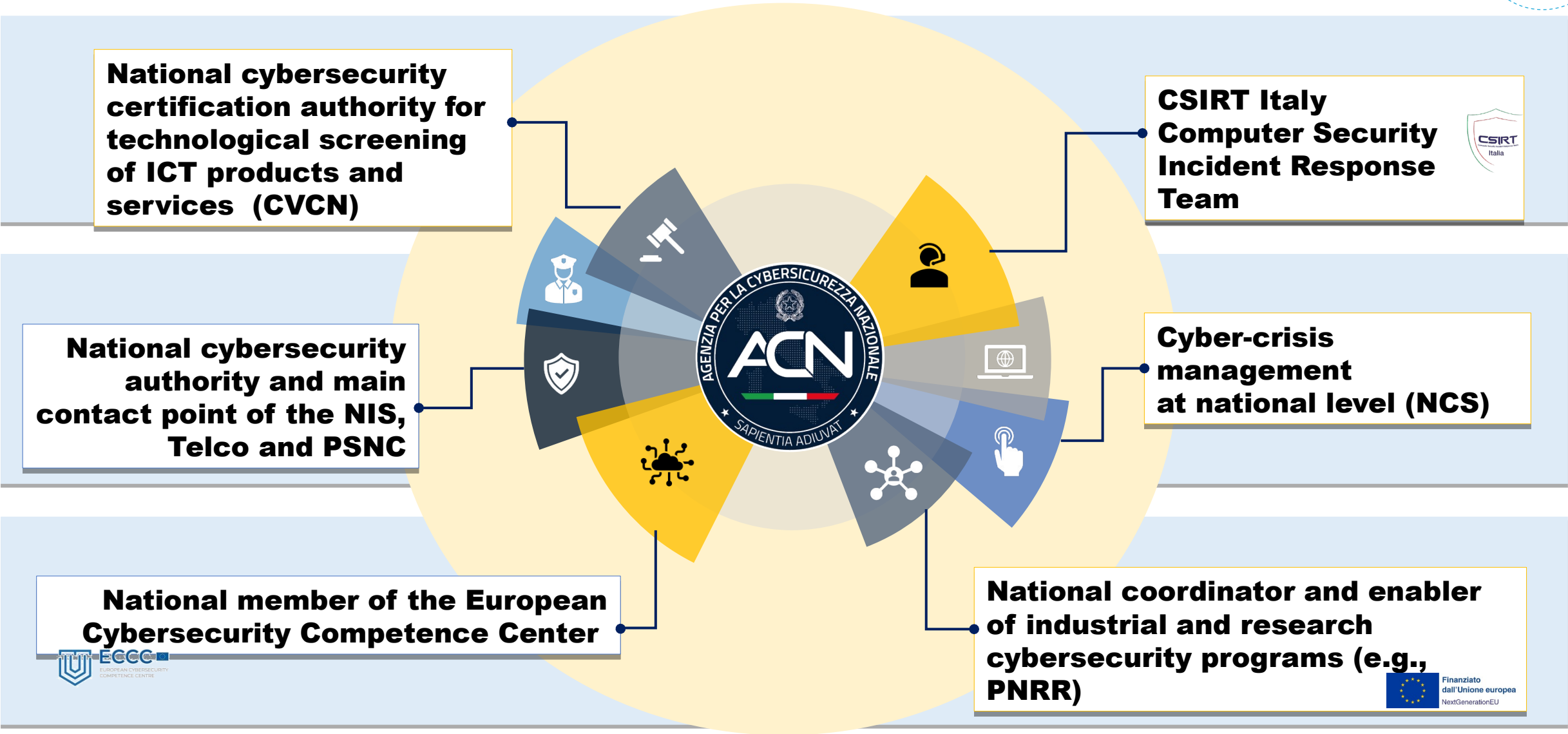
Guiding Principles:
➢ Rationalization
➢ Harmonization
➢ Competence

Holistic approach:
from the strategic
⬇
through the operational
⬇
to the tactical level

3

Key Roles

National cybersecurity certification authority for technological screening of ICT products and services (CVCN)

CSIRT Italy Computer Security Incident Response Team

National cybersecurity authority and main contact point of the NIS, Telco and PSNC

Cyber-crisis management at national level (NCS)

National member of the European Cybersecurity Competence Center

National coordinator and enabler of industrial and research cybersecurity programs (e.g., PNRR)

Finanziato dall'Unione europea
NextGenerationEU

Start-up & Key roles

Cabinet

Strategy and Cooperation

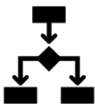**Authorities and sanctions**

Industrial, technological, research and training programs

Human and instrumental resources

Certification and supervision

Operations

It is responsible for activities carried out by the Agency to promote **strategic autonomy** and **national technological authority** namely:

- **promote, develop and support specific national and international projects** and initiatives on cybersecurity;
- **develop industrial, technological and scientific skills**, through the involvement of universities, research institutions, and national production system;
- **promote the development of competences in cybersecurity**;
- Coordinate and the functioning of the National Coordination Centre for cybersecurity;
- **manage activities** to set up and participate in public-private partnerships on the national territory;
- **promote training** initiatives aiming to qualification, technical and professional development of human resources in the field of cyber security.

Stakeholders

Public Sector:
- Central and local government
- Other Public Entities
- Universities and Research

Private Sector:

Start-Up, PPP, …

Industry:
- Telco
- Transportation
- Banking & Financial Services
- Utilities
- Engineering and Innovation
- Manufacturing and mobility
- Health

Professionals and other companies

Cybersecurity Programs: Vision

1. STEER

Guide and evolve the national cybersecurity architecture

2. DESIGN

Design and improve cybersecurity capabilities towards the national digital autonomy
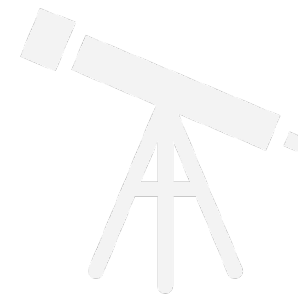
3. PROMOTE

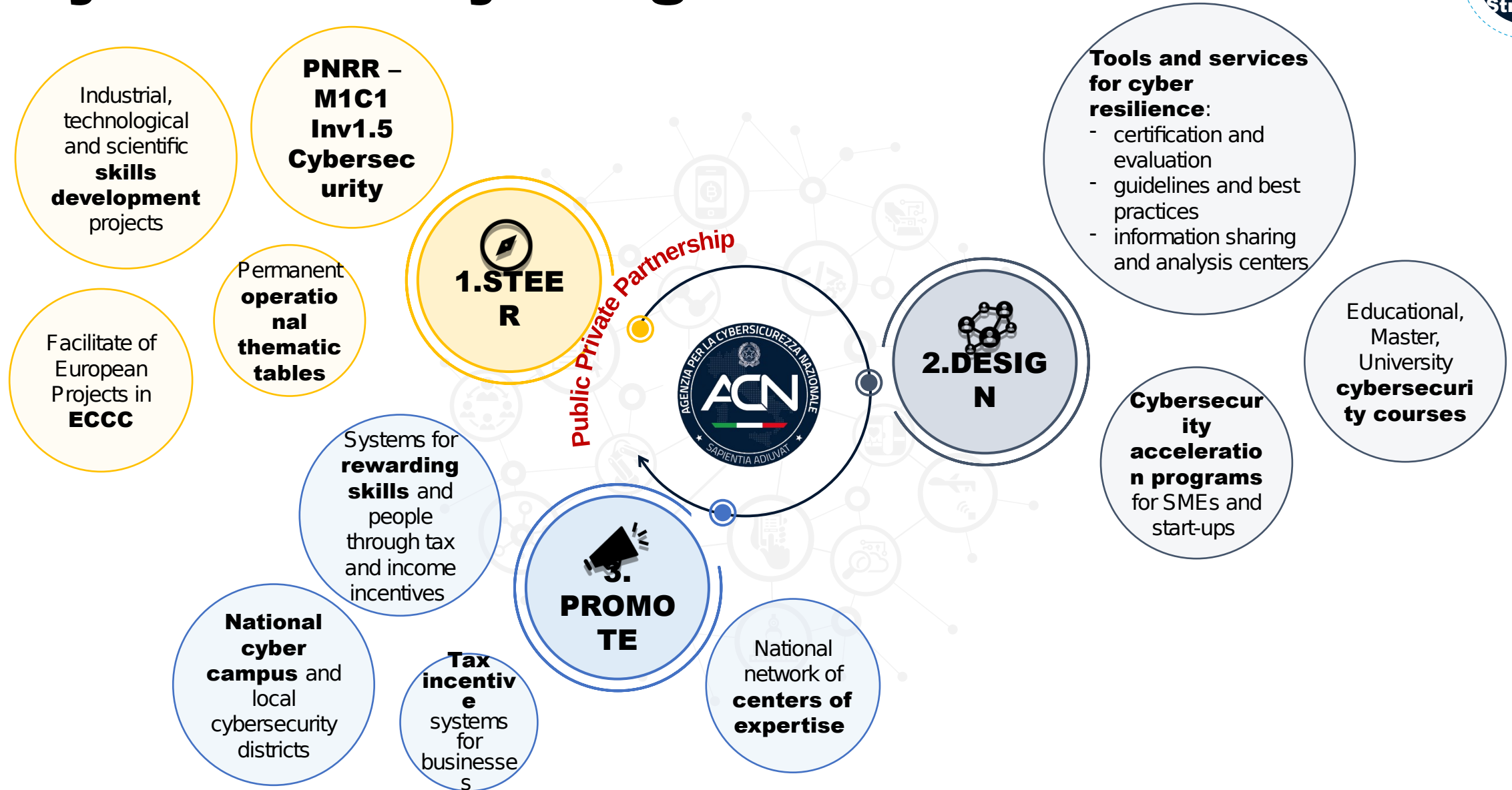National and international, public and private, synergies and opportunities and attract external experts

Single point of contact for institutions, citizens and businesses to strengthen the national cyber-resilience posture

Cybersecurity Programs: Actions

Industrial, technological and scientific **skills development** projects

PNRR – M1C1 Inv1.5 **Cybersecurity**

Permanent **operational thematic tables**

Facilitate of European Projects in **ECCC**

1.STEER

Public Private Partnership

2.DESIGN

Tools and services for cyber resilience:
- certification and evaluation
- guidelines and best practices
- information sharing and analysis centers

Educational, Master, University **cybersecurity courses**

Cybersecurity acceleration programs for SMEs and start-ups

Systems for **rewarding skills** and people through tax and income incentives

3. PROMOTE

ACN — AGENZIA PER LA CYBERSICUREZZA NAZIONALE — SAPIENTIA ADIUVAT

National cyber campus and local cybersecurity districts

Tax incentive systems for businesses

National network of **centers of expertise**

PNRR - the Cybersecurity Program

The goal is to improve the resilience of our country's data and services, strengthening the digital infrastructures and specialist skills necessary to ensure adequate levels of cyber-resilience.

ACN Agenzia per la Cybersicurezza Nazionale · SAPIENTIA ADIUVAT

Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE ·D

PNRR - Cybersecurity Program

PNRR – *National Recovery and Resilience Plan*

MISSION 1
Digitalization, innovation, competitiveness, culture and tourism

COMPONENT 1
Digitalization, innovation and security in the PA

INTERVENTION 1.5
Cybersecurity

PNRR - Cybersecurity

Main Output

1 NATIONAL CYBER SERVICES

National HyperSOC	*Cyber collaboration and mitigation services* *(e.g., supply chain)*	*Information Sharing and Analysis Center (ISAC)*
Central Audit Unit *for PA and private sector*	*Advanced Analysis tools (HPC & AI / ML)*	*Network of cyber incident response centers (CERTs)*

2 NATIONAL RESILIENCE CYBER INTERVENTIONS FOR THE PUBLIC ADMINISTRATION

Enhancement packages to increase basic cyber capabilities	**Projects to enhance the cyber-defense capabilities**

3 CYBERSECURITY SCREENING AND CERTIFICATIONS LABORATORIES

National Assessment and Certification Center (CVCN)	**Assessment Centers (CVs) of Interior and Defence**	**Network of screening and certification laboratories**

3 Project Streams

12 Work Packages

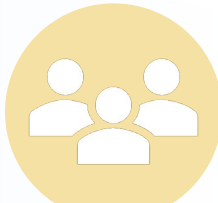**5** Milestone/Target 2022

4 Milestone/Target 2024

623 M€

Finanziato dall'Unione europea
NextGenerationEU

Next steps

Define the **partnership model** with private markets

Define the roles of stakeholders (Es, ACN, Confindustria, ecc) and the methods (ex. co-design) in the design of the partnership model

Identify and plan the services covered by the partnership: **needs, key resources, activities and skills to be shared**

Outline the **implementation roadmap ...**