The Italian cybersecurity action plan and the current cyber threat

Emanuele Urselli

Introduction

National Strategic Framework for Cyberspace Security - Strategic guidelines
Italian Action Plan - Action items
Core Tasks

Introduction

National Strategic Framework for Cyberspace Security - Strategic guidelines

1. Strengthening national Critical Infrastructures and other strategic players' defence capabilities
2. Improving cyber actors' technological, operational, and analytic capabilities
3. Encouraging public-private cooperation
4. Fostering cybersecurity culture
5. Supporting international cooperation on cybersecurity
6. Reinforcing counter-action capabilities against online criminal activities

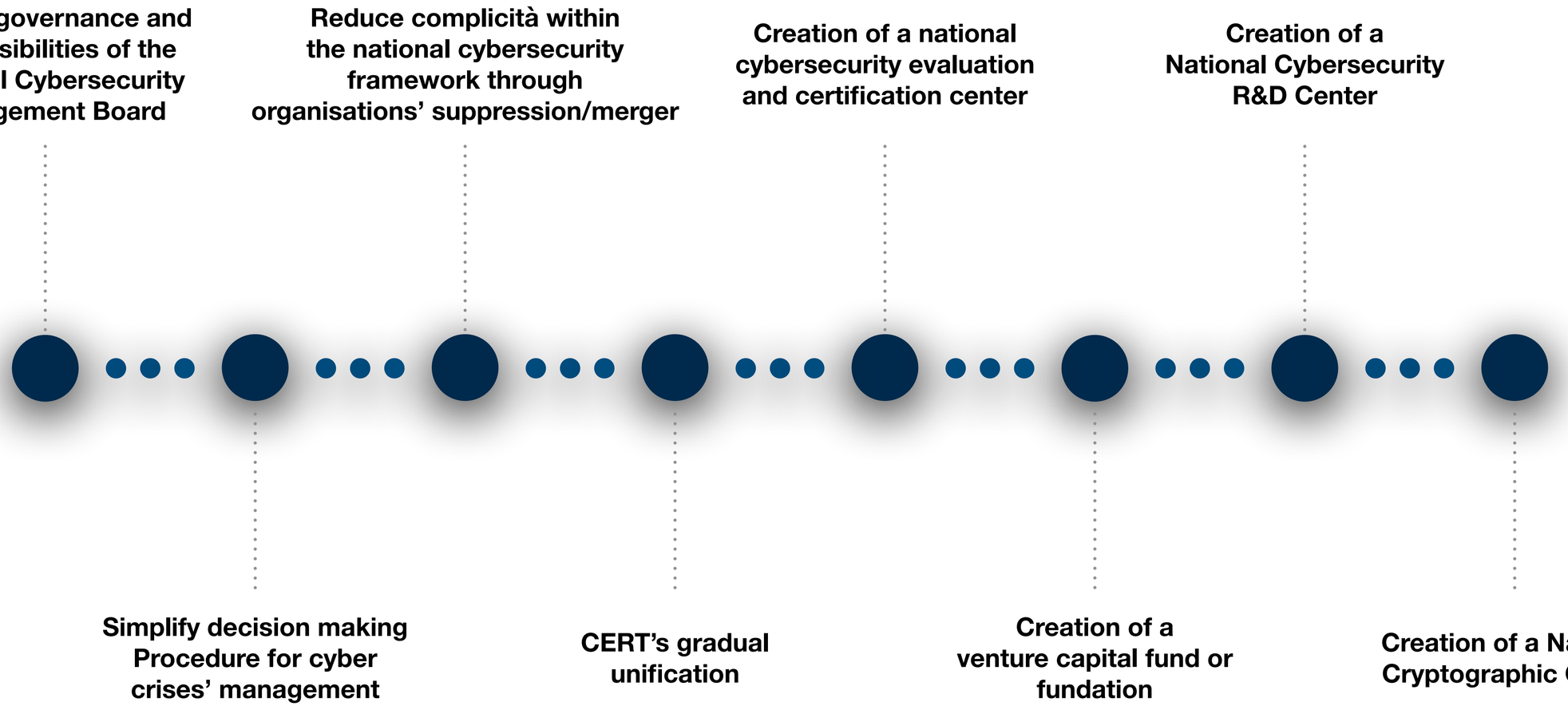
Introduction

Italian Action Plan - Action items

- **AI 1** Reinforcing intelligence, law enforcement, and defence capabilities
- **AI 2** Strengthening public-private cooperation
- **AI 3** Fostering IT security culture. Education and training
- **AI 4** International cooperation and cyber exercises
- **AI 5** Incident prevention, response and remediation
- **AI 6** Updating cybersecurity legislation and managing compliance at international level
- **AI 7** Security protocols and standards compliance
- **AI 8** Supporting industrial and technological development
- **AI 9** Strategic and operational communication
- **AI 10** Resources
- **AI 11** Implementing national cyber risk management

Introduction

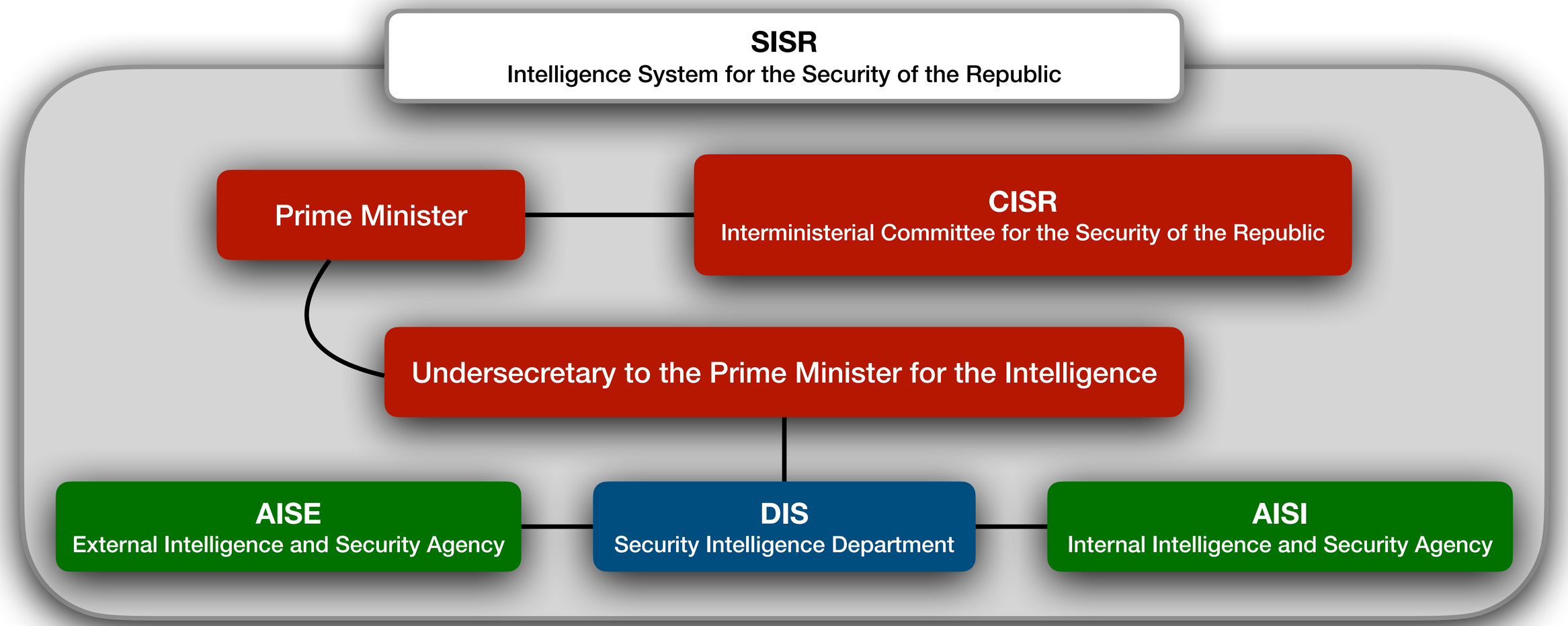
Core Tasks




Intelligence System
for the Security of the Republic

Intelligence System for the Security of the Republic

Organization

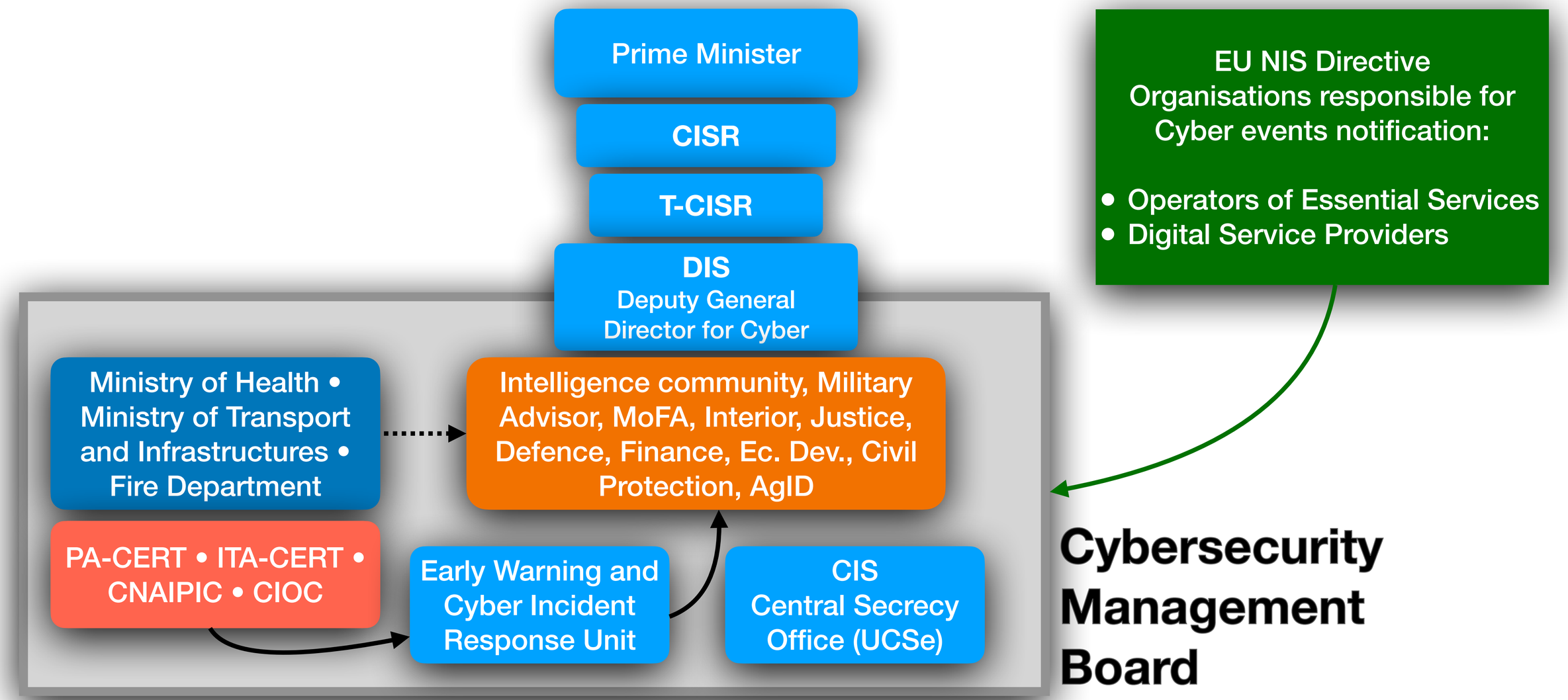


Italian Cybersecurity Core Tasks

Updated Cybersecurity Crisis Management System
National Cyber Security Framework

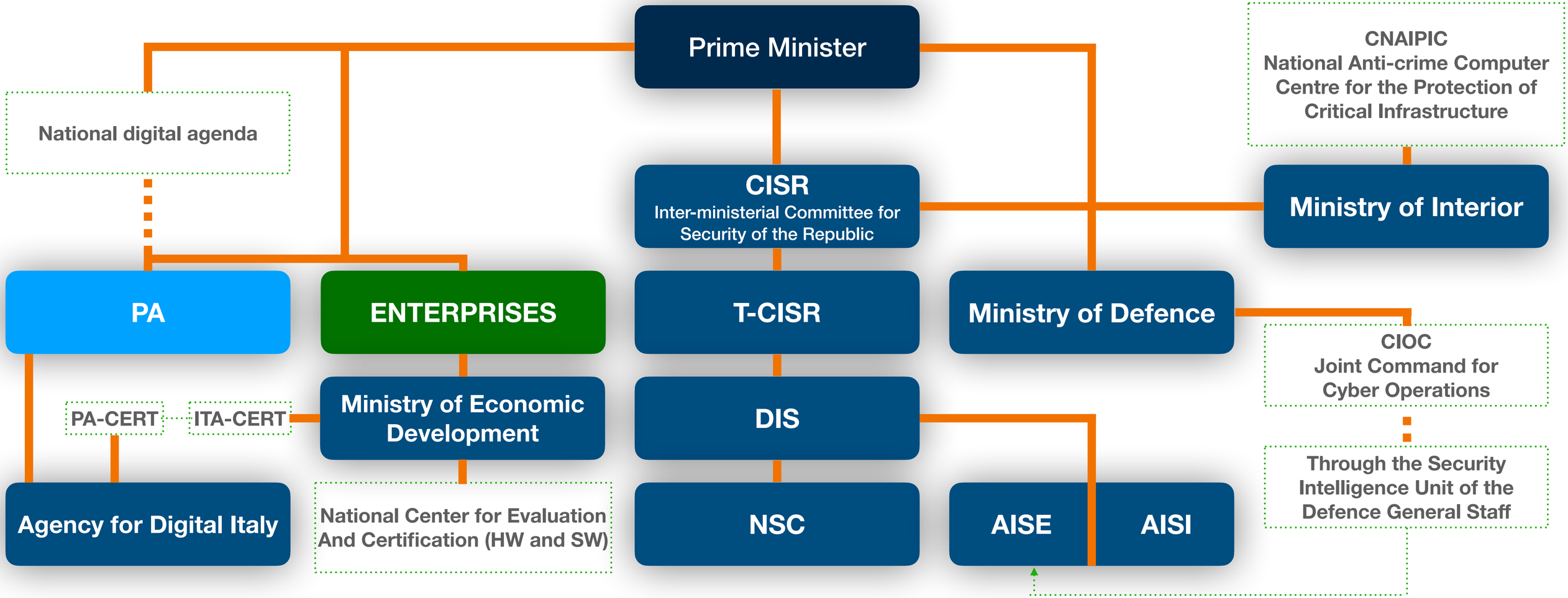
Italian Cybersecurity Core Tasks

Updated Cybersecurity Crisis Management System



Italian Cybersecurity Core Tasks

National Cyber Security Framework



Action items

Action item 1

Reinforcing intelligence, law enforcement, and defence capabilities

Threat and vulnerability analysis	Assess/Evaluate cyber threats and vulnerabilities
	Monitor technological innovations to anticipate potential vulnerabilities
	Share relevant analysis with OES and Critical Infrastructures
	Cooperate with universities and research centres
Cyber intelligence and cyber knowledge management	Improve capabilities on cyber threats
	Improve threat detection
	Implement early warning procedures
	Develop integrated intelligence capabilities

Countering cyber threats	Improve attribution capabilities
	Develop a consistent cyber situational awareness
	Facilitate info-sharing between public authorities and private sectors
	Improve incident and cybercrime integrated response capabilities
Cyberspace defines operational capabilities	Strengthen cyberspace defence structures
	Establish structures capable of cyberspace military operations planning/implementation
Cyber incident management	Create relevant tools for managing cyber incidents

Action item 2

Strengthening public-private cooperation

Public-private sector's cooperation tools	Process a methodology to identify ICT critical systems
	Strengthen info-sharing, also by adopting common taxonomy
	Develop synergies among Critical infrastructures' competent Authorities, Ministries, private organisations, and partner Nations to manage cyber crises
	Set specific evaluation standards and develop communication formats for infrastructures' vulnerability assessments

Integration	Facilitate operability of public-private existing cooperation schemes
	Support activities implemented by competent bodies involving Critical Infrastructures and OES
Involve private players in national and international cybersecurity events	Consolidate existing public-private communication
	Facilitate private operators' involvement in international exercise on Critical Infrastructures' protection

Action item 3

Fostering IT security culture. Education and training

Education, training, and exercises	
Partecipate in EU, NATO, and other international organisations' cybersecurity initiatives	Concentrate cyber training capacities in education excellence hubs
Raise awareness among decision makers on cybersecurity threats' latest developments	Develop partnerships with universities and research centres
Organize training exercise	Map national cybersecurity excellence centers
Develop, test, and validate cyberspace operational activities	

Doctrine development
Keep up with the latest international strategic posture

Cybersecurity awareness
Organize awareness initiatives

Action item 4

International cooperation and cyber exercises

EU projects and other international organizations' initiatives	Promote and ease access to EU funding initiatives among public and private operators
	Maximize access to EU funding
	Partecipate in EU funded projects
	Partecipate in NATO and other International organisations projects

Enhancing bilateral and multilateral cooperation	Consolidate relations with EU and NATO members, and other partner nations
	Maximize integration and interoperability of cybersecurity operations' planning and implementation
	Participate in international fora
Cyber exercises	Organize recurring national cyber exercises
	Coordinate public and private national players participating in exercises

Action item 5

Incident prevention, response and remediation

Integrated capacity	Create a single point of contact and one or more CSIRT
	Establish one or more NIS National Authorities
	Fully implement legal framework for CSIRT/ CERT, SOC, and teams
	Align capacities of current national cybersecurity actors with NIS requirements
	Develop automated and standardised cyber incident management model
	Minimize the impact of IT cyber incidents
	Develop a proactive approach to IT security
	Develop a resilient approach

CERTs development	Develop CERTs functions according to the NIS Directive
	Increase CERTs' efficacy
	Find efficient approaches to support Local PA
	Support EU and international cooperation among CERTs
Procurement	Define PAs' purchasing mechanisms
	Identify procurement regulations and procedures for a cyber secure Public Administration supply chain

Action item 6

Updating Cybersecurity Legislation and Managing Compliance at International Level

Legislation update	Share PAs' best practices and coordinate their legal cybersecurity capabilities
	Assess current legislation on cybersecurity
	Finalize critical infrastructures' national legislation bearing in mind sectors covered by the NIS Directive
	Harmonize national obligations for public and private operators
	Promote initiatives at EU level to harmonize legal obligations and to simplify processes
Attribution and sanctions	Create a legal framework for the attribution of security violations by network managers and users

National legal framework	Update legal framework on cybersecurity
	Introduce legal provisions for the deployment of tools aimed at detecting cyber threats
Directive concerning measures for s high common level of security of networks and information systems across the Union (2016/1148)	Promote dialogue with private operators facilitate the NIS Directive transposition process
	Assess impact of the NIS Directive over the National Cybersecurity Architecture to align national regulations
	Transpose the NIS Directive and unify new requirements with those concerning Critical Infrastructures

Action item 7

Security Protocols and Standards Compliance

ICT security certification	Manage the National Framework for ICT Certification of un-classified products/services through the CSCO
	Keep the national scheme for certification of information systems' processes up to date
	Enhance operational capability of the Evaluation Center
	Take part to the activities carried out by international organisations
	Increase evaluation competences of DIS-UCSe
Cyber defence measures for Essential Service Providers and Critical Infrastructures	Test protection systems on a regular basis
	Establish an independent control system

Standardization and compliance	Update the national framework to international standards
	Identify and update basic security measures for PA and Critical Infrastructures network and information systems
	Adopt standards, best practices, and minimum requirements to enhance security of networks and information systems
	Establish a validation and an audit system for organizations responsible for issuing digital and IT security certificates
Reference documents	Assess impact of the NIS Directive over the National Cybersecurity Architecture to align national regulations
Updating cybersecurity management programs	Transpose the NIS Directive and unify new requirements with those concerning Critical Infrastructures

Action item 8

Supporting Industrial and Technological Development

Production, Innovation and Technological Cooperation	Stimulate the creation of a secure and resilient supply chain for ICT components
	Promote ICT innovation to develop a competitive industrial base at national and international level and facilitate the creation of a vertical supply chain based on security-by-design
	Enhance bilateral and multilateral cooperation programs to improve national R&D at both EU and international level
National laboratory for comparative analysis	Facilitate the creation of a government laboratory for comparative analysis of ICT systems to be adopted by PAs and Critical Infrastructures

Action item 9

Strategic Communication

Strategic and operational communication
Develop coordination capacity on situational awareness to increase communication efficiency, to facilitate response and remediation activities and to identify appropriate communication channels

Action item 10

Resources

Evaluation of cyber-events relevant costs	Identify relevant metrics for the evaluation of cyber-events' economic impact
	Analyze Critical Infrastructures' interdependencies to improve the evaluation of cyber-events' economic impact in case of a "domino effect"
	Map incidents and potential scenarios from an economic point of view
Financial planning	Identify priorities and budget related to Critical Infrastructures' cybersecurity and cyberdefense
Promoting efficient spending	Implement efficient cyberdefence spending measures at national and international level
Human capital	Facilitate inter-institutional coordinated recruitment activities of speicialized resources

Action item 11

Implementing National Cyber Risk Management

Methodology	Adopt risk evaluation measures at national level
	Identify a unique and agreed cyber-risk management methodology for essential services, Critical Infrastructures and other national strategic actors
	Engage research sector and Academia in developing performing risk management tools

The Cyber Threat

Extract from the annual intelligence report to parliament

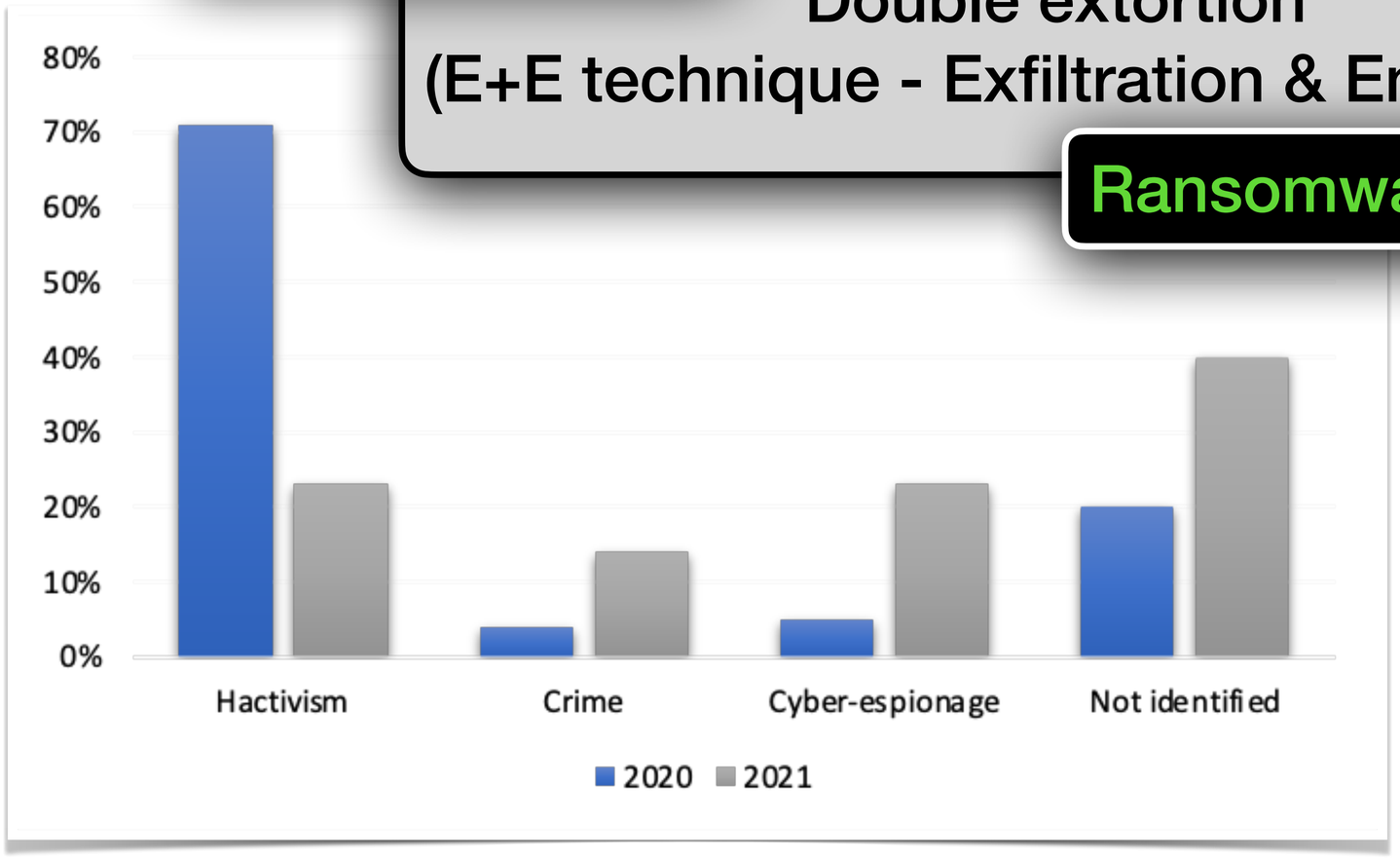
The Cyber Threat

Status and trend of the Cyber Threat (Part 1)

RANSOMWARE

Double extortion
(E+E technique - Exfiltration & Encryption)

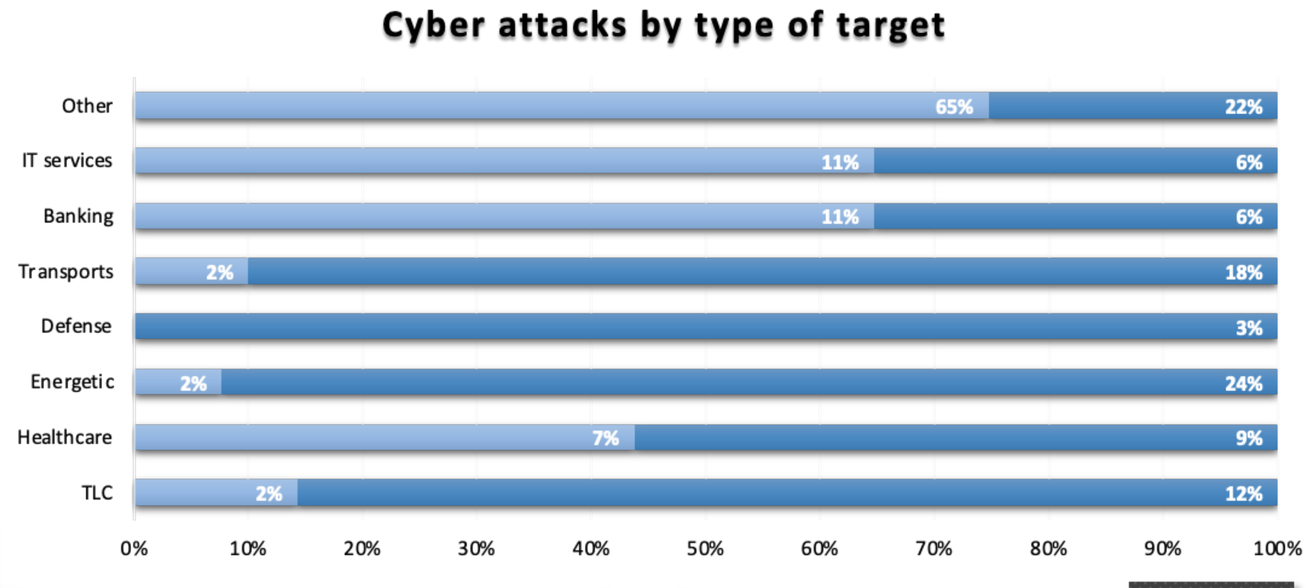
Ransomware-as-a-Service (RaaS)

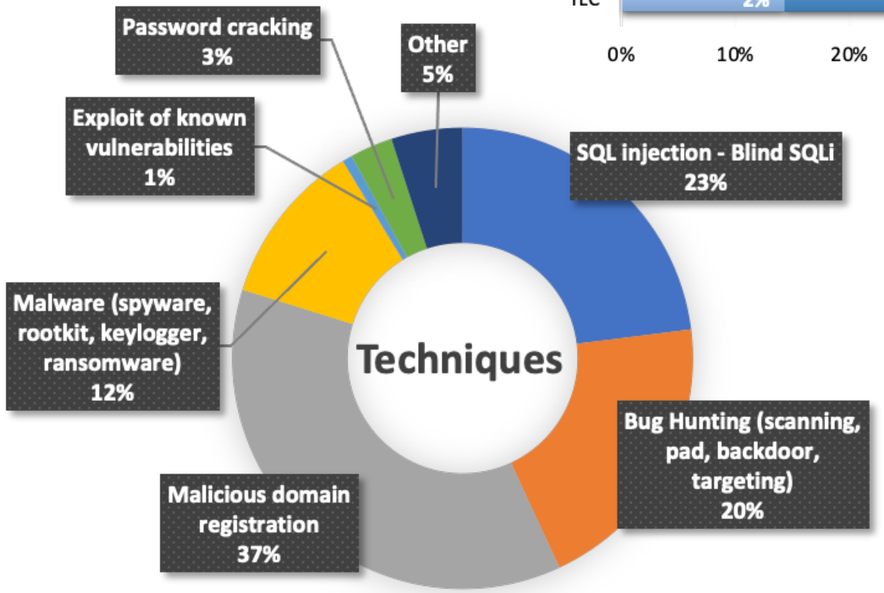


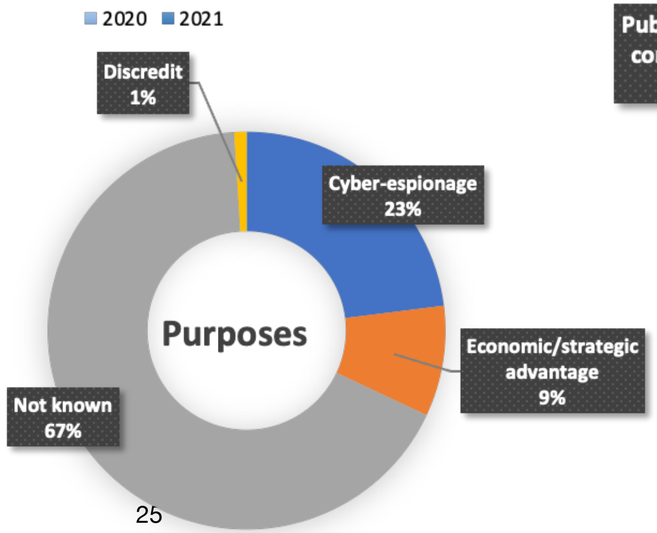
Cyber attacks by type of actors

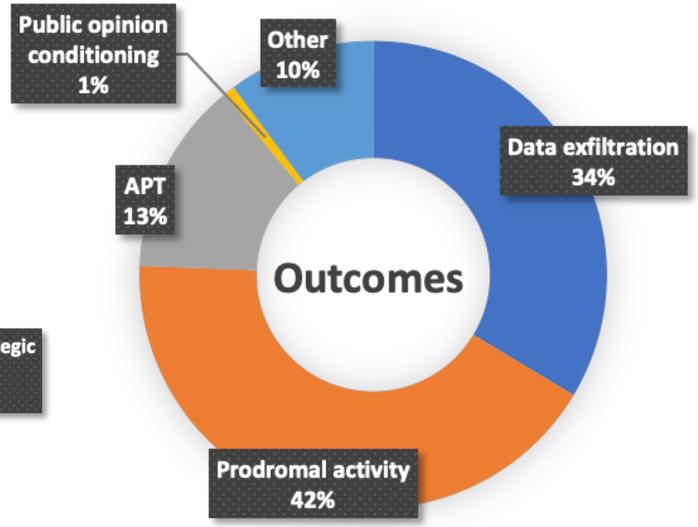
The Cyber Threat

Status and trend of the Cyber Threat (Part 2)



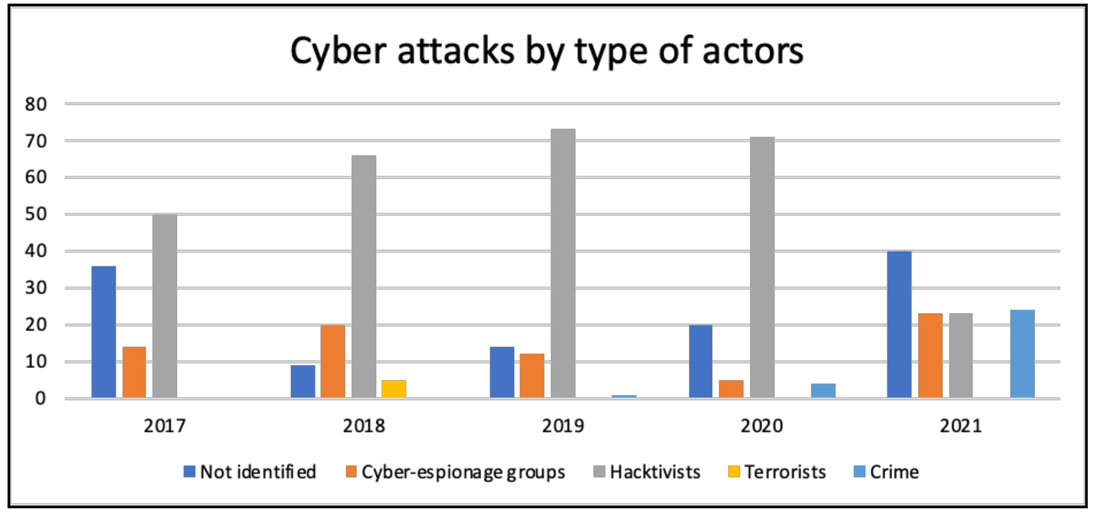


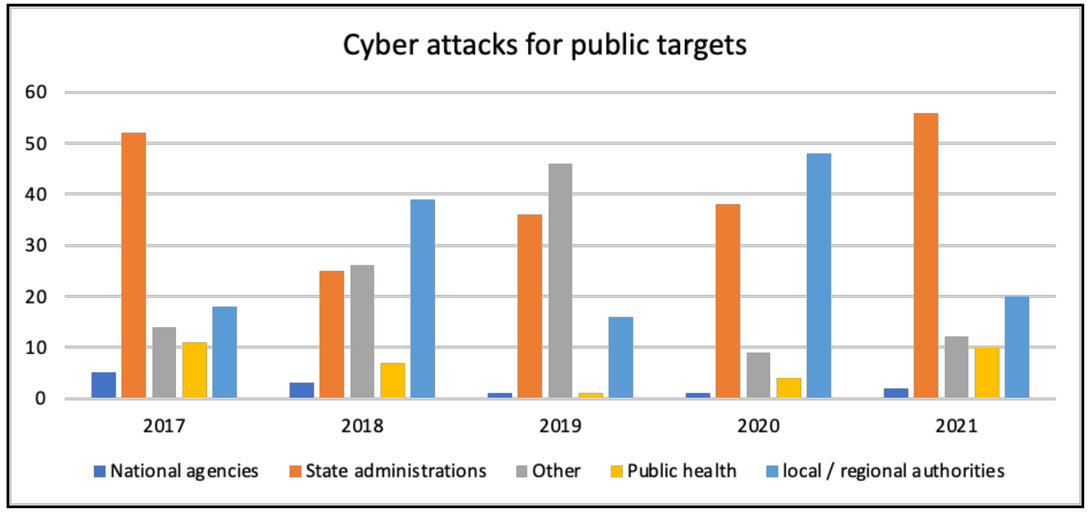


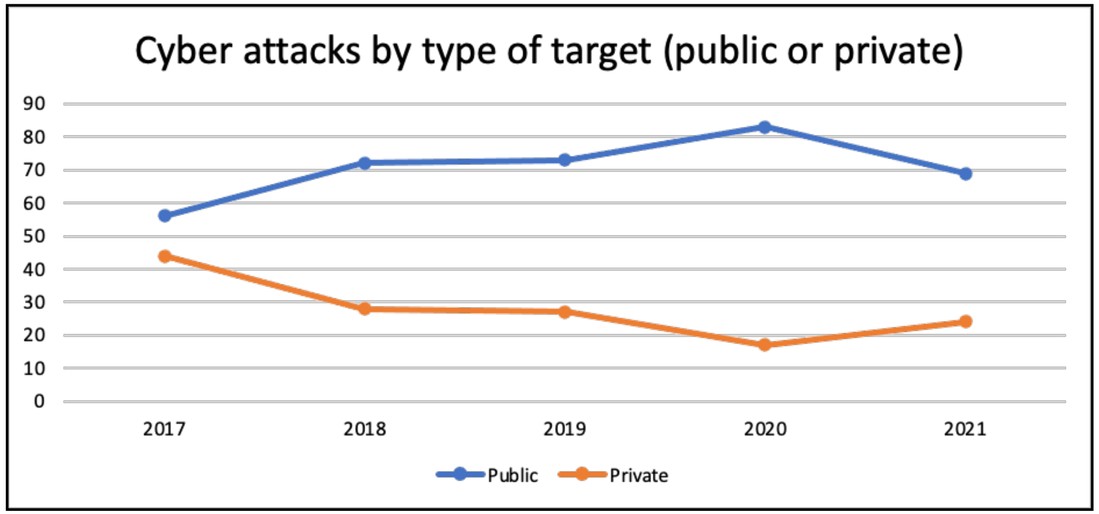


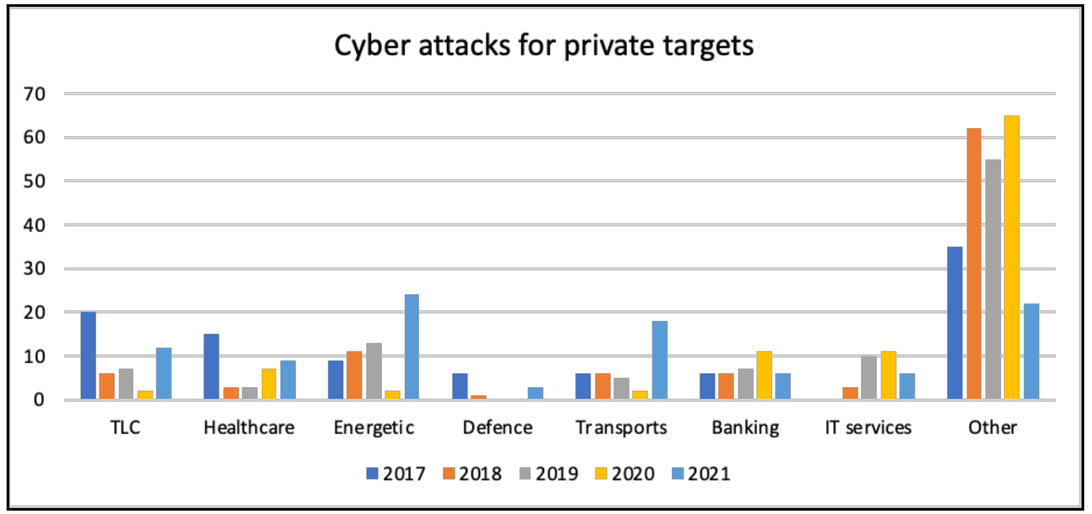
The Cyber Threat

Differences from 2017 to today









The Cyber Threat

Synergies with ACN

It supports national public and privare entities in the prevention and mitigation of accidents

It pursues national and European autonomy in the digital sector

It favours training courses for the development of the workforces and promotes awareness campaigns

THANK YOU

for your precious time and attention