Opportunities for Innovation and Maturity in Cybersecurity

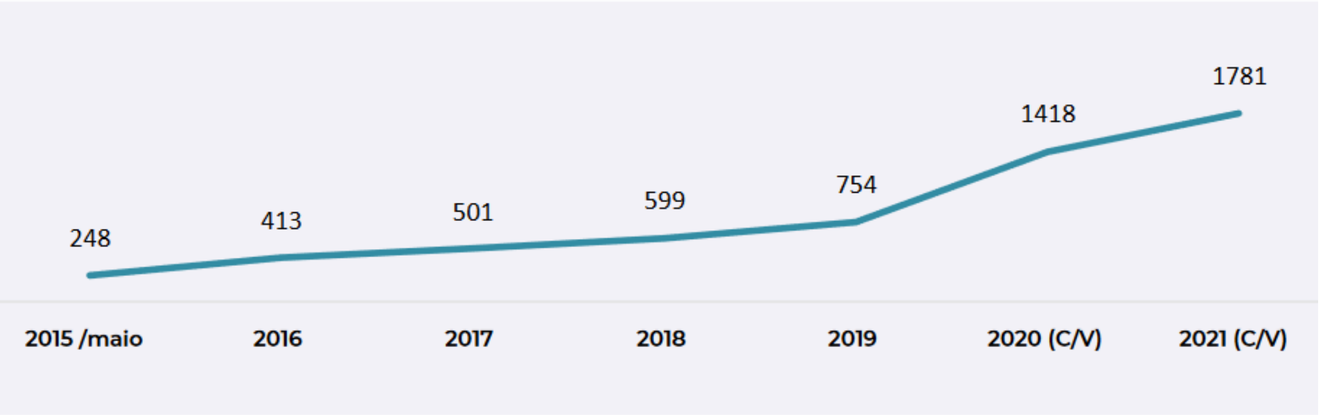
António Rio Costa
Centro Nacional de Cibersegurança

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

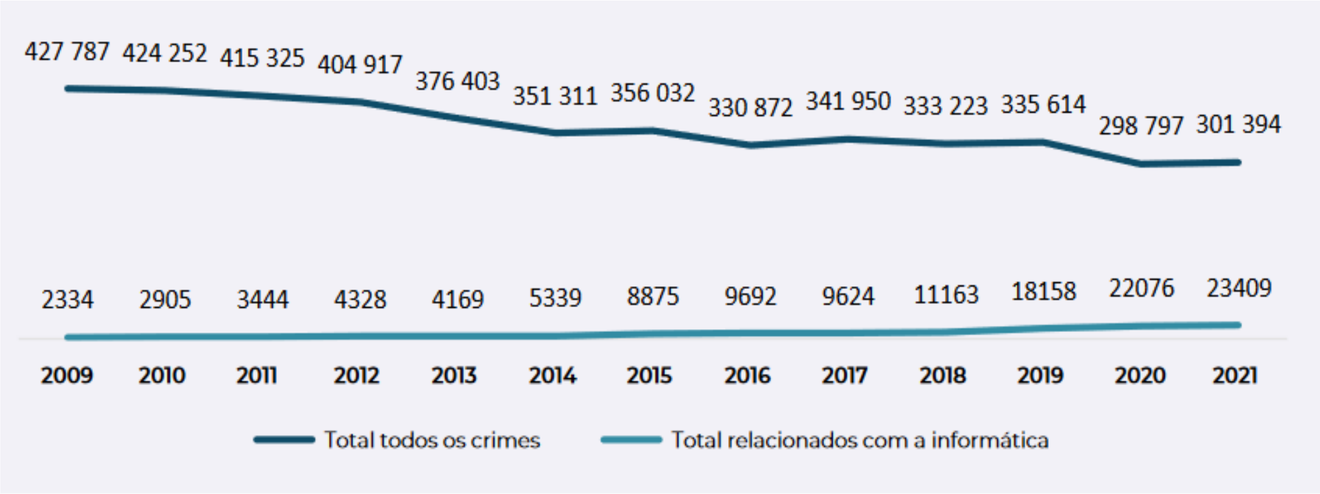
Presentation Objectives

Demonstrate the importance of the **problem** regarding the lack of cybersecurity, to present the CNCS work and vision regarding the **opportunities** for organizations.

Introduction (1/2)



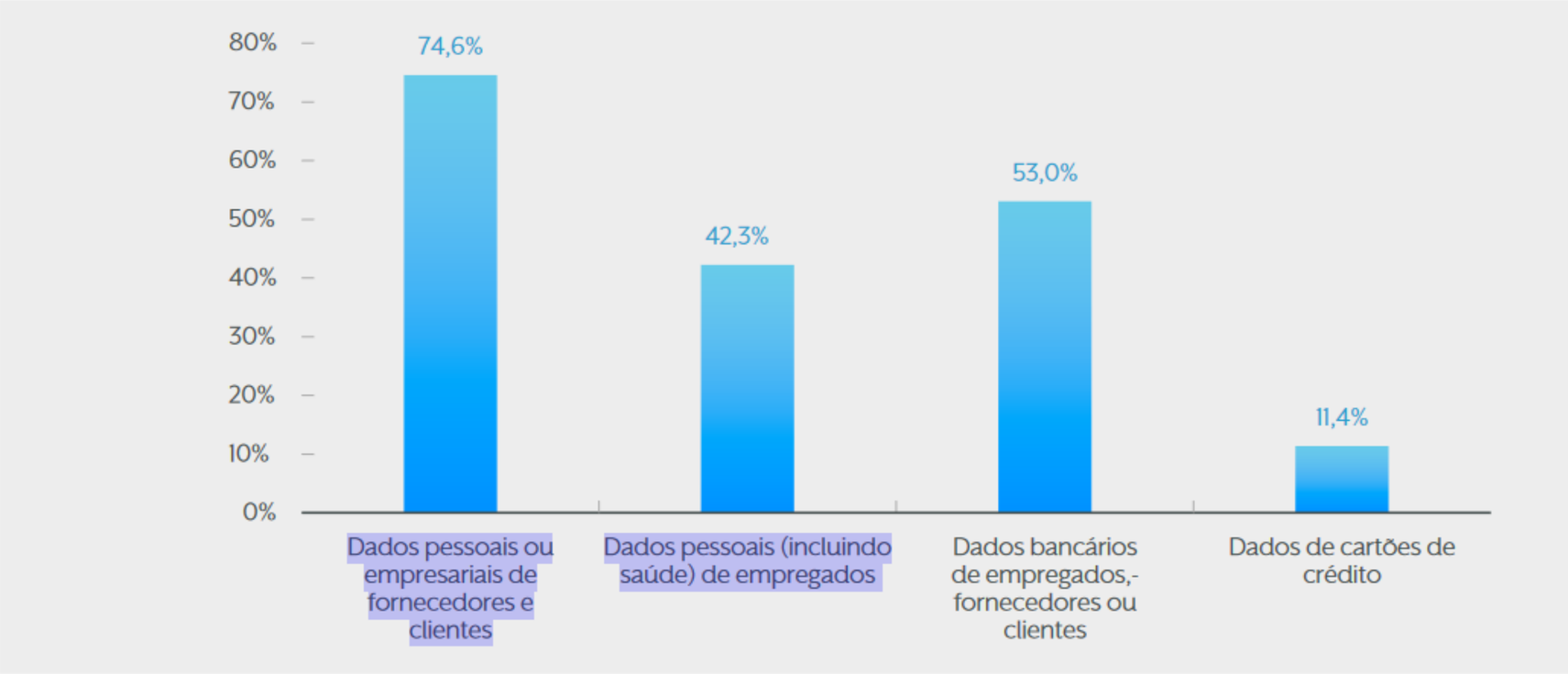
Number of cybersecurity incidents registered by the CERT.PT - 2015 -2021



Number of ICT related crimes registered by the police authorities, from 2009 to 2021

Source: *Relatório Cibersegurança em Portugal – Riscos e Conflitos 2022*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.

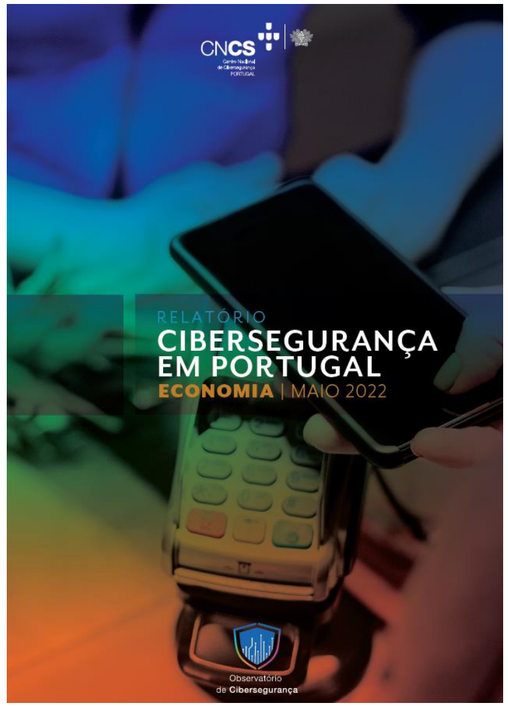
Introduction (2/2)



Types of processed data by enterprises in Portugal (%) - 2021

Source: *Relatório Cibersegurança em Portugal – Economia 2022*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.

Supply and Demand in Cybersecurity



Supply in Portugal, 2021

- There are at **least 144 companies** offering cybersecurity services (**there is potential**);
- In 2021, the market value in the country was **approximately 165M€** (**relatively low**);
- 42% of professionals have **5 years or less of experience** in the area (**young professionals**).

Demand in Portugal, 2021

- Just over a third of SMEs have a budget below **3000 euros in cybersecurity** (**it is low**);
- About 78% of SMEs complain about the difficulty in **hiring cybersecurity locally** (**demand**);
- More than half of the SMEs mention the **high costs of these professionals** as a problem (**costs**).

CNCS

Source: *Relatório Cibersegurança em Portugal – Economia 2022*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança

Emerging technologies and new threats requires innovation

Source*: Infographic – Top 10 emerging cyber-security threats for 2030, Enisa*

Legal requirements requires community training

ASSEMBLEIA DA REPÚBLICA

Lei n.º 46/2018

de 13 de agosto

Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

Artigo 2.º

Âmbito

1 — A presente lei aplica-se:

a) À Administração Pública;
b) Aos operadores de infraestruturas críticas;
c) Aos operadores de serviços essenciais;
d) Aos prestadores de serviços digitais;
e) A quaisquer outras entidades que utilizem redes e sistemas de informação.

New NIS Directive (2) – more sectors involved, more obligations and more supervision

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank [1],

Having regard to the opinion of the European Economic and Social Committee [2],

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure [3],

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council [4] aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.

CNCS

Remarks

Cybersecurity is a **problem.**

But also a business **opportunity**.

Its absolutely necessary to respond to the demands of **threats** and **legislation**.

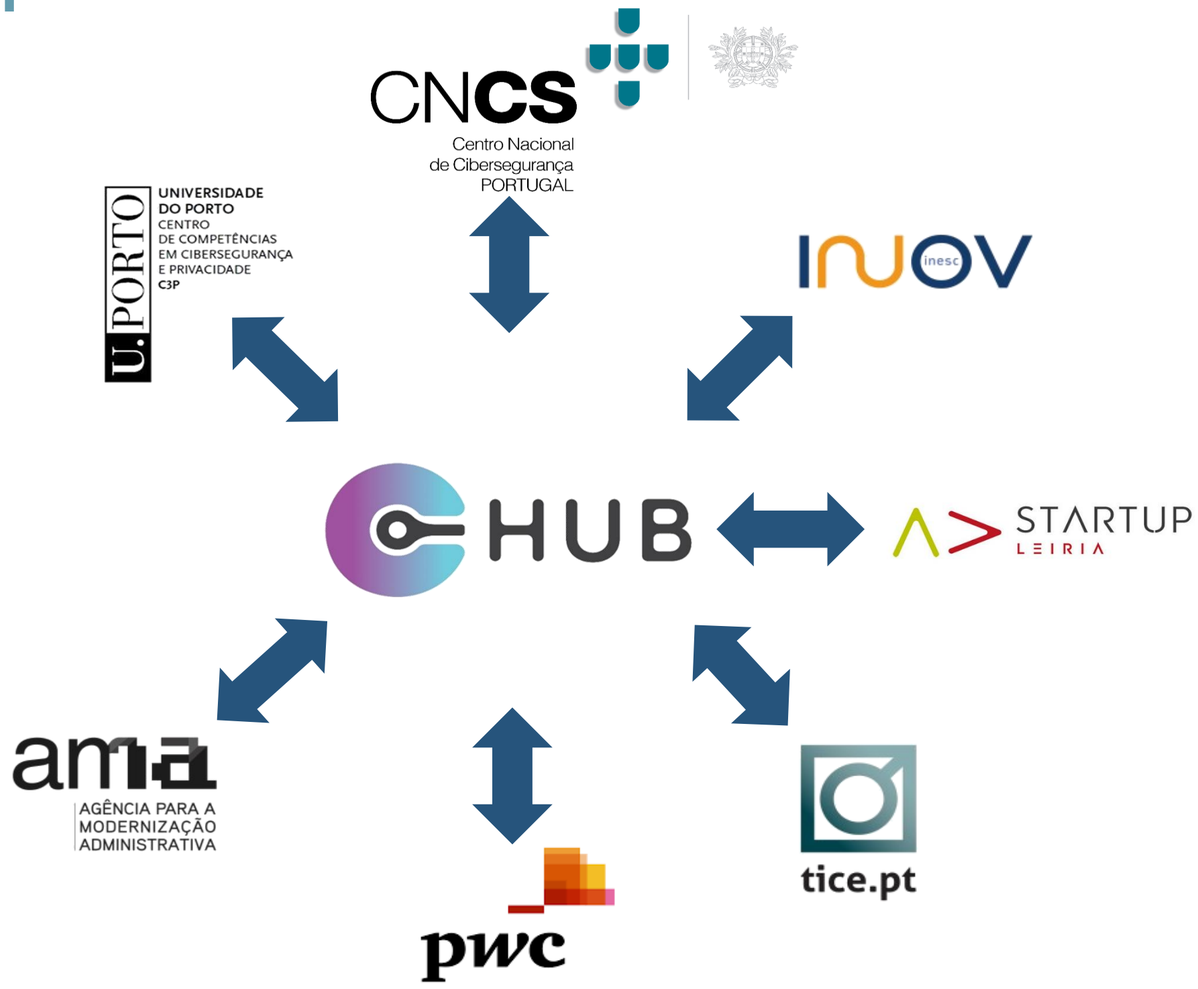
Enterprises should be mobilized not only to their **capacitation and cyber resilience**, but also towards **business** creation in cybersecurity.

Digital Innovation Hub
C-HUB

Digital Innovation Hubs (DIHs) are **collaborative networks** that include centres of **specific digital competence**s, with the objective to **disseminate and to promote the adoption of advanced digital technologies** by companies, in particular, SMEs, **through the development, testing and experimentation**.

The Digital Innovation Hubs act as a **gateway and strengthen the innovation ecosystem**, as they result from **cooperation** between **several partners with complementary skills and competences**, including research centres, universities, technological interface centres, incubators, competitiveness clusters, associations companies, development agencies, among other players in the national or regional innovation ecosystem.

Digital Innovation Hub
C-HUB



HUB CYBER SECURITY DIH

*Aims to foster research and development, introduce **Cybersecurity innovation in the digital transformation** processes, supporting in this manner SMEs and Public Administration entities in their path to become more cyber resilient and cyber mature.*

CNCS

Digital Innovation Hub
C-HUB

- The C-HUB is a consortium composed by **seven entities**. Given the focus of the C-HUB and the characteristics of its members, the C-HUB has a national scope, and it is transversal to the various sectors.

- The multidisciplinarity of its members and its network, allows it to seek answers to local, regional, and national, or even international needs, and crossing the various sectors of the economy and society.

Digital Innovation Hub
C-HUB

- The C-HUB: Cybersecurity DIH, aims to **support the process of digital transformation, technology transfer**, to SMEs and Public Administration **by providing services, experimental laboratories and technical expertise focused on cybersecurity to foster the use of technologies and enhance their cyber resilience and maturity in a test-before-invest model**.

- This is achieved by **aggregating services provided by the partners**, **complementing each one's offer with a set of new services available through the Hub** and increase its **geographic coverage, responding in a more integrated and multidisciplinary** way to the needs of SMEs and Public Administration.

- The C-HUB can **provide experimentation and demonstration activities, prototyping, certification, and technology transfer in Cybersecurity**. These activities focus essentially in areas such **as incident response, intrusion detection, social engineering, industrial control systems, IoT, communication systems and networks, distributed systems and decentralised, cryptographic protocols, computer forensics, and blockchain**. The C-HUB also focus its attention on people’s empowerment and decision support by providing specialised **training and awareness**.

Digital Innovation Hub
C-HUB

Technology privacy and data privacy	Cryptanalysis	Quantum computing	Cryptography protocols
Mobile devices IoT and OT	Digital Identity	Incident response and Csirt Training	Intrusion detection
Social Engineering	Industrial control systems security	Forensics	Blockchain
Support to find investments/funding opportunities	Entrepreneurship and incubation	...	

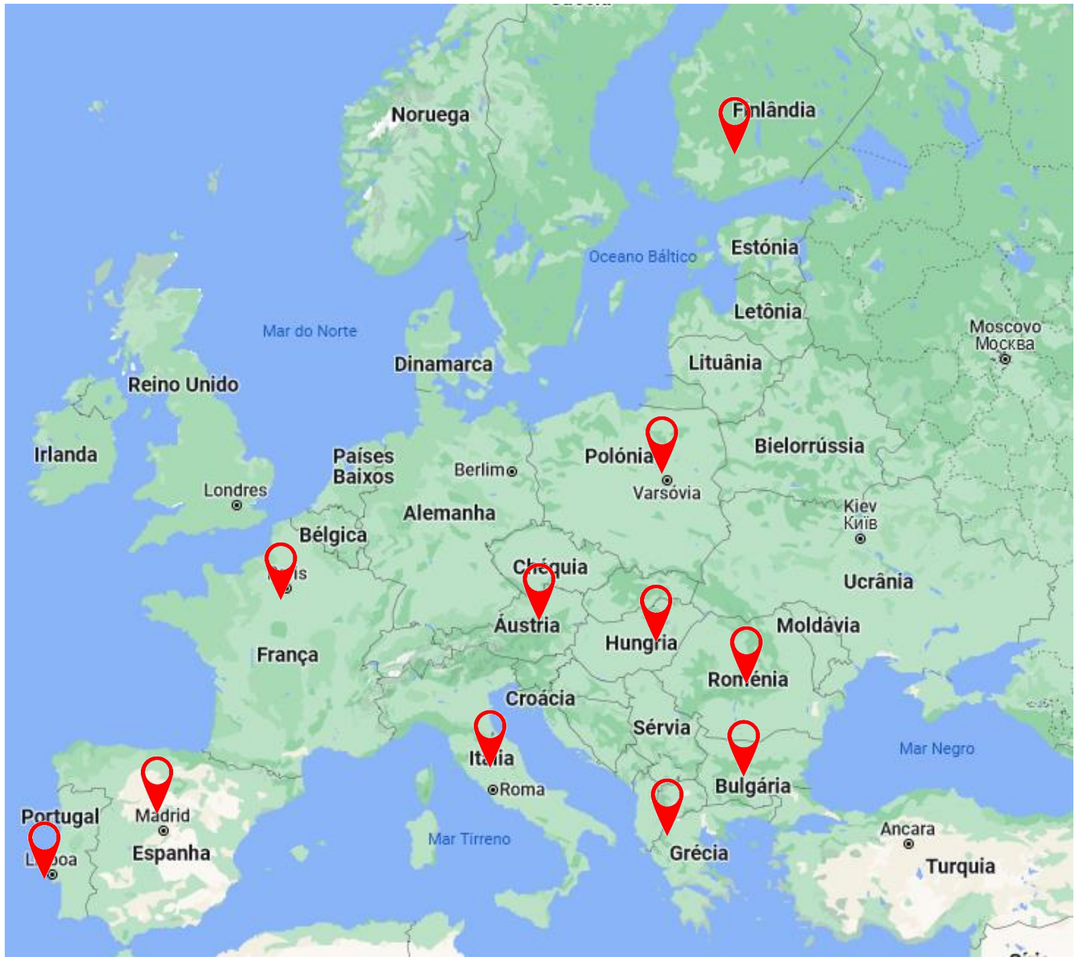
- HPC for classified information processing
- Innovation management centre
- Cryptographic and functional analysis laboratory
- IoT Laboratory focused to technology transfer
- Laboratory for national data transfer, interoperability and digital identity identification
- .
- .
- .

CNCS

Digital Innovation Hub
C-HUB

MoU’s – already established

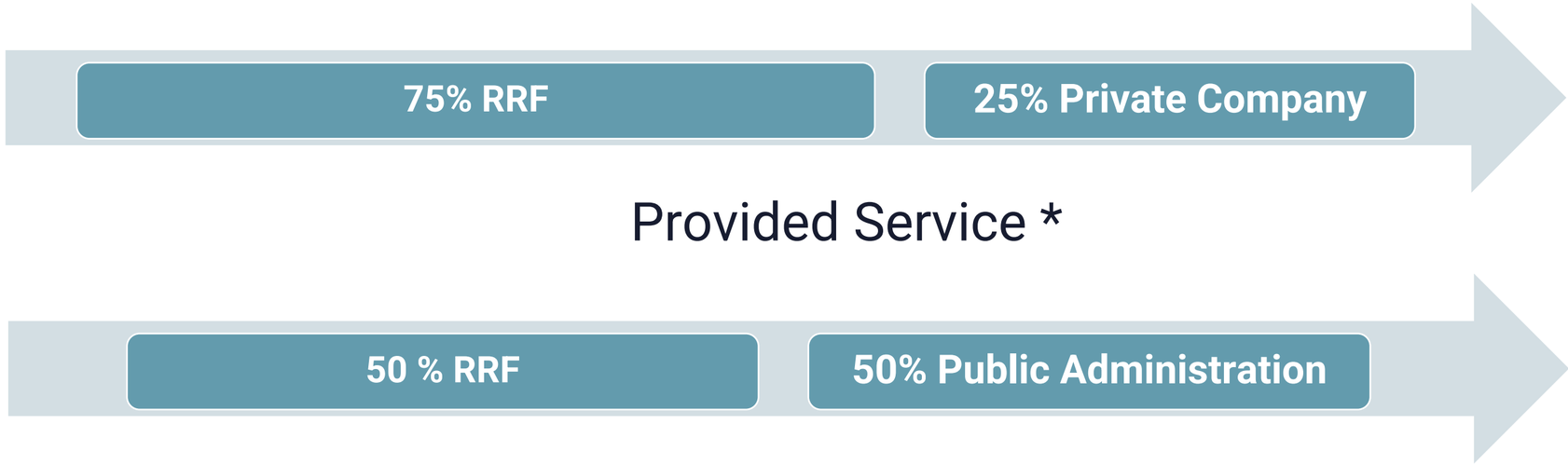
AI4PA (Portugal); CONNECT5 (Portugal); AzoresInnovationHUB (Portugal); DIH DIGIHALL (France); CEA (France); Robocoast DIH (Finland); DIGS3 (Spain); Futures of Innovation and Technology Digital Innovation Hub (Romania); Transylvania Digital Innovation Hub (Romania); LIVINGTRAC (Greece); CityInnoHub (Romania); RoTechNation (Romania); Digital Innovation Zone DIH (Romania);Tuscany X.0 (Italy); DanubeDIH (Romania); EDIH L’Artis (Bulgaria); HealthGoDigital! (Poland); CrowdInMotion (Austria).



Digital Innovation Hub
C-HUB

Providing support to companies:

- Open calls.
- Problem pitching.
- Direct approach.



* In some services the support can go up to 100%

National Coordination Centre
NCC-PT

- The **Digital Europe Programme** (DIGITAL) intends to **strengthen the capacities and capabilities of the European Union** in protecting its citizens and organisations by **enabling the conditions to improve the security of digital products and services**, thus contributing for a secure and functional Digital Single Market.

- With the presentation of the **European Union Cybersecurity Strategy for the Digital Decade** and the resolution on the EU's Cybersecurity Strategy for the Digital Decade, linked with the **work programmes and the Agenda defined by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)** (a component of the Digital Europe Programme, namely in its Specific Objective 3: Cybersecurity and trust), and the actions to be implemented within the scope of the **EU Cybersecurity Strategy for the Digital Decade** and the future NIS Directive, a further step was taken towards strengthening Europe's resilience against cyber threats, **putting the focus on collaboration between organisations and countries**.

National Coordination Centre
NCC-PT

- The NCC-PT aims to address the requirements and the tasks set laid out by the **Regulation (EU) 2021/887 establishing the ECCC and the Network of National Coordination Centres**. To fulfil its tasks and attributions the NCC-PT is based in a consortium coordinated by the CNCS assisted by two relevant National Agencies, the National Agency for Innovation S.A (ANI) and the Foundation for Science and Technology I.P. (FCT), **aiming to support cybersecurity capacities and capabilities building at the national leve**l and to **develop and enhance the national cybersecurity ecosystems** exploring the best synergies within the **Network of National Coordination Centres**.

- These include, for example, the **support to national policies on research, development and innovation** in line with the National Cybersecurity Strategy; to **provide technical assistance** and to **promote and facilitate the participation of national entities in projects in the field of cybersecurity** funded by European Union Programmes; to **promote research and development activities**; to **ensure that expertise is shared**; to promote **knowledge exchange with stakeholders and relevant actors at the national and European levels**; to **establish a cybersecurity community**; and to **promote awareness and mentoring activities**.

National Coordination Centre
NCC-PT

The activities to be performed by the NCC-PT follows the dispositions laid out by Article 7 of the Regulation (EU) 2021/887, seeking to contribute in a decisive and particular manner to:

- **Involve** as much as possible the relevant stakeholders within the **Cybersecurity Community** and **promote its engagement in the activities developed by the European Cybersecurity Competence Centre**;
- **establish synergies with relevant activities at national**, regional and local levels, **intertwining cybersecurity and research, development and innovation**, dovetailing with **national policies and strategies**;
- **support the uptake and dissemination of state-of-the-art cybersecurity solutions**;
- **promote and disseminate the outcomes** of the work of the **European Cybersecurity Competence Centre, the Network of National Coordination Centres, and the Cybersecurity Community**;
- **provide technical assistance** to stakeholders when **applying to projects**, in particular those managed by the European Cybersecurity Competence Centre; and
- **give financial support to third parties to implement specific actions** for which grants have been awarded by the European Cybersecurity Competence Centre.

Thank you for your attention

António Rio Costa - *antonio.costa@cncs.gov.pt*

Centro Nacional de Cibersegurança