Fostering Digital Sovereignty

Fabio Martinelli

National Research Council of Italy

Several perspectives

- Concepts from SPARTA competence network
- One approach from SERICS the Italian partnership in cyber security
- Digital sovereignty as part of the (European Cyber Security Organization) ECSO Vision for the future

“Cybersecurity is no longer a technological ‘option’, but a societal need”

Digital sovereignty is a multidisciplinary concept derived from the legal concept of self-determination and applied to the digital sphere, to address the unique challenges to individual and collective autonomy arising with increasing digitalization of many aspects of society and daily life.

THE SPARTA ROADMAP For Digital Sovereignty

SPARTA is one of the 4 Pilot Compentence Network

The Roadmap has been elaborated by a committee involving FhG, INRIA and CNR

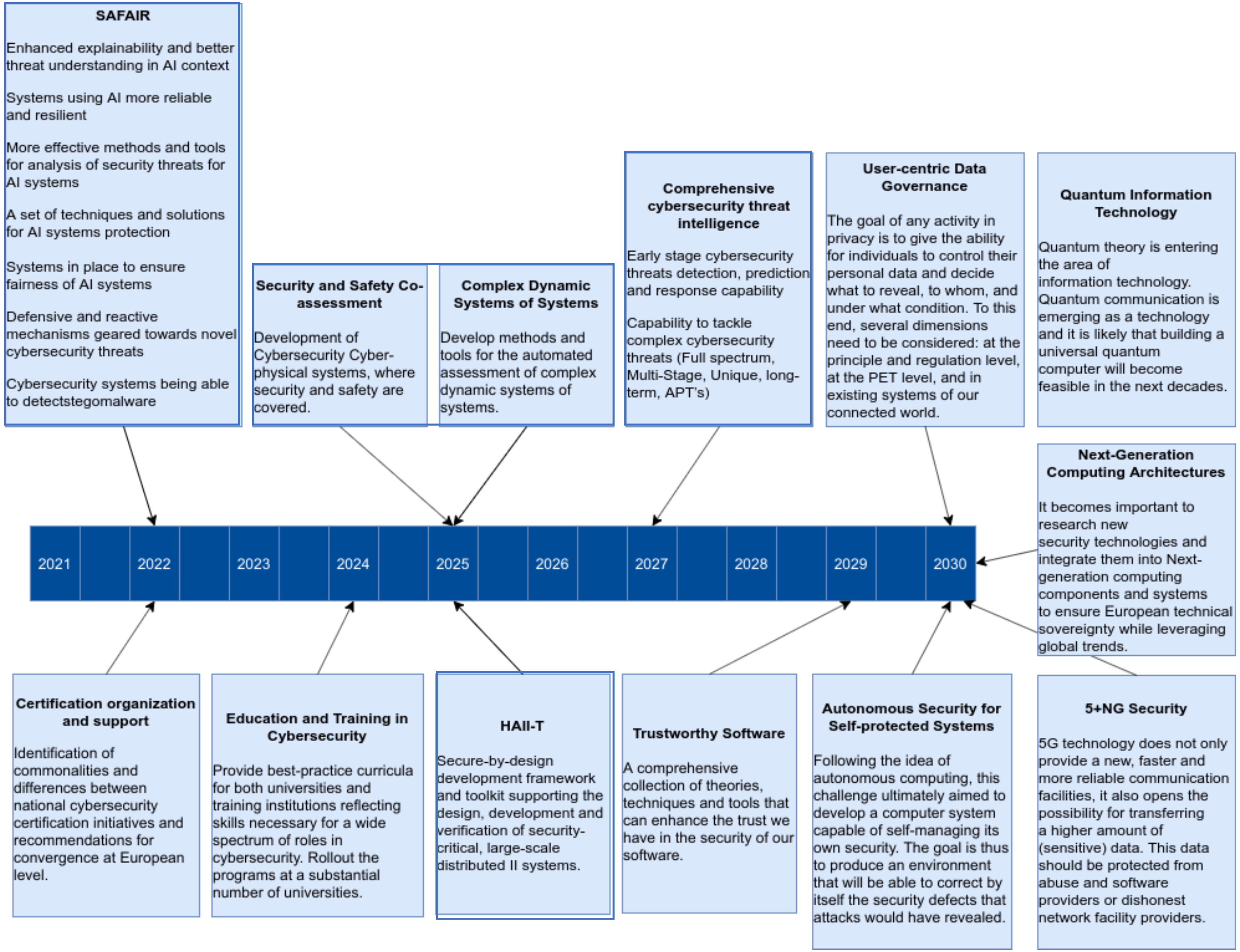
Introduces **13 Mission Programmes**

Defined milestones for each MP based on three dimensions:

Technology

Education

Certification



SAFAIR

Enhanced explainability and better threat understanding in AI context

Systems using AI more reliable and resilient

More effective methods and tools for analysis of security threats for AI systems

A set of techniques and solutions for AI systems protection

Systems in place to ensure fairness of AI systems

Defensive and reactive mechanisms geared towards novel cybersecurity threats

Cybersecurity systems being able to detectstegomalware

Security and Safety Co-assessment

Development of Cybersecurity Cyber-physical systems, where security and safety are covered.

Complex Dynamic Systems of Systems

Develop methods and tools for the automated assessment of complex dynamic systems of systems.

Comprehensive cybersecurity threat intelligence

Early stage cybersecurity threats detection, prediction and response capability

Capability to tackle complex cybersecurity threats (Full spectrum, Multi-Stage, Unique, long-term, APT's)

User-centric Data Governance

The goal of any activity in privacy is to give the ability for individuals to control their personal data and decide what to reveal, to whom, and under what condition. To this end, several dimensions need to be considered: at the principle and regulation level, at the PET level, and in existing systems of our connected world.

Quantum Information Technology

Quantum theory is entering the area of information technology. Quantum communication is emerging as a technology and it is likely that building a universal quantum computer will become feasible in the next decades.

Next-Generation Computing Architectures

It becomes important to research new security technologies and integrate them into Next-generation computing components and systems to ensure European technical sovereignty while leveraging global trends.

Certification organization and support

Identification of commonalities and differences between national cybersecurity certification initiatives and recommendations for convergence at European level.

Education and Training in Cybersecurity

Provide best-practice curricula for both universities and training institutions reflecting skills necessary for a wide spectrum of roles in cybersecurity. Rollout the programs at a substantial number of universities.

HAII-T

Secure-by-design development framework and toolkit supporting the design, development and verification of security-critical, large-scale distributed II systems.

Trustworthy Software

A comprehensive collection of theories, techniques and tools that can enhance the trust we have in the security of our software.

Autonomous Security for Self-protected Systems

Following the idea of autonomous computing, this challenge ultimately aimed to develop a computer system capable of self-managing its own security. The goal is thus to produce an environment that will be able to correct by itself the security defects that attacks would have revealed.

5+NG Security

5G technology does not only provide a new, faster and more reliable communication facilities, it also opens the possibility for transferring a higher amount of (sensitive) data. This data should be protected from abuse and software providers or dishonest network facility providers.

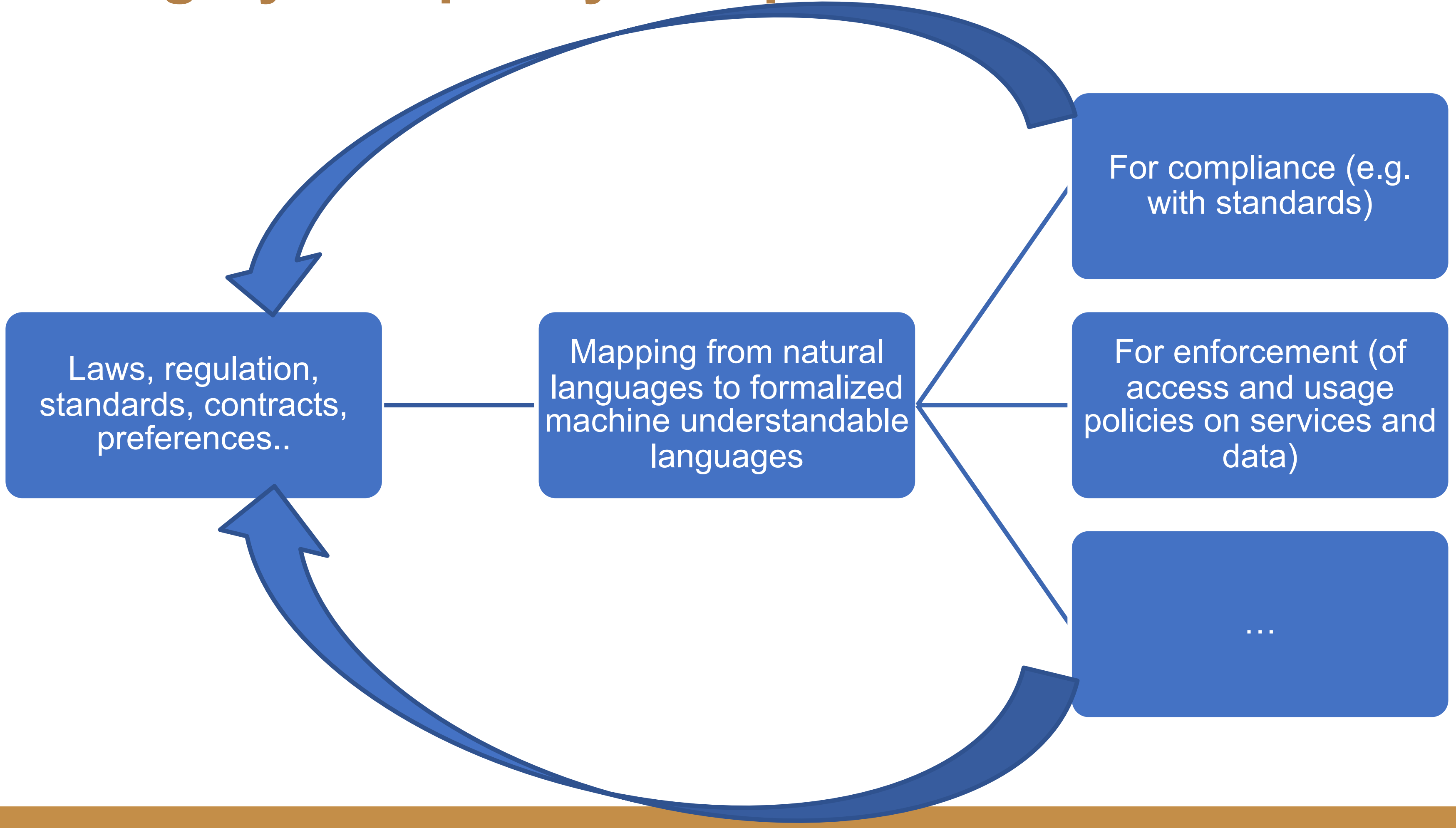
Focus on Data Sovereignty

- “Data sovereignty as the self-determination of individuals and organizations (and states) about how to control their data”
  - As part of digital sovereignty

From the State of Union speech 2020

…. technology where we can control ourselves what **data** and **how data** is used…..

Data sovereignty and policy compliance and enforcement



Laws, regulation, standards, contracts, preferences..

Mapping from natural languages to formalized machine understandable languages

For compliance (e.g. with standards)

For enforcement (of access and usage policies on services and data)

…

DiSe in a nutshell

Digital sovereignty entails capability of citizens, organizations and states to control their data, usage of such **data** and their **computations** and ensure those are compliant with business rules, laws, social norms, usability, privacy and/or other **human, social, and legal (HSL)** aspects.

We study **methods** to extract knowledge and rules and then translate those into data and computation usage policies and verify these policies and assess their **compliance**; we build mechanisms **for data usage control** enforcement for scenarios as iot, big data, cloud…

- **Economic** aspects as understanding costs and incentives for data sharing, and the value of data sovereignty and interactions and conflict management between laws and market
- We study **data sovereignty and trust models** by providing proper data sharing approaches and corresponding policies on derived data/algorithms.
- Data are also instrumental to full situation awareness for **threats to digital services**. We need specific technologies for ensuring data sovereignty of cyber threat intelligence (CTI), providing data credibility and integrity, mandatory data routing and compliant data flow control

A main focus is on **confidentiality and compliance of computations** that should be done in agreement with laws, norms and standards, in particular for secure analytics:

- We research in privacy preserving computation, social behavior analysis, and analytics for malware/ransomware
- We research on full spectrum awareness of cyber and physical threats through proper data sharing and analysis
- We develop advanced testing approaches for access and usage control policies will be defined and developed.

We plan Lab validation of methodologies/tools in at least ones of the possible scenarios as **smart grids, social communities, transport or e-health.**

ECSO Roadmap

ECSO is an industrial association in cyber security that counts more than **300** Members + a few thousand indirectly via Associations

ECSO WG6 is devoed to roadmapping activities.

WG6 ORGANISATION: Current WG6 activities largely focus on the definition of R&I priorities

- **SWG 6.1 “Ecosystem”**
- **SWG 6.2 “Digital Transformation in Verticals”**
- **SWG 6.3 “Data and Economy”**
- **SWG 6.4 “Basic and Disruptive Technologies”**
- **SWG 6.5 “Cybersecurity for Defence and space”**

REPORTS & STRATEGIC DOCUMENTS

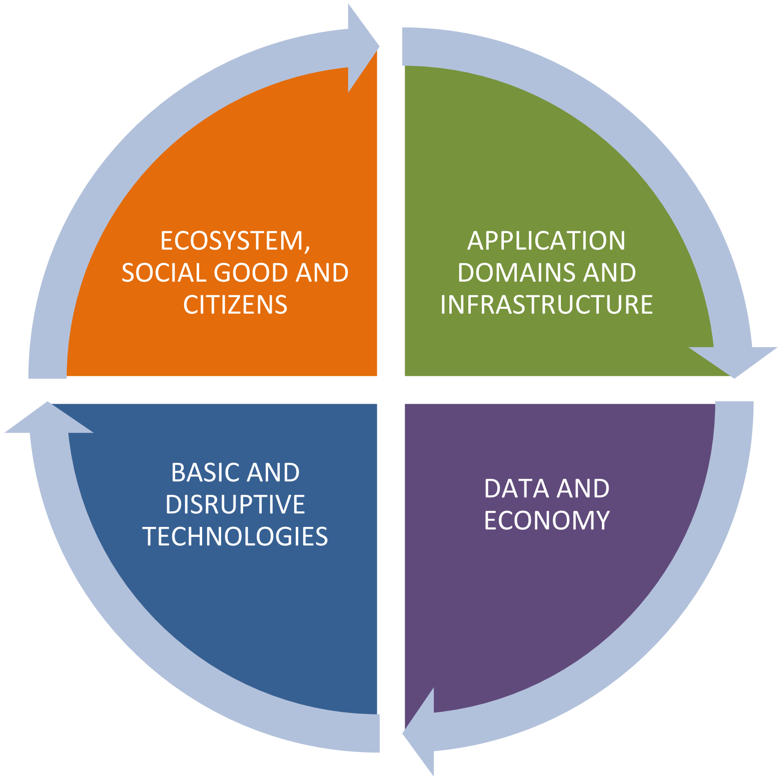
- **Technical papers on Digital Twins, Artificial Intelligence, Internet of Things and Blockchain on going**
- **Vision papers on cyber security priorities towards Horizon Europe** (ECSO 2021-2027 vision): ongoing activity.

COLLABORATIONS

- the ECSO technical papers will be used to continue the collaboration with the cPPPs. A joint paper will be proposed where cyber security will be the glue factor to present common challenges with all relevant stakeholders-

Area	Code	Priority
ECOSYSTEM, SOCIAL GOOD AND CITIZENS	HEU.1.A	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification
	HEU.1.B	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP
	HEU.1.C	Development of digital forensics mechanisms and analytical support
	HEU.1.D	Cyber ranges and simulation environments
	HEU.1.E	Cyber-physical systems security and cyber secure pervasive technology
APPLICATION DOMAINS AND INFRASTRUCTURE	HEU.2.A	Cyber resilient digital infrastructures
	HEU.2.B	Secure Quantum Infrastructures
	HEU.2.C	Cyber secure future communication systems and networks
	HEU.2.D	Vertical sectors cyber challenges
	HEU.2.D1	Industry 4.0 and ICS
	HEU.2.D2	Energy (oil, gas, electricity), and smart grids
	HEU.2.D3	Transportation (road, rail, air; sea, space)
	HEU.2.D4	Financial Services, e-payments and insurance
	HEU.2.D5	Public services, e-government, digital citizenship
	HEU.2.D6	Healthcare
	HEU.2.D7	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities
	HEU.2.D8	Robotics security
	HEU.2.D9	Agrifood
DATA AND ECONO MY	HEU.3.A	Data security and malicious use of data
	HEU.3.B	End-to-end Privacy
	HEU.3.C	Economic aspects of cybersecurity
BASIC AND DISRUPTIVE TECHNOLOGIES	HEU.4.A	Secure and Trustworthy Artificial Intelligences
	HEU.4.B	Software and hardware cybersecure engineering and assurance
	HEU.4.C	Cryptography
	HEU.4.D	Blockchains and Distributed Ledger technologies
	HEU.4.E	IoT Security
	HEU.4.F	Artificial Intelligence techniques for better security and malicious use of AI
SUPPORT TO POLICY IMPLEMEN TATION	DEP.1.A	Develop tools to support the implementation of EU Cybersecurity Act
	DEP.1.B	Threat management and cross-vertical platforms
	DEP.1.C	Governance, policy and legal aspects
SUPPORT TO TECHNOLOGY IMPLEMENTATION	DEP.2.A	Deploying resilient digital infrastructures in the field
	DEP.2.B	Platform for privacy management
	DEP.2.C	Platform and processes for wide-scale digital identity in Europe: decentralised technologies, self-sovereign identity and blockchain
	DEP.2.D	Establishing an engineering platform for trustworthy hardware, software. and systems

ECSO priorities for HE and DEP definied in 2020


ECOSYSTEM, SOCIAL GOOD AND CITIZENS
APPLICATION DOMAINS AND INFRASTRUCTURE
BASIC AND DISRUPTIVE TECHNOLOGIES
DATA AND ECONOMY

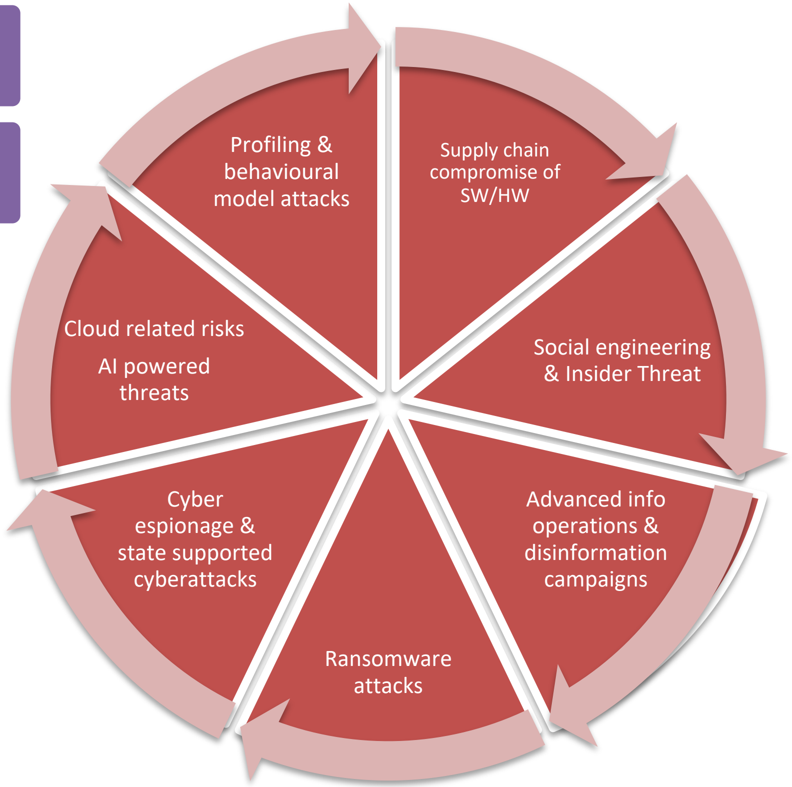
WG6 – SRIA and Cyber Security Technologies – Civilian, dual use and space

Cybersecurity trends: a draft vision

- Resilience (SP1)
- Digital Autonomy (SP2)
- Strategic Sovereignty (SP3)
- Fundamental rights (SP4)

Four main pillars

An initial analysis of cybersecurity threats


Profiling & behavioural model attacks
Supply chain compromise of SW/HW
Social engineering & Insider Threat
Advanced info operations & disinformation campaigns
Ransomware attacks
Cyber espionage & state supported cyberattacks
Cloud related risks
AI powered threats

Complex ecosystem of factors

GEOPOLITICAL

- Cyberspace will continue to become a force multiplier
- Creation of EU multinational cyber structures
- US and China will reduce technological dependency
- Non-EU ownership over submarine cables
- Non-EU companies will control VPN providers
- Non-state actors in cyber operations
- Cyber threats in information campaign to create instabilities

ECONOMIC

- Increase in cybercrime
- Disruptive Technologies will increase consistently EU GDP
- Increase in cyber spending
- Adversarial machine learning deployed to target critical infrastructure

SOCIAL

- Surge in attacks to privacy and data protection
- Increase in digital connectivity
- Growth of Tech Skeptics
- Use of disruptive technology for fake news campaigns
- Increase in cyber education and awareness
- Increase in digital skills shortages
- Growing involvement of national governments in digital matters

TECHNOLOGICAL

- Global landscape characterized by Intelligent, Interconnected, Distributed and Digital technologies, such as AI, 6G, IoT, edge and cloud computing.
- Quantum technology (PQC, QCI, QKD)
- Augmented reality, virtualisation, digital twins and metaverse
- Data spaces
- IT predominately impacting OT operations
- Advent of EDTs, which are becoming more accessible
- New strategic emerging sectors: Robotics, Autonomous driving, Space, Bionics, etc.

Thanks and join our efforts and discussions!!!