European Commission

FIRST CYBER SECURITY JOINT PROJECT WORKSHOP

29 November 2019

1ST CYBER SECURITY JOINT PROJECT WORKSHOP

29 November 2019 10:00 – 16:30

Room S1 BU 25, Avenue de Beaulieu, 25 - Brussels

Agenda

Introduction

European Cyber Atlas

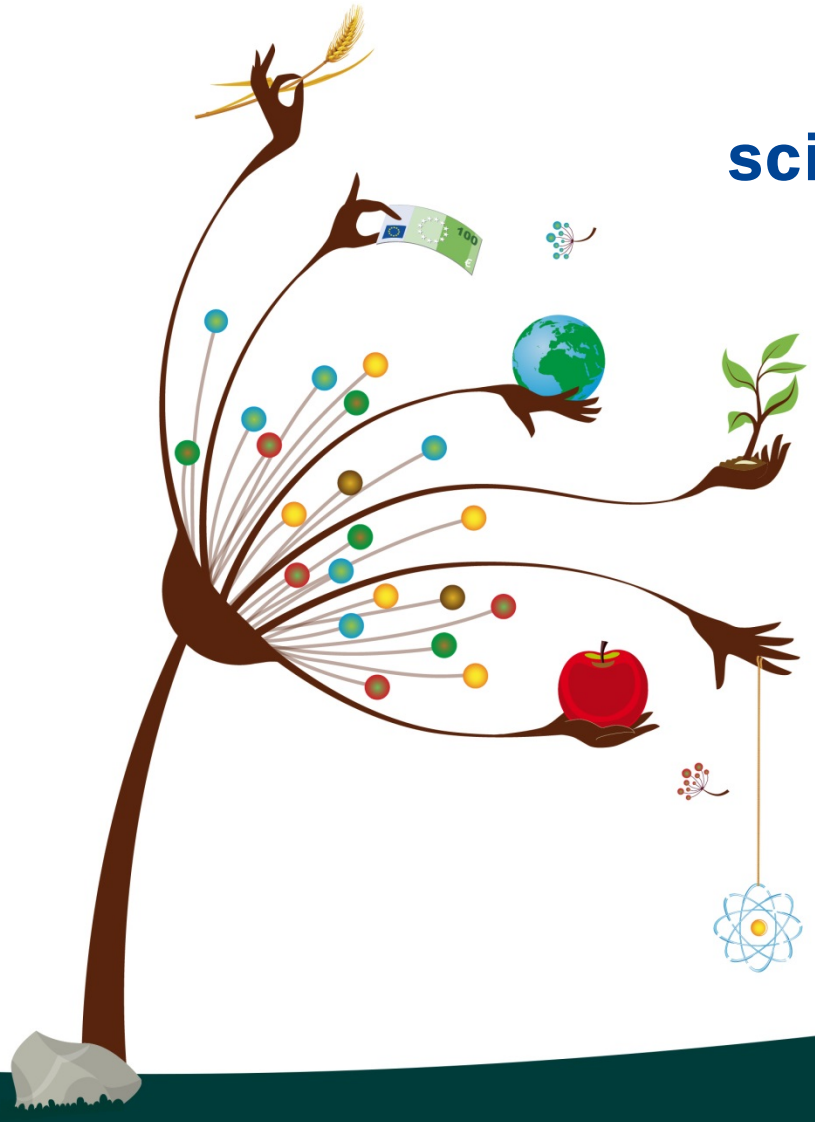
Presentations followed by discussions

- *Cyber ranges/skills, data lakes, AI tools and Cyber Thread Intelligence*
- *Cyber secured hardware, operating system and middleware*
- *Cybersecurity and quantum technologies: Quantum Key Distribution, Quantum Communication Infrastructure, quantum computing*
- *Certification tools and standards*

Conclusion

European Commission

European Commission



The European Commission's science and knowledge service

Joint Research Centre

Cybersecurity Atlas

Igor Nai Fovino

Deputy Unit Head

Cyber and Digital Citizens' Security Unit

Space, Security and Migration Directorate

DG-JRC

Joint Research Centre

Why an Atlas

A one stop shop…

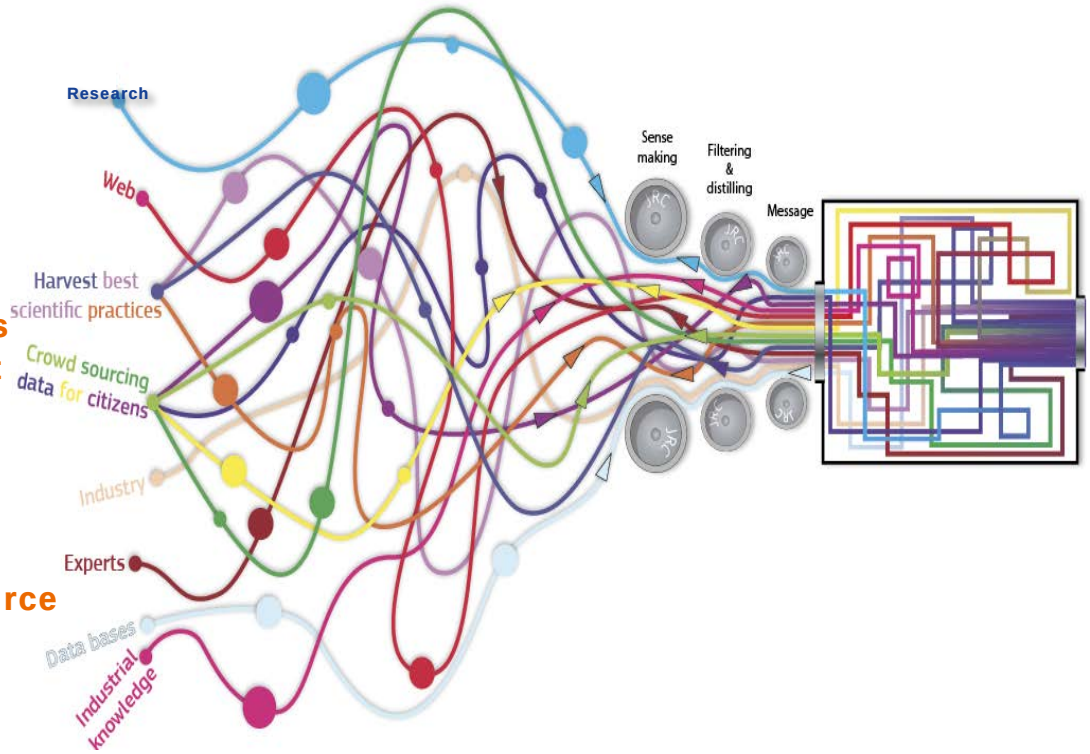
- Providing a comprehensive mapping of the European Cybersecurity landscape
- Facilitating the networking among cybersecurity R&D actors in Europe
- Enabling the identification of weaknesses in the European Cybersecurity value chain (including the Strategic Autonomy aspects)
- Supporting the decision-making process for policy interventions
- Facilitating the coordination of national initiatives
- Supporting the future European Cybersecurity Research and Competence Centre

Ingredients

Taxonomy

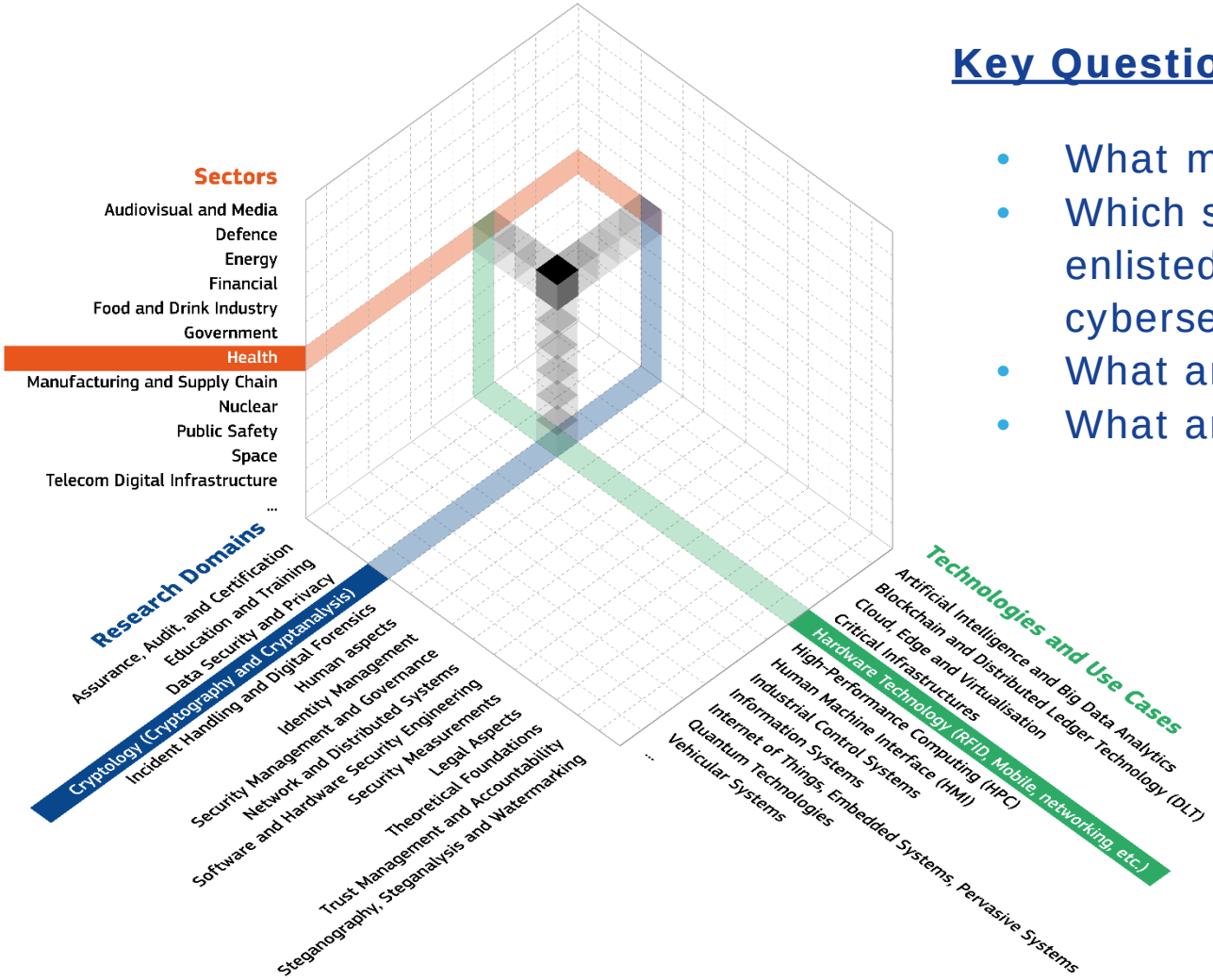
Stakeholders Engagement

Online Resource Analysis



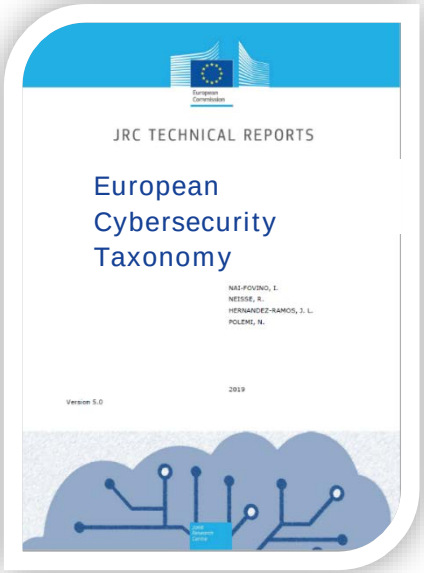
EU-Cybersecurity Atlas

Taxonomy – a Tridimensional Approach



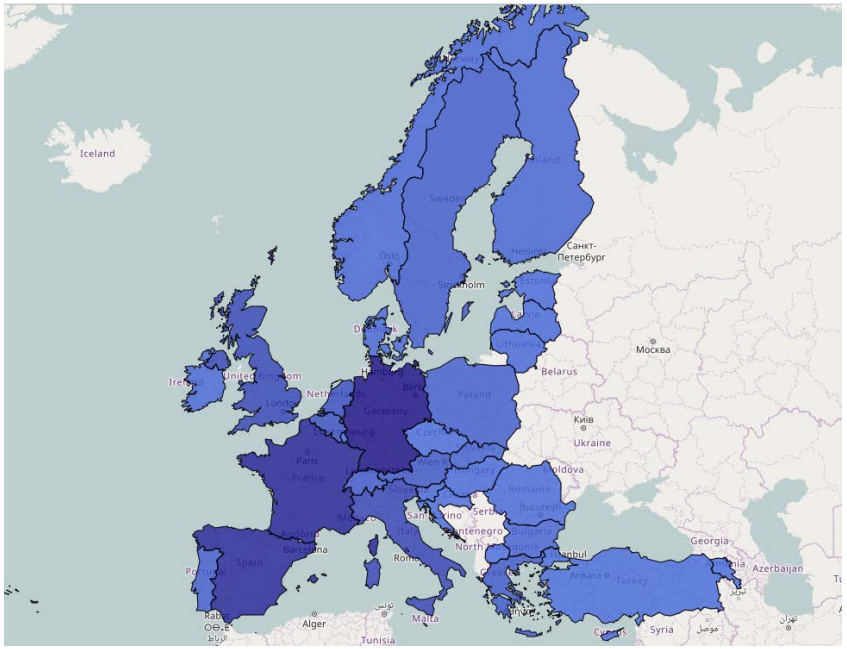
Key Questions:

- What means Cybersecurity?
- Which scientific domains can be enlisted within the term cybersecurity?
- What are the Sectors impacted?
- What are the applications?



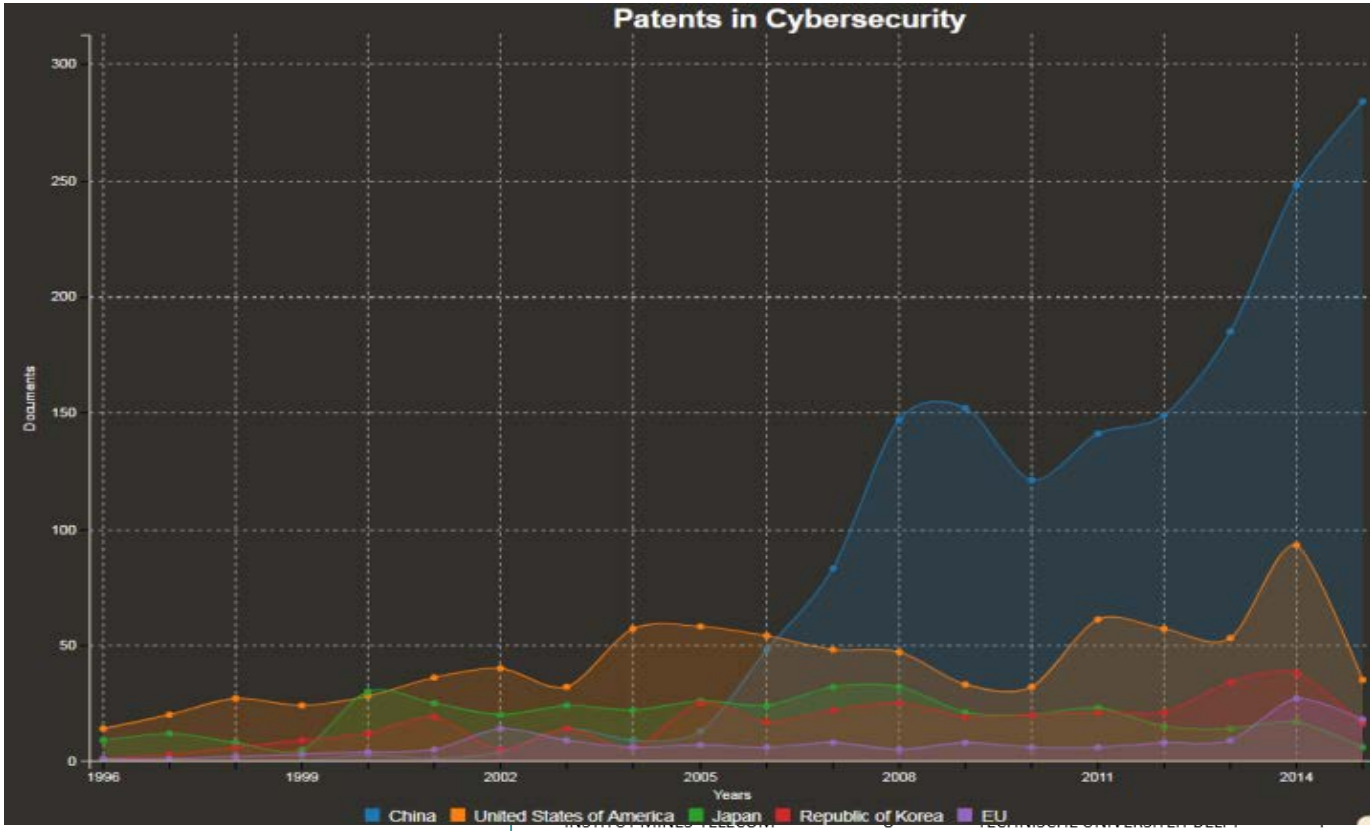
Stakeholders Engagement

- *Survey conducted in 2018 involving 700 European Research Centres*
- *Consultation with relevant European Cybersecurity associations*
- *Day-by-day engagement with the 4 Pilot Networks of European Cybersecurity Competence and Research Centres*



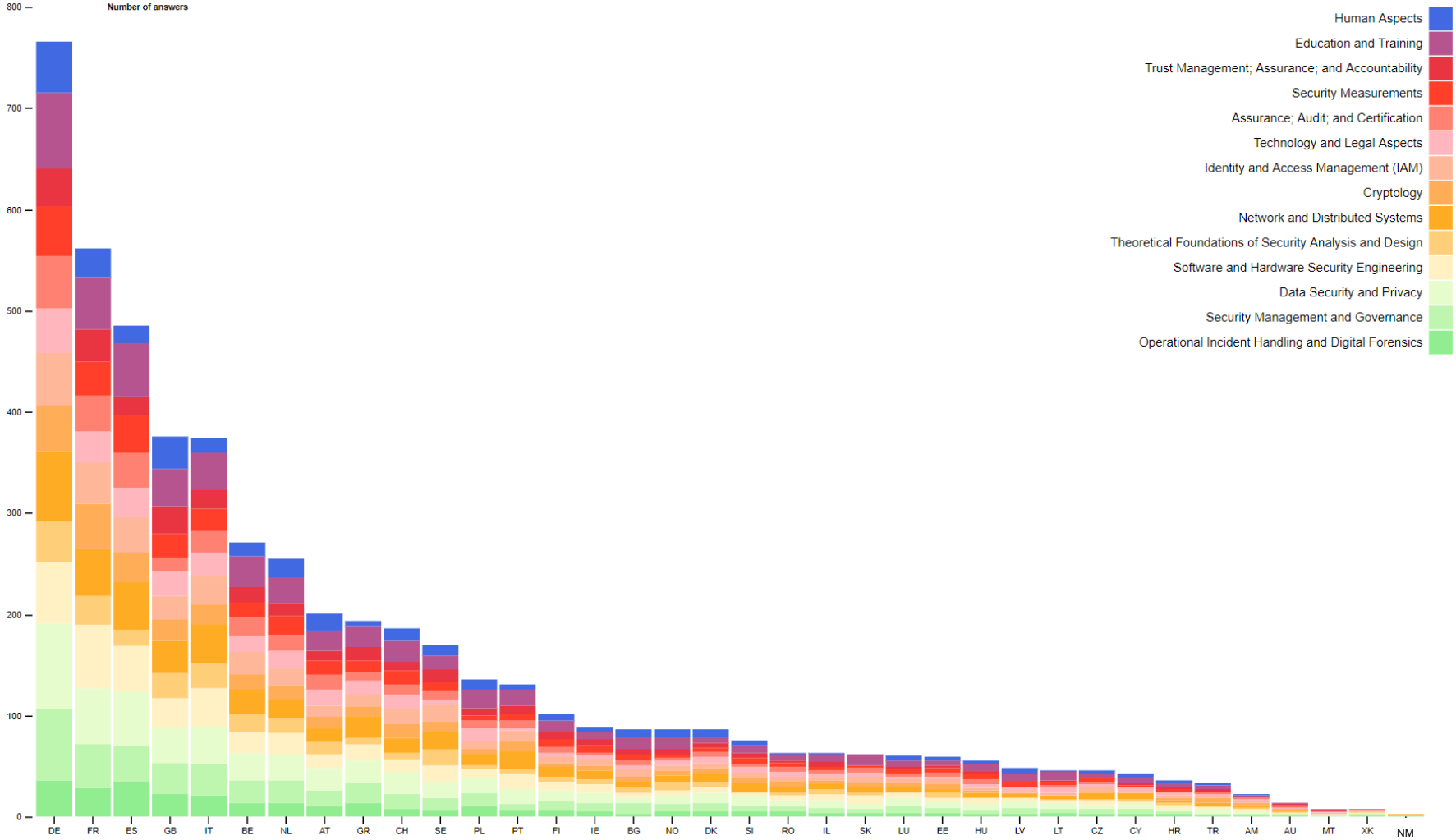
Exploitation of Online Resource

- *Scientific Pubblications (SCOPUS)*
- *EU Grants (Cordis)*
- *Pantents (Patstat)*



CONSIGLIO NAZIONALE DELLE RICERCHE	7	UNIVERSITE CATHOLIQUE DE LOUVAIN	4
TECHNISCHE UNIVERSITAT DARMSTADT	7	UNIVERSITY OF SURREY	4
AUSTRIAN INSTITUTE OF TECHNOLOGY	6	"NATIONAL CENTER FOR SCIENTIFIC RESEARCH ""DEMOKRITOS"""	3
EURECOM	6	CEFRIEL - SOCIETA CONSORTILE A RESPONSABILITA LIMITATA	3
INSTITUT NATIONAL DE RECHERCHE ENINFORMATIQUE ET AUTOMATIQUE	6	EIDGENOESSISCHE TECHNISCHE HOCHSCHULE ZUERICH	3

Overall Statistics per Domain



Thematic Coverage

Most explored Subdomains

- Protocols and frameworks for access control (authentication and authorization)
- Security testing and validation Attack modelling and countermeasures
- Standards for Information Security
- Vulnerability discovery and penetration testing
- Identity management models; (e.g. PKI; RFID; SSO; etc.)
- Threats and vulnerabilities modelling
- Network layer attacks and mitigation techniques
- Privacy by design and Privacy Enhancing Technologies (PET)Security principles;

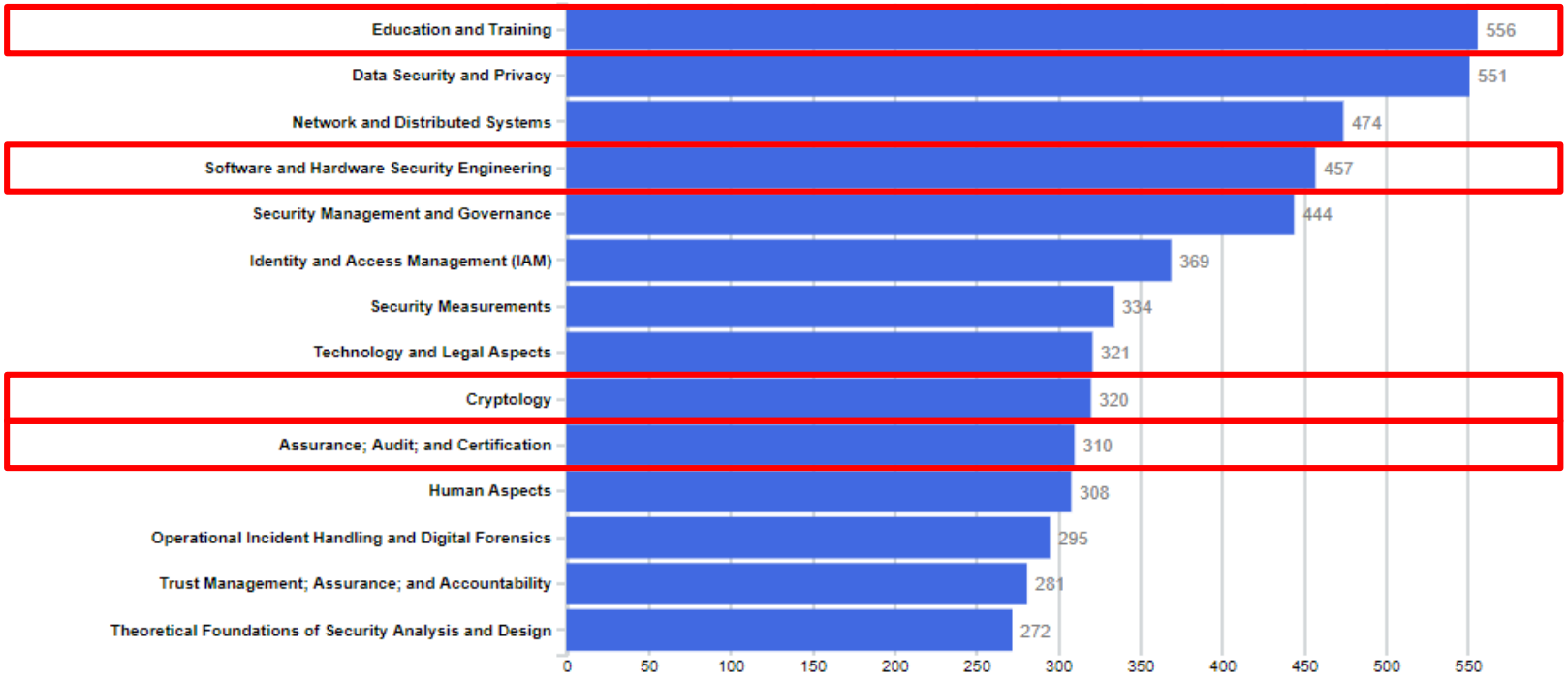
Less explored Subdomains

- Self-healing systems
- Transparent security
- Optical and electronic document security
- Trust and reputation of social and mainstream media
- Trust in decision making algorithms
- Legal aspect of certification
- Quantum cryptology
- Post-Quantum
- Trusted computing
- Information flow modelling and its application to confidentiality policies
- Formal Verification of security assurance
- Digital forensics, Cybercrime prosecution and law enforcement
- Attacker profiling
- Cyber-ranges

Domains in agenda for this workshop:

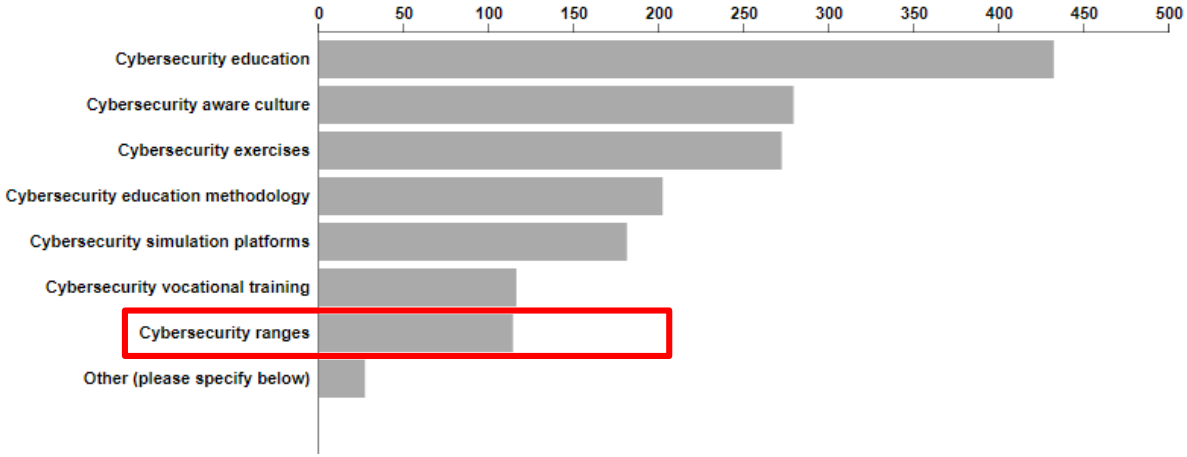
- *Cyber ranges/skills, data lakes, AI tools and Cyber Thread Intelligence*
- *Cyber secured hardware, operating system and middleware*
- *Cybersecurity and quantum technologies: Quantum Key Distribution, Quantum Communication Infrastructure, quantum computing*
- *Certification tools and standards*

Education, Hardware, Crypto, Certification

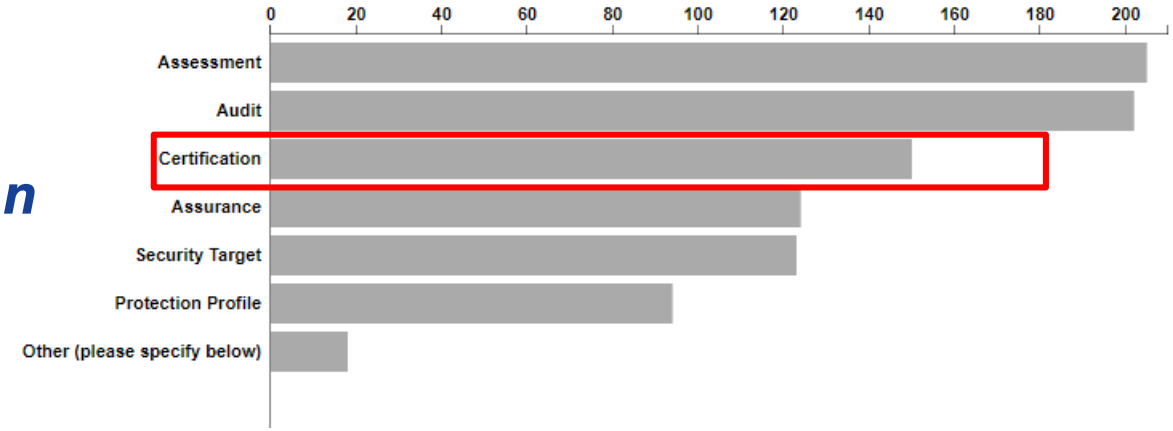


Some Numbers

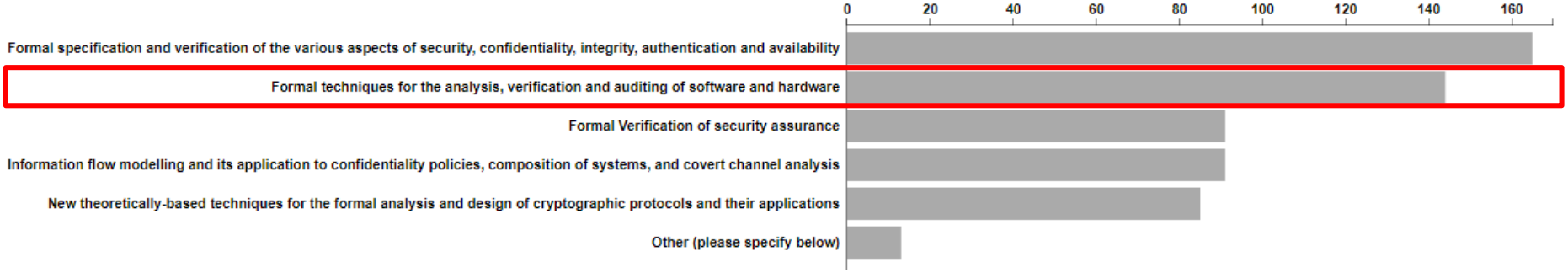
Cyber Ranges



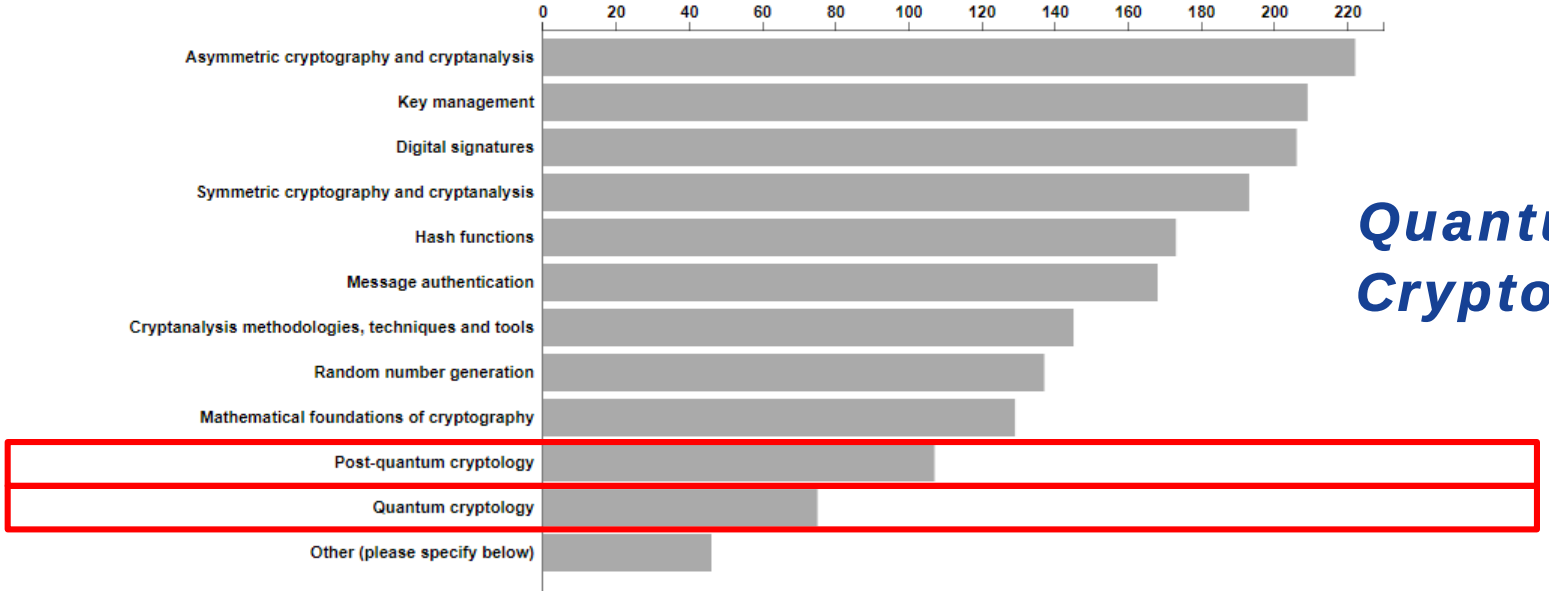
Certification



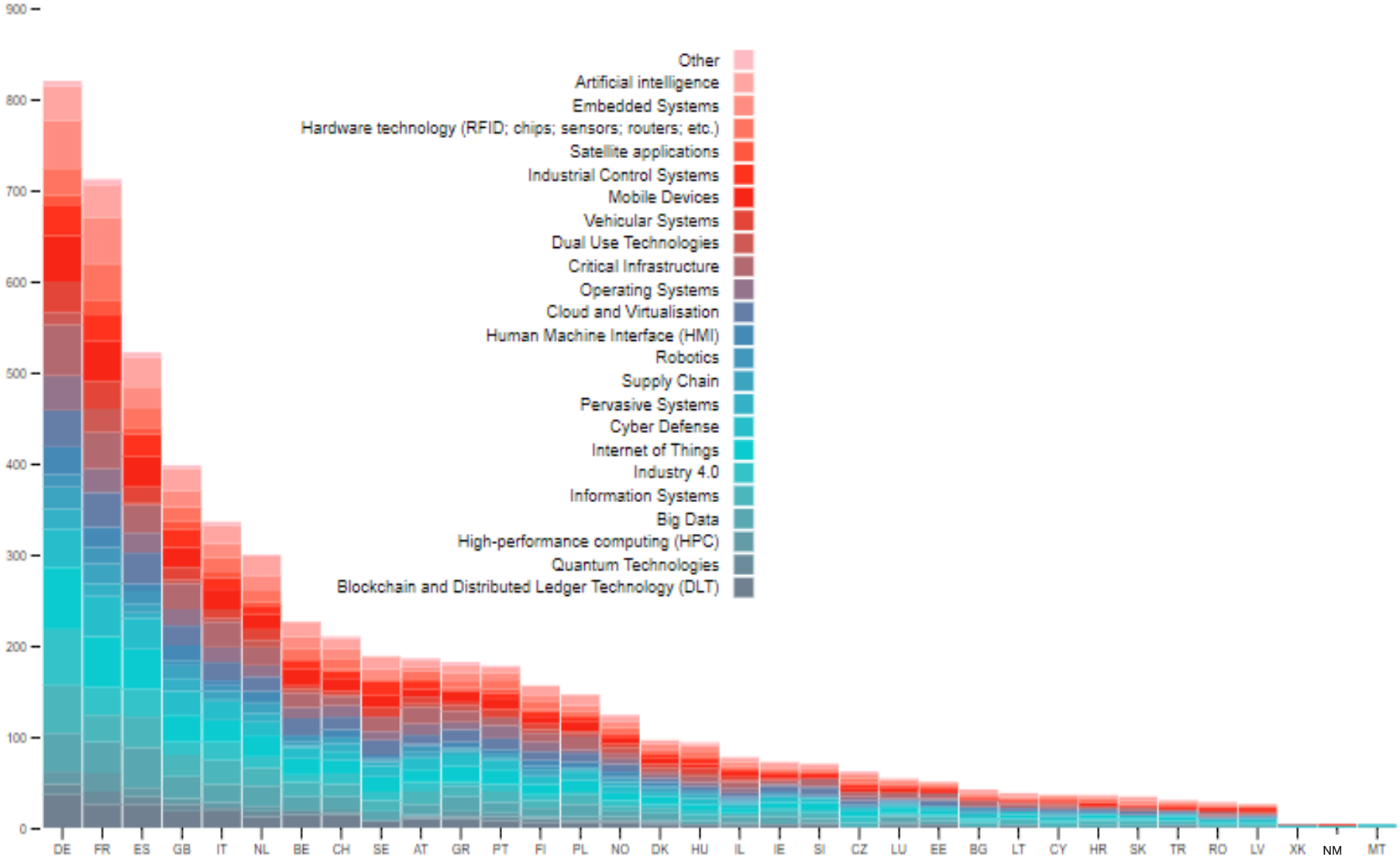
Hardware & Software Security

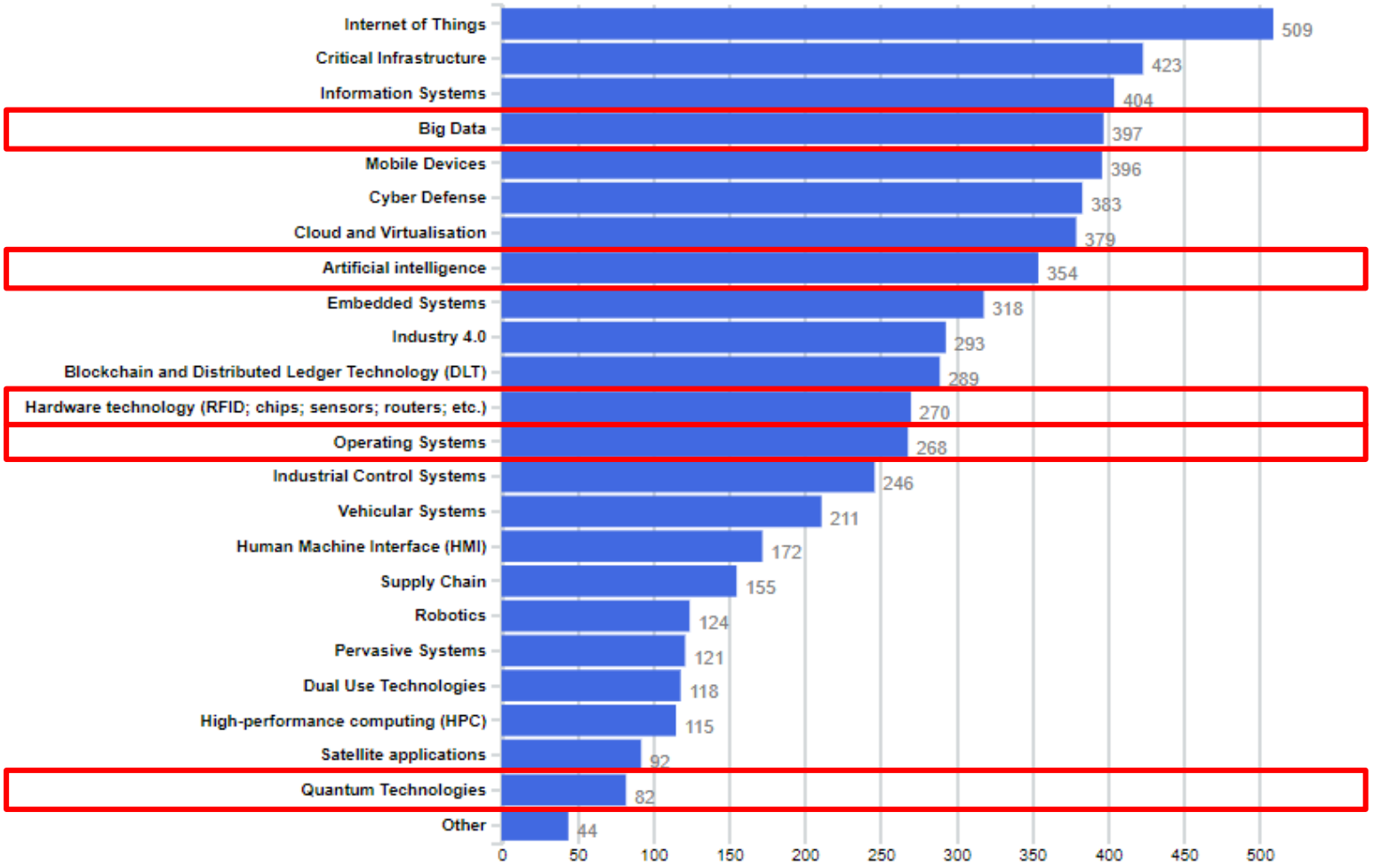


Quantum Cryptology

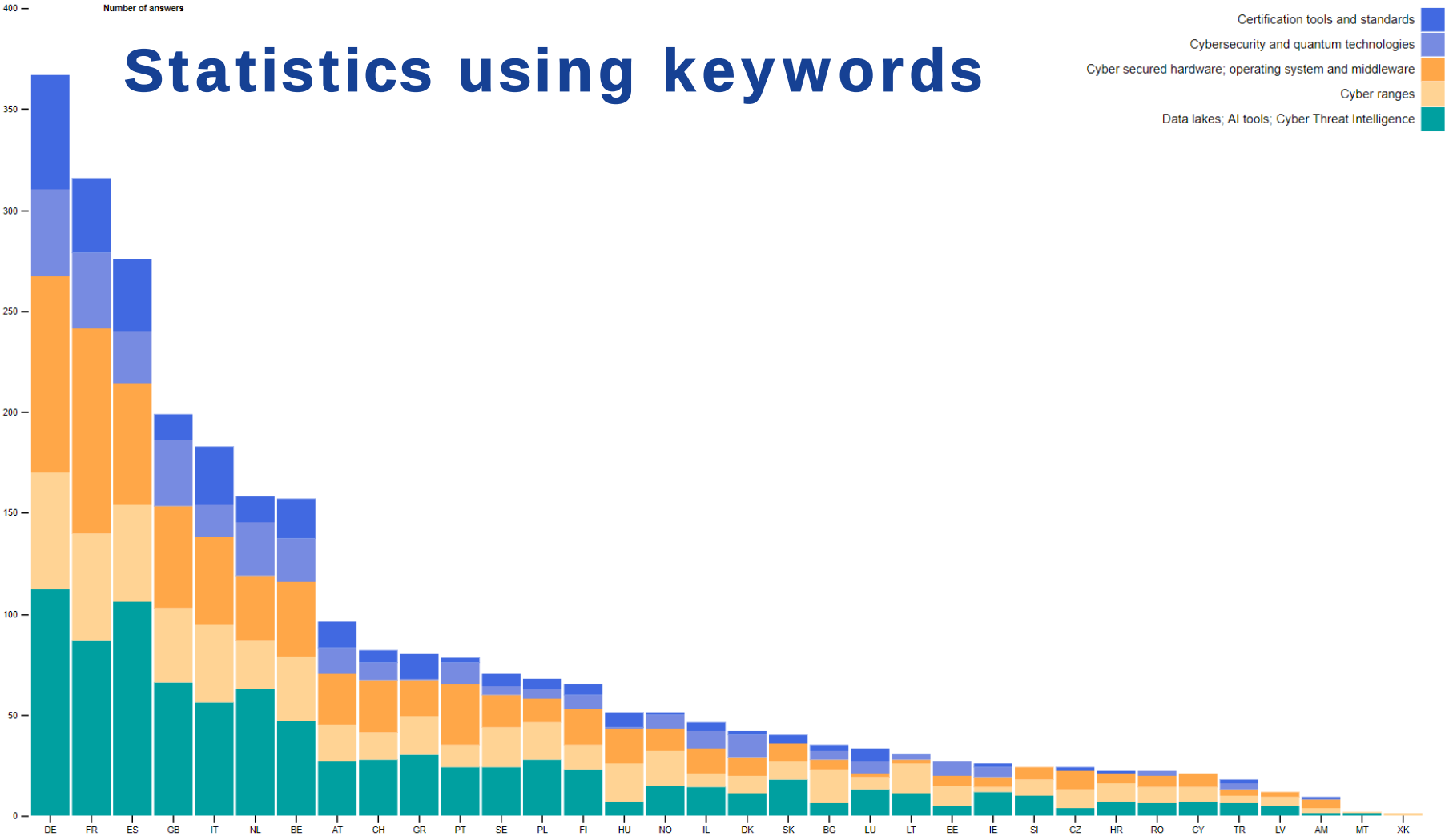


Applications




Internet of Things 509
Critical Infrastructure 423
Information Systems 404
Big Data 397
Mobile Devices 396
Cyber Defense 383
Cloud and Virtualisation 379
Artificial intelligence 354
Embedded Systems 318
Industry 4.0 293
Blockchain and Distributed Ledger Technology (DLT) 289
Hardware technology (RFID; chips; sensors; routers; etc.) 270
Operating Systems 268
Industrial Control Systems 246
Vehicular Systems 211
Human Machine Interface (HMI) 172
Supply Chain 155
Robotics 124
Pervasive Systems 121
Dual Use Technologies 118
High-performance computing (HPC) 115
Satellite applications 92
Quantum Technologies 82
Other 44
0 50 100 150 200 250 300 350 400 450 500

Statistics using keywords



European Commission

European Cybersecurity Atlas

Cybersecurity Atlas

European expertise network

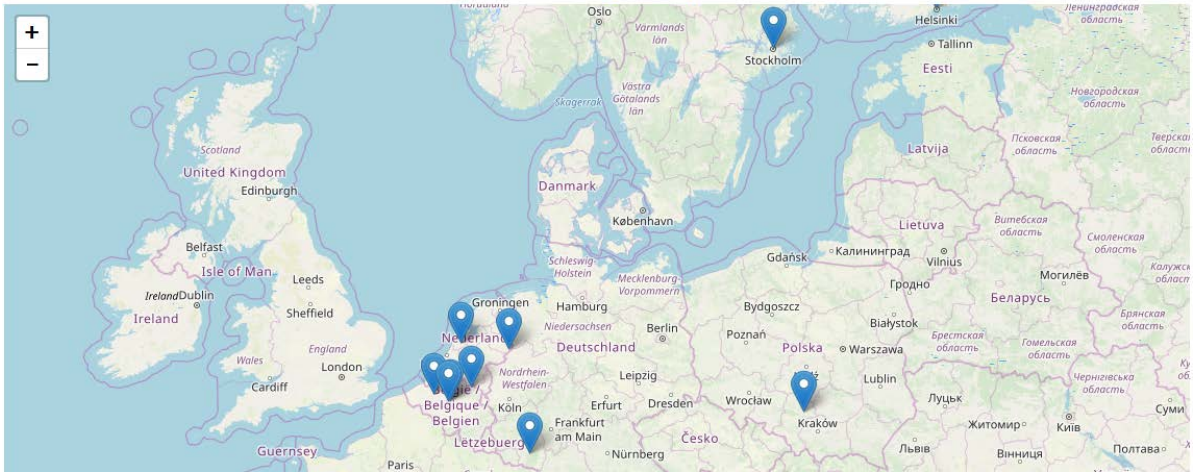
Competence Map | Charts and statistics | Online Community | Taxonomy and glossary | My account | Help

Via this website you can access useful data and important facts about Europe's Cybersecurity ecosystem.

Cybersecurity domain: - Any -

Country - Any -

Filter



Joint Research Centre

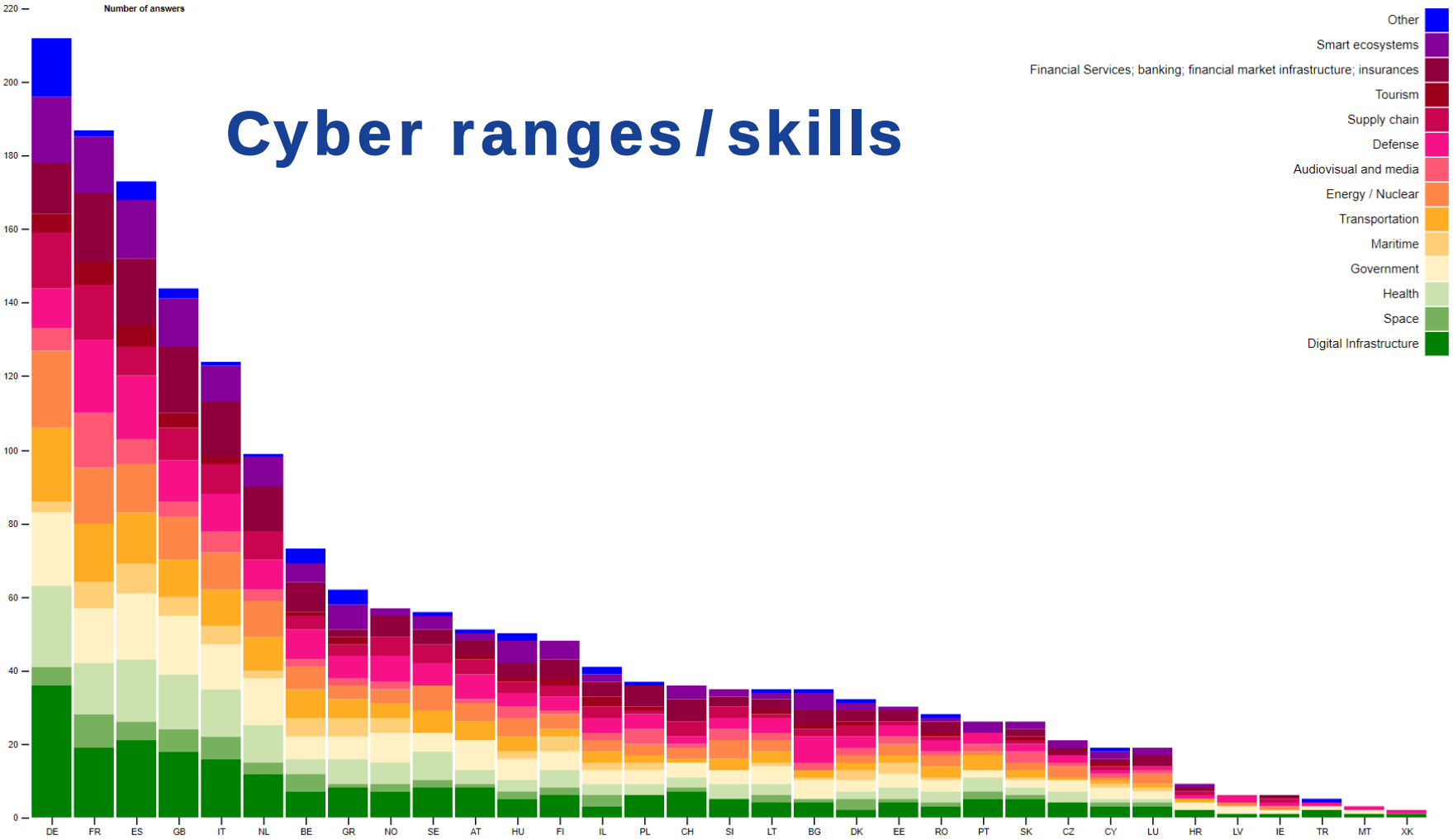
Thanks for your attention !

Joint Research Centre (JRC)

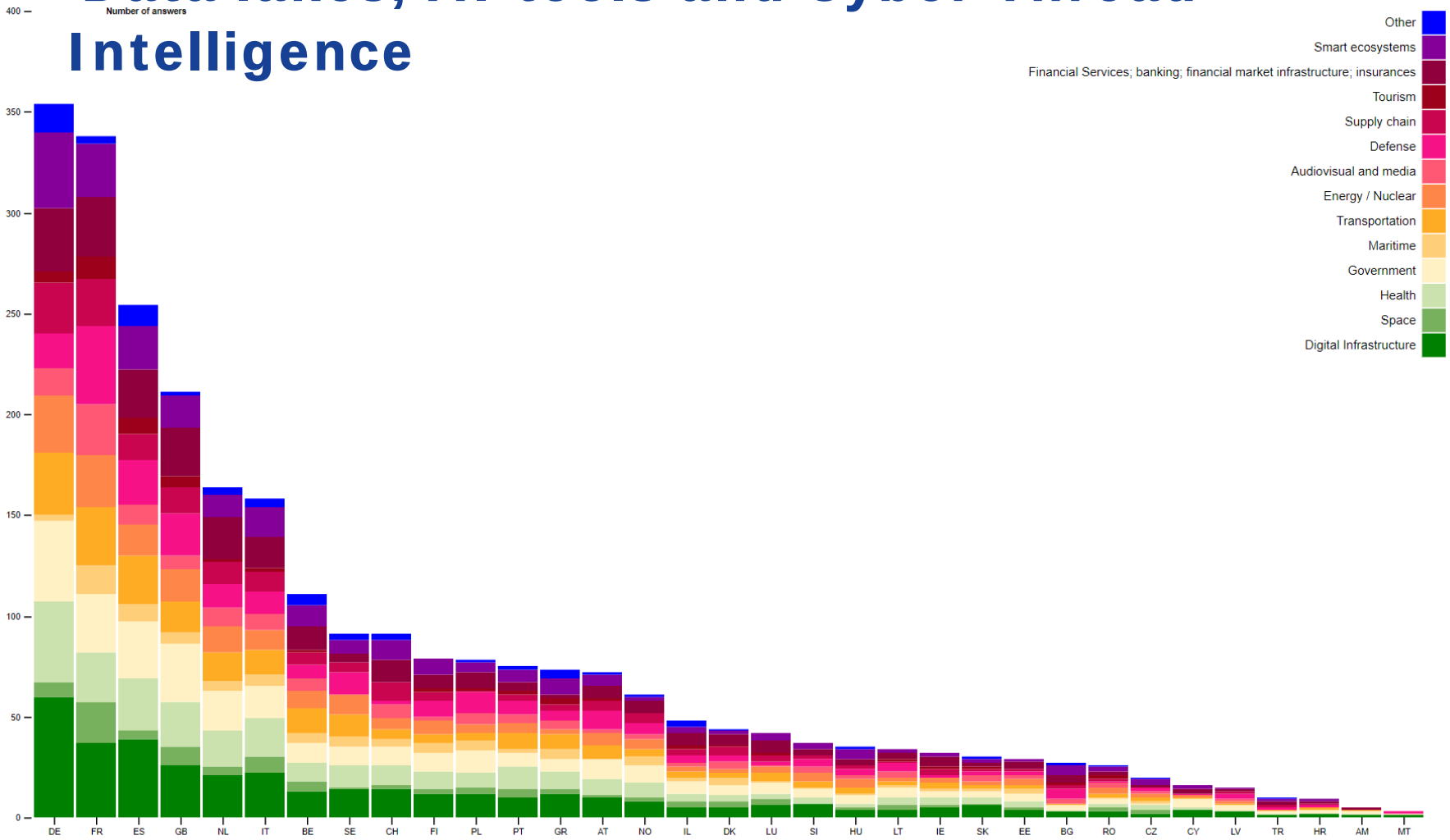
Web: www.jrc.ec.europa.eu

Email Contact:
igor.nai-fovino@ec.europa.eu

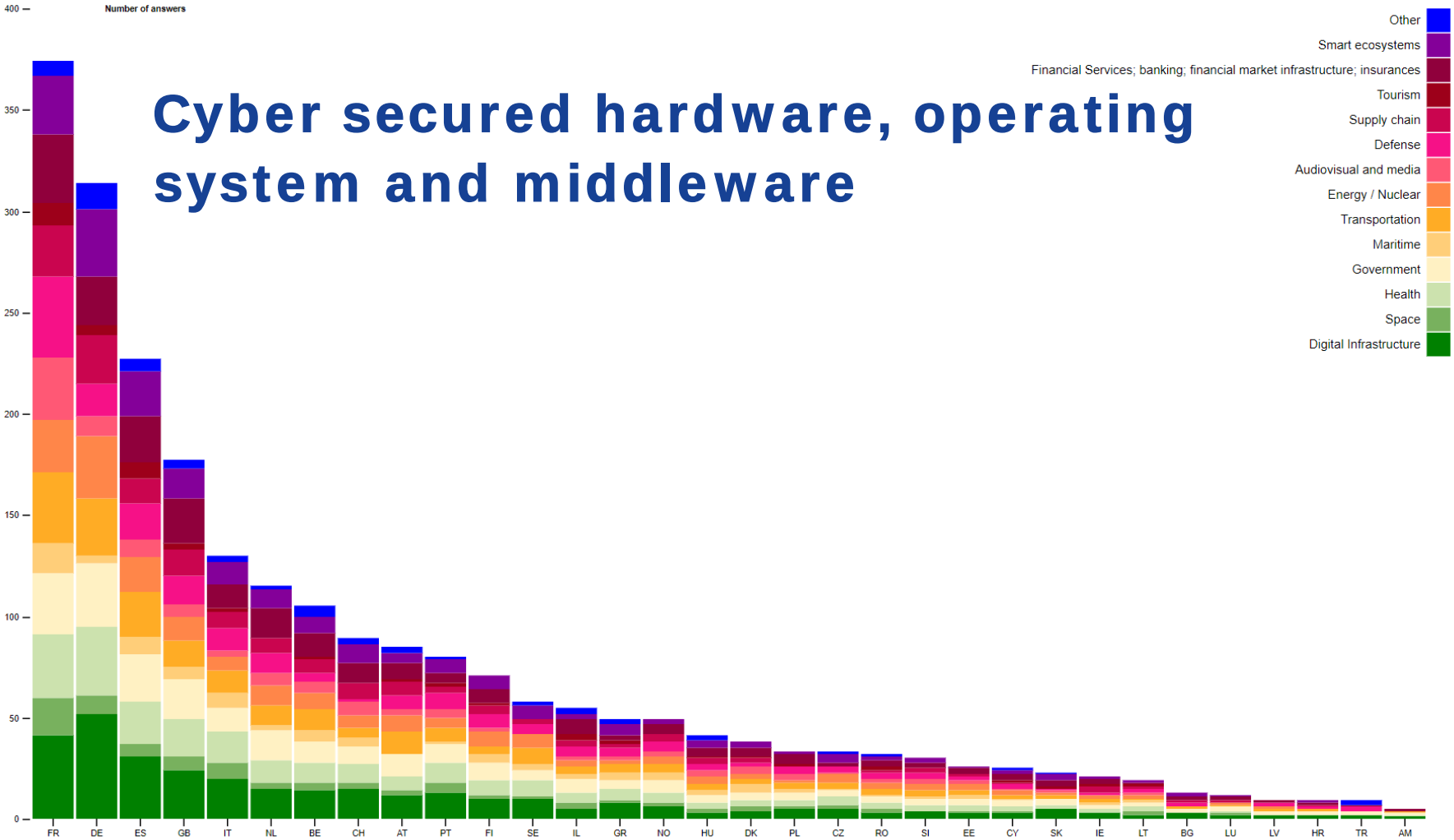
Cyber ranges / skills



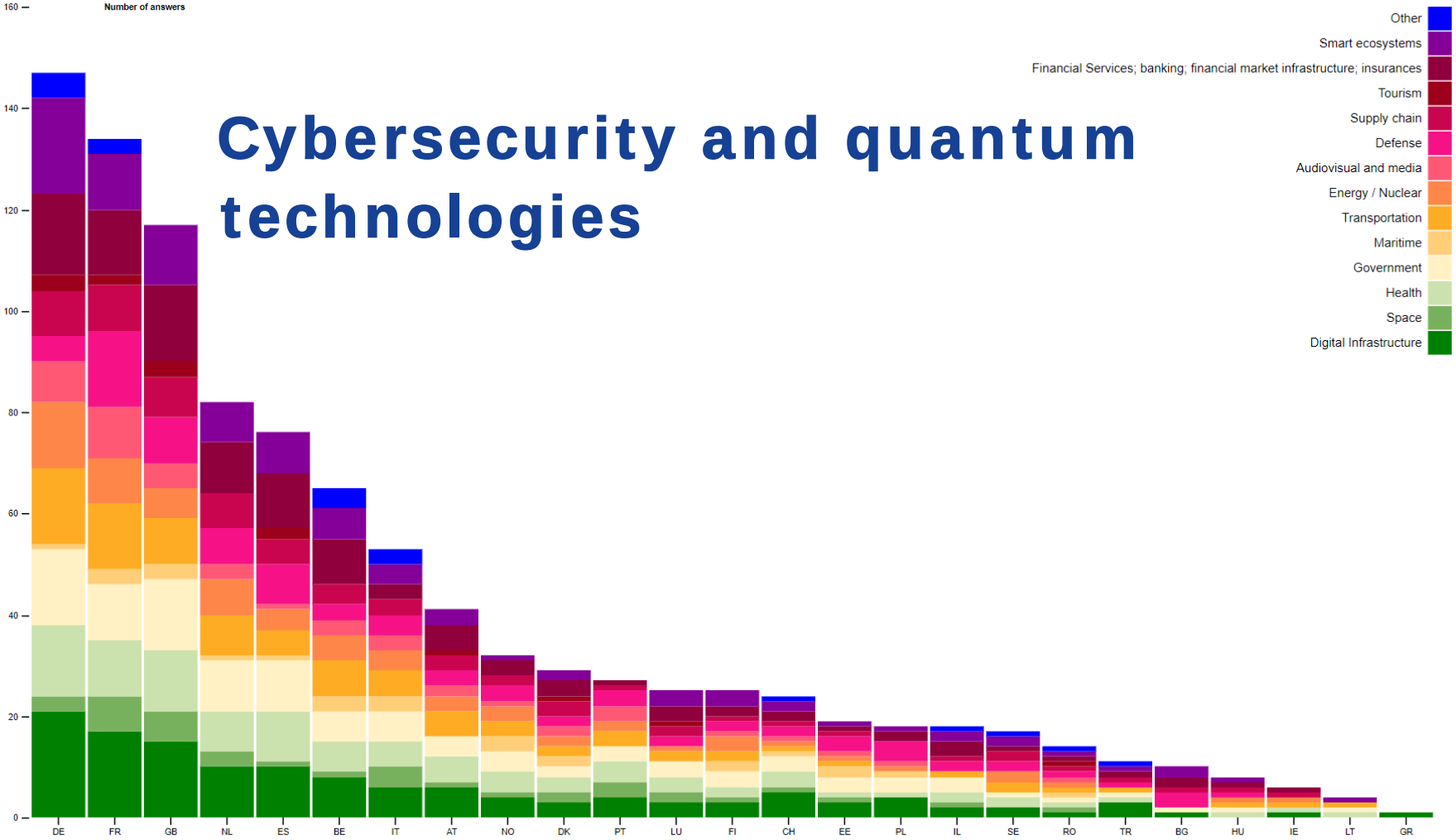
Data lakes, AI tools and Cyber Thread Intelligence



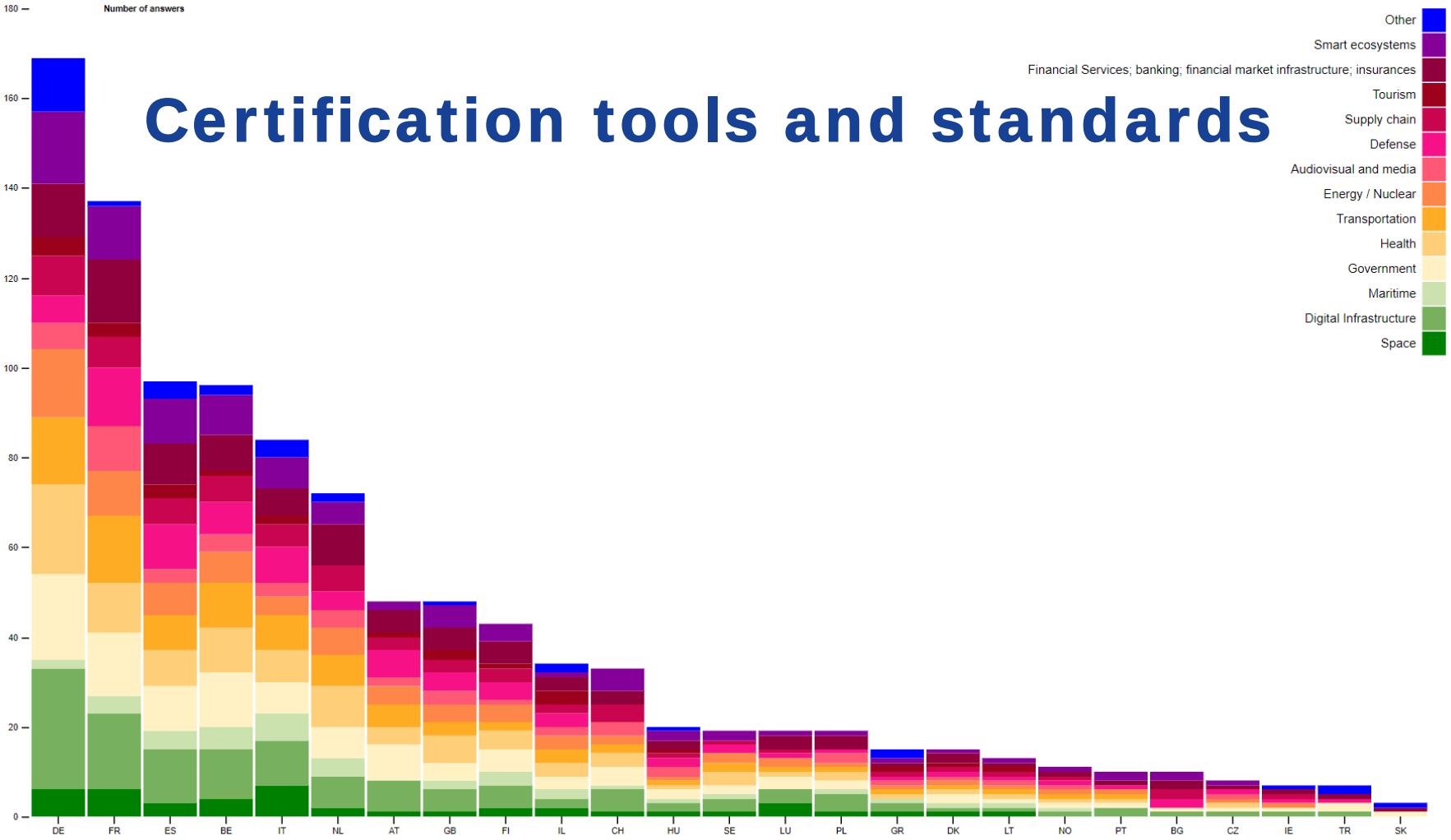
Cyber secured hardware, operating system and middleware



Cybersecurity and quantum technologies



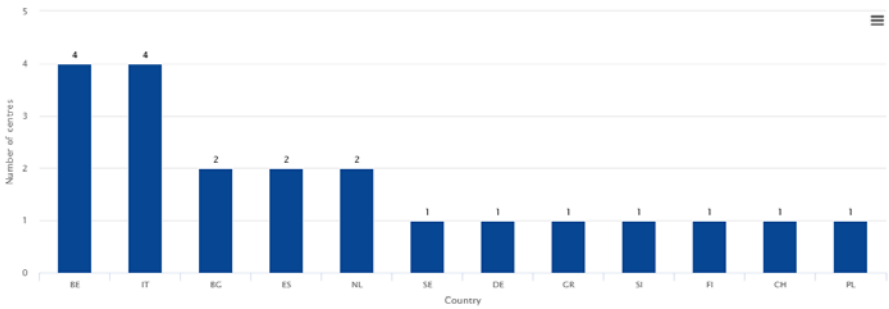
Certification tools and standards



European Commission

Competence Map | Charts and statistics | Online Community | Taxonomy and glossary | My account | Help

Number of institutions per country



Competence Map | Charts and statistics | Online Community | Taxonomy and glossary | My account | Help

List of institutions per cybersecurity domain

Cybersecurity domain

- Any - | Apply

Cryptology and Steganography

BBRI Cluster BIM
European Commission Joint Research Centre (JRC)

Data Security and Privacy

Smartgridgotland
University of Twente

Assurance, Audit, and Certification

European Commission Joint Research Centre (JRC)
University of Ispra
University of Twente

Competence Map | Charts and statistics | Online Community | Taxonomy and glossary | My account | Help

List of institutions per cybersecurity domain

Cybersecurity domain

- Any - | Apply

Cryptology and Steganography

BBRI Cluster BIM
European Commission Joint Research Centre (JRC)

Data Security and Privacy

Smartgridgotland
University of Twente

Assurance, Audit, and Certification

European Commission Joint Research Centre (JRC)
University of Ispra
University of Twente

List of institutions per cybersecurity domain

Cybersecurity domain

- Any - | Apply

Cryptology and Steganography

BBRI Cluster BIM
European Commission Joint Research Centre (JRC)

Data Security and Privacy

Smartgridgotland
University of Twente

Assurance, Audit, and Certification

European Commission Joint Research Centre (JRC)
University of Ispra
University of Twente

European Cybersecurity Atlas Roadmap

- ✓ Taxonomy definition
- ✓ Taxonomy validation
- ✓ First European Cybersecurity R&D Survey (first test of the Atlas Concepts) (https://ec.europa.eu/jrc/en/research-topic/cybersecurity/cybersecurity-competence-survey)
- ✓ Core-functionalities of the Atlas portal implementation
- ✓ Publication of the European Cybersecurity Taxonomy

Mid October 2019

- ☐ Atlas 1.0 goes online (restricted access)

January 2019

- ☐ Testing phase with the four EU pilots on Cybersecurity competence networks
- ☐ Definition of Governance Rules
- ☐ Taxonomy periodical Validation

April 2020

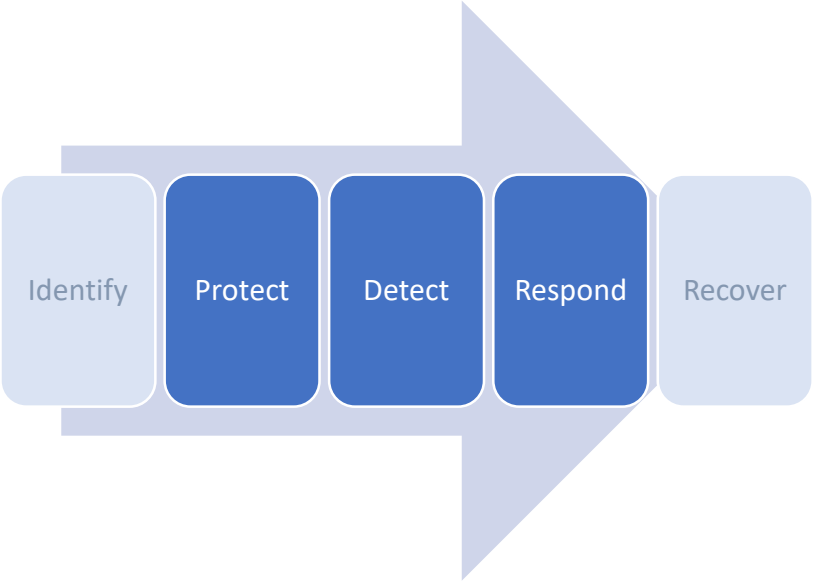
- ☐ Atlas integration with additional R&D datasets (e.g. Patents, pubblications, FP projects etc. etc.)
- ☐ … … …

Competence and Capability building

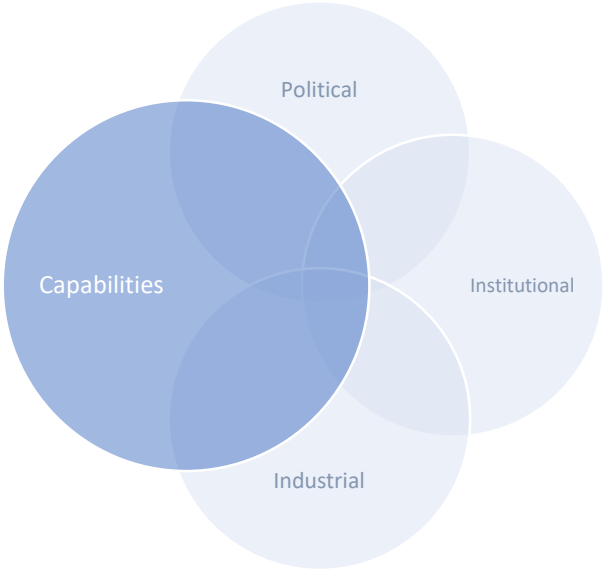
Wim Mees, Royal Military Academy, Cyberdefense research unit
Csaba Virág, Cyber Services Plc, Head of cybersecurity competence center
Evaldas Bruze, Lithuanian Cybercrime Centre of Excellence for Training, Research, Development and Education

European strategic autonomy

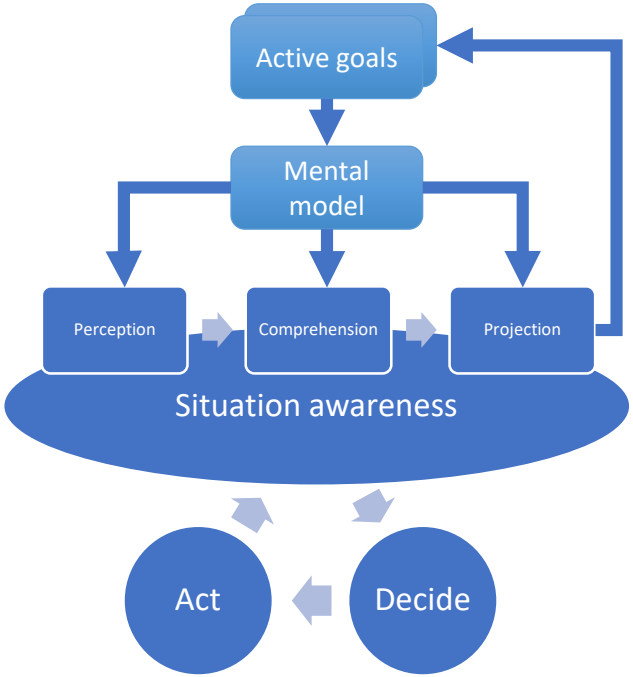
Cyber resilience pillars



Strategic autonomy dimensions



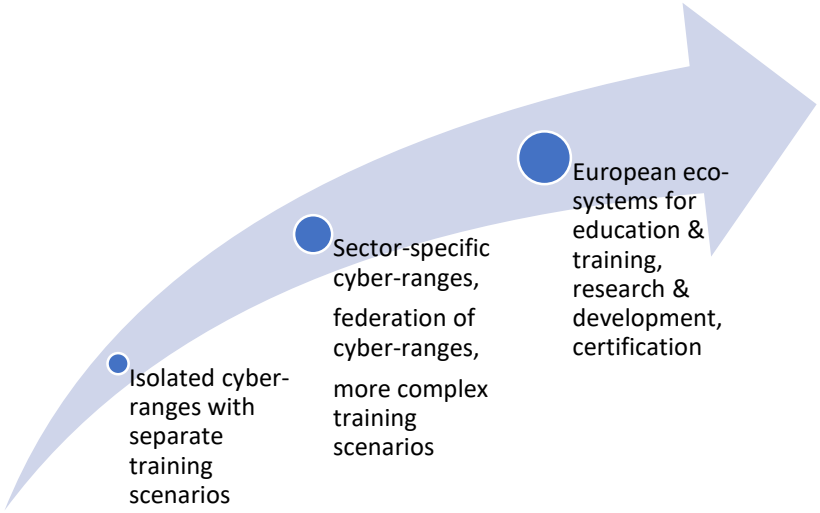
Capabilities for cyber resilience



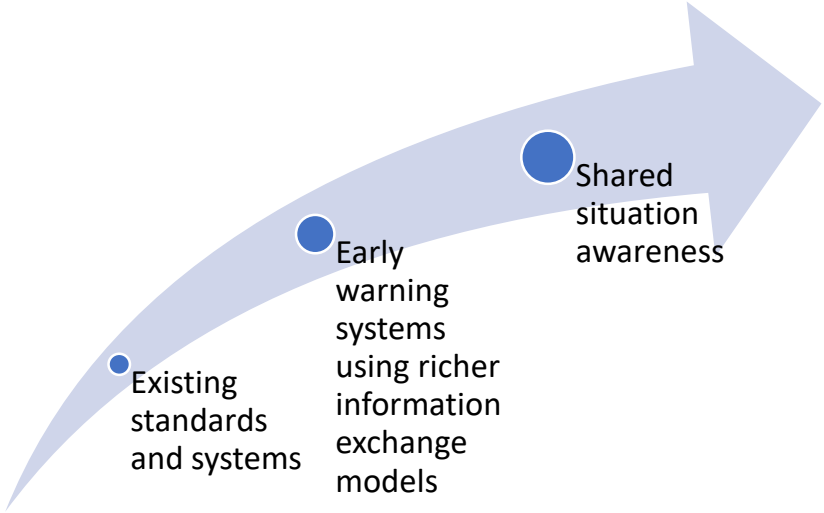
- Decision making requires high-quality situation awareness
- Situation awareness is based on:
  - Threat intelligence (early warning)
  - Mental models
- Mental models are built using:
  - Education and training
  - Requiring realistic scenarios
- Automation and decision support require:
  - AI
  - Huge amounts of data (data lakes)

Evolution of cyber ranges and threat intelligence

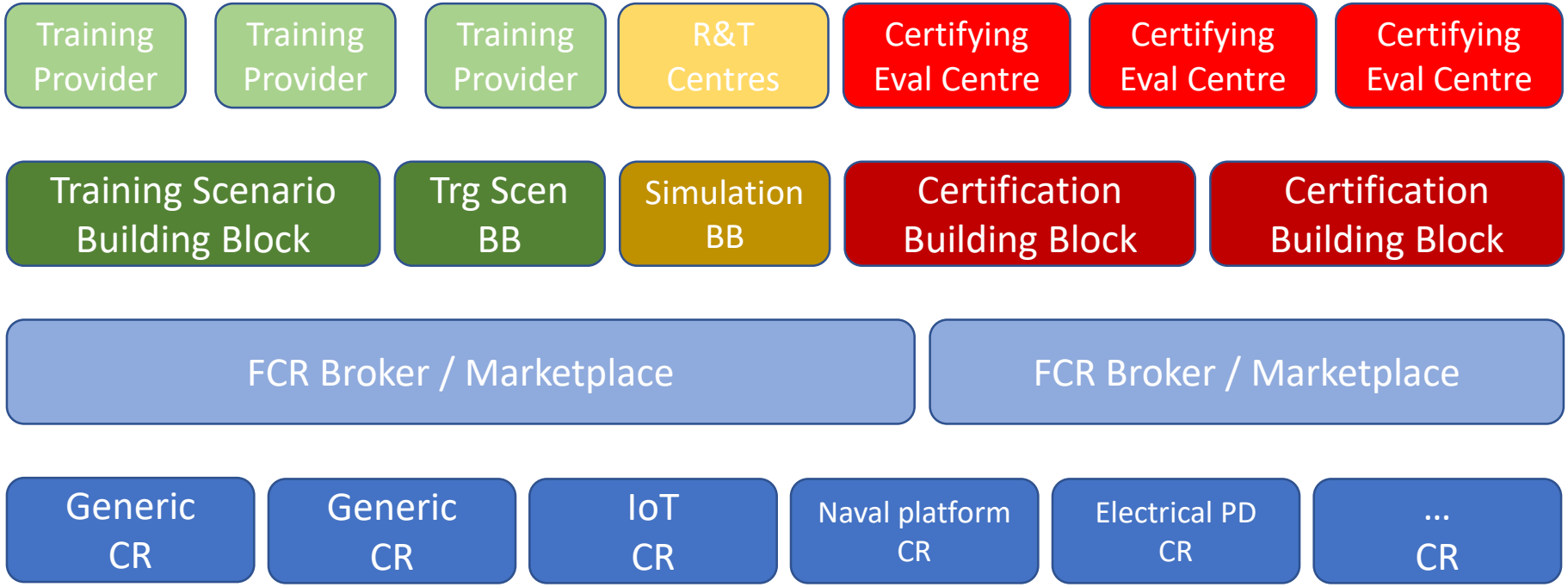
Cyber ranges



Threat intelligence



Cyber ranges as the basis for eco-systems



Showcases of ongoing initiatives and projects

- Pilots
- Cyber Valleys
- ENISA
- ECSO
- MS level initiatives
- European e-Competence Framework 3.0
- International developments (NIST/NICE, ISO, ISACA, $(ISC)^2$ ISECOM, SANS)

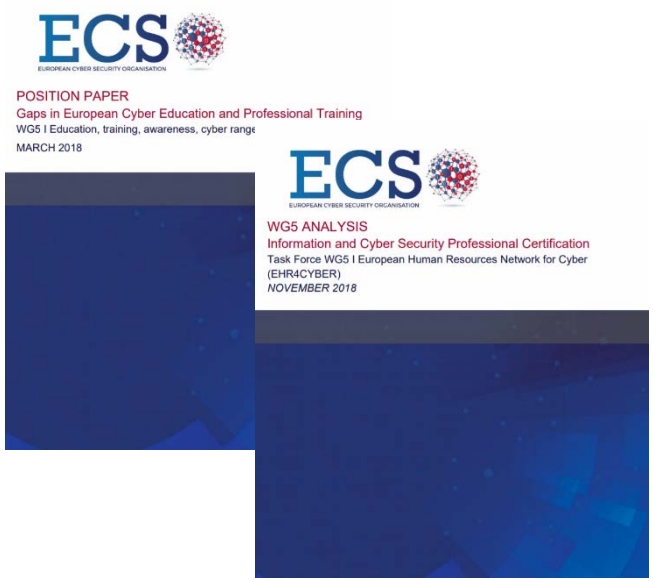
The way forward – What the industry expects

- Comprehensive market study into age structure and career histor of cybersecurity professionals in the European market, training paths and industry deman should be conducted.
- Leveraging on already available solutions and initiatives instead of developing new ones
- Investing in soft content creation (curriculas, competence building methodology, MS level education, etc)
- Evidence based education (identifying current and future trends and threats and build targeted competences to have the job done)
- Utilising cyber ranges and simulation environments as standards in competence and resilience building (set technical and methodological background, create content and supporting methodology)
- Better use of cyber ranges (technical, research and education types)
- Create the Cyber Education in Europe verification/certification and education framework scheme

ECSO work already available….

Education & Professional Training; Jobs & Skills: Gaps in Education & Professional Training

Cyber Security Professional Certification: Best practices and recommendations for a European framework for education and competences



COMING SOON

Paper on Cyber Ranges: Understanding Cyber Ranges (what makes a CR, use cases, foundation for taxonomy)

What should be done

Education made in EU verification

- Benefits and why this is needed
  - As an industry, we're still very dependent on certificates that are US-centric, and which are not based on formal training. It shows knowledge obtained by the certificate holder. This hinders the education of young people and the recognition by employers of competent staff.
  - In some European countries, first steps have been taken to set up a certification scheme. In some cases, this includes validating that formal education support these certificates. Uptake of these schemes is still very limited.
  - The certification market is dominated by non-European, especially US, companies. A European wide certification scheme including an education framework is lacking.
  - Alignment with other international frameworks in this area (like ISO and NIST) is lacking
- How to implement it
  - With the development of a certification and educational framework through supporting young professionals, existing professionals and professionals joining the cybersecurity field at a later stage
  - Solutions should leverage on the shift in the education and training market, utilise simulation based competence building and remote learning
  - Solutions shall develop and suggest career paths and knowledge building blocks adaptable on European level
- Impact that can be achieved
  - Cyber resilient Europe
  - Closing the gap between demand and supply
  - Faster and more productive delivery of "market ready professionals with hands-on experience"
  - Create common understanding of cybersecurity training and education fundamentals
- Expected funding
  - 100 Mio euro for mapping and developing cyber security certification and verification competence building curricula and tools.

What should be done

Develop tools to support scalable competence building

- Benefits and why this is needed
  - Reduce “go-to market” time for trainees and students
  - Close the competence gap
  - Currently most of the initiatives are either academic or industry, there needs to be a common approach
  - To defragmentat EU wide competence building
- How to implement it
  - Tools for content and supporting competence building methodology
  - Cyber threat intelligence and evidence based education by utilising simulation environments based on a common approach
  - Define common curricula as foundation
  - Automated challenge scenario generation supporting competence building
- Impact that can be achieved
  - Rasing cyber resilience on EU level
  - Provide common understanding of cybersecurity education and training requirements
  - Provide of-the-shelf solutions for providers to utilise
- Expected funding
  - 60 Mio euro and additional funding for mapping and developing domain specific solutions and requirements

What should be done

Utilisation of cyber ranges and simulation environments

- Benefits and why this is needed
  - Cyber ranges as technical platforms are more and more available to any organisation
  - Lack of joint criteria and know-how to utilise cyber ranges and simulation environments
  - Competence and capability building is based more on theory than on practice
  - To leverage on the different type of cyber ranges (academia, training and research)
  - Evidence based cyber attack emulation to prepare blue teams for defence
- How to implement it
  - Develop common understanding of cyber ranges regarding technical and operational capability for easy deployment of content
  - Investigate how the different type of cyber ranges can collaborate and share resources and functions to support competence building
  - Develop automated content delivery options supporting specific job profiles
  - Develop the capability of delivering automated evidence based threat and knowledge building scenarios based on CTI reports and incident responses.
- Impact that can be achieved
  - High return on investment into competence and capability building as organisations receive what they truly require
  - Higher supply chain and critical infrastructure cybersecurity resilience (as attacks can be simulated)
  - The capability to leverage multisector training, test & certification activities, at a fraction of cost
  - Improve national security capabilities supplying a hands-on training capability on environments that cannot usually be available or tested, or situations where multiple behaviours related to users and machine to machine services compete on the same network
- Expected funding
  - 100Mio euro and additional funding is required to map and develop the common usage tools for cyber ranges and environments

How AI tools can enhance cybersecurity?

- Both ways:
  - To identify that the attach is AI based / used
  - Bring wider scope, faster, predictive and automated response and mitigation

IMPLICATIONS FROM T-SHARK

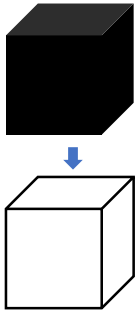
Current focus	Emerging
Cyber	Cyber + cyber in context
Internal perimeter	Internal perimeter + external infrastructures
Incidents	Incidents + wider threats
Response	Response + predictive / proactive / automated

Should we trust such tools?

DATA

- Availability of complete sets;
- Trusted sources;
- Data modification.

AI



FINDINGS

- Weight of implications;
- Verification and ability to inspect;
- Inclusion in process combined activities human / tools .

- Sensitive data for AI still to be handled in the same secure regime as original data.
- Can data handling procedures help?

Ensure trustworthiness of AI systems, including security, privacy and reliability (SPARTA – SAFAIR Program).

- Dual competence specialists for the dialog (Legal / Technology).

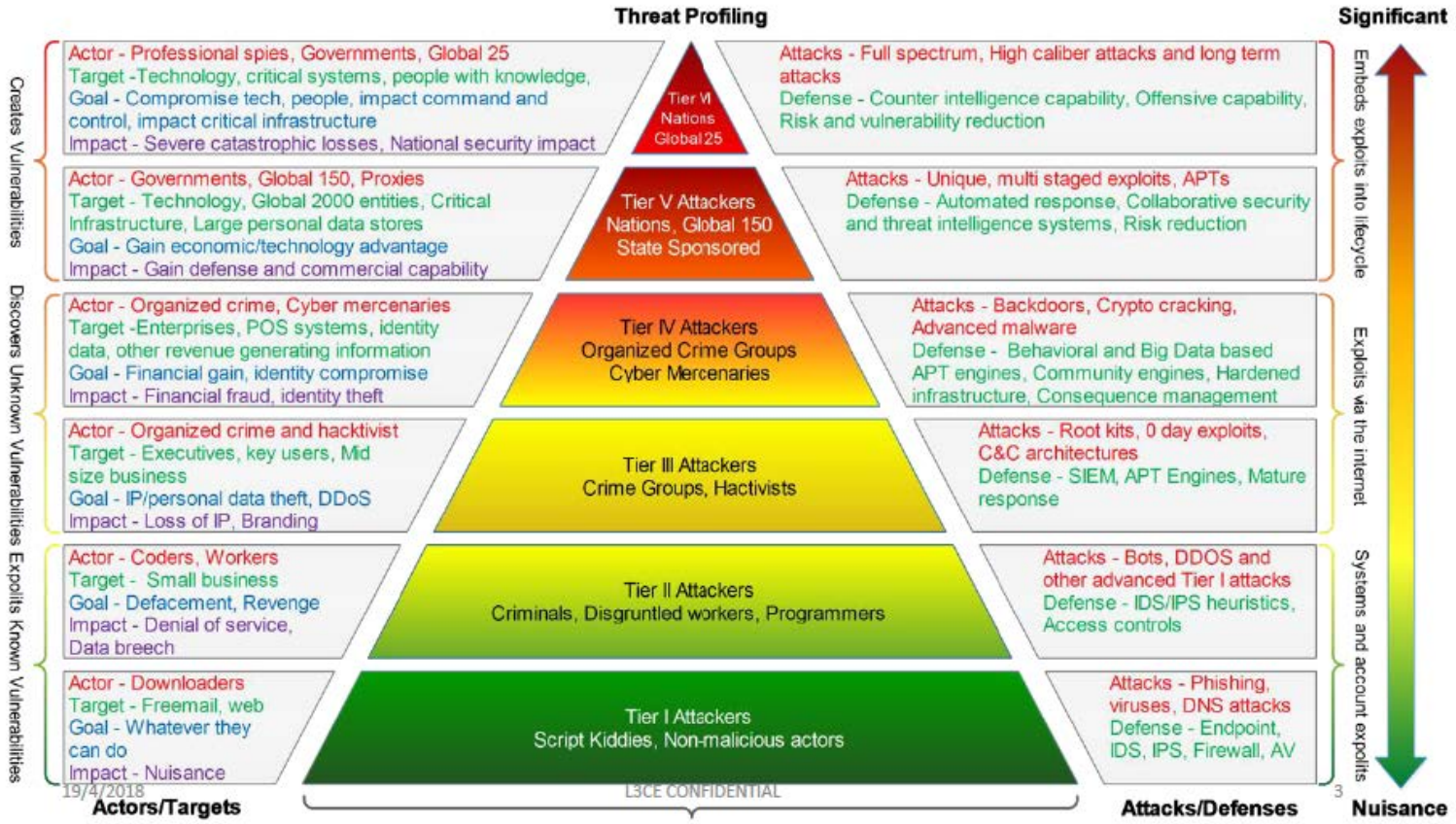
Secure environments for sandboxing, co-creation, training and dissemination?

What about their certification at European/International level?

- Certification of? – security, privacy, ethics?
- Testing to be separated, especially critical case testing.

- Expected solution – certified toll +certified specialist + common sense?

Cyber Security Threats are growing by complexity



Trending

What should be done

Develop comprehensive Cyber Threats Intelligence methodology

- Benefits and why this is needed
  - Multi-stage and long-term cyber threats can be identified only providing comprehensive situational picture
  - Complex threats (attacks) can be prevented and/or managed only in early stages
  - Current response ecosystem is mostly focused on technological aspects of incidents (Perimeter protection, HW/SW safety, content protection)
  - Lack of trustworthy practitioners network effectively sharing the developments
  - Limited role of decision-makers in operational part
  - Lack of integrity and continuity between threats intelligence, incrimination, justice and response actions
  - Competence and capability building is based on individual effort rather than on structured way
- How to implement it
  - Define and implement complex cyber threats taxonomy/model (extend and integrate Mitre Attack Framework with InfoSec, Hybrid Threats and other aspects of complex threats)
  - Consolidate methods, practices, tooling and concepts into integral methodology
  - Develop legal framework enabling cyber threats intelligence and preventive measures
  - Develop common discipline and common understanding of complex cyber threats, tactical schemas
  - Integrate cyber and societal sciences and context knowledge into common discipline
  - Develop new professional profiles capable effectively deal with phenomena
  - Establish technical and operational capability for continues phenomena research and timely adoption of response measures
- Impact that can be achieved
  - Higher ecosystem/market resilience, prevention and more effective response to complex threats (responses are more proactive and prediction driven)
  - Protection of high value targets: top fortune businesses, unicorns, inventions, sensitive political and societal processes
  - Focused and efficient capability development
  - Strategic leadership in the domain
- Expected funding
  - 40Mio euro and additional funding is required to develop regulatory framework, integral discipline, the common usage tools and environments for continues phenomena research

What should be done

Develop EU comprehensive cybersecurity threat intelligence platform

- Benefits and why this is needed
  - Current solutions are on national level, that limits the scope and perspective of phenomena analysis
  - Exchange of relevant information and alert processing is rather slow
  - Defragmented technical solutions
  - Absence of trustworthy environment for fussed information exchange
- How to implement it
  - Establish common threat intelligence platform
  - Utilize advanced analytics, analysis automation, ML, visual analytics techniques
  - Define common data processing, exchange formats and API standards
  - Define and implement required anonymization, masking and encryption techniques
  - Define and implement required data/information access control mechanisms
  - Research, test, certify techniques and methods for trustworthy process organization
- Impact that can be achieved
  - Raising cyber resilience on EU level
  - Provide common platform for complex threats processing
  - Expected to deliver capabilities able to predict elections interference and similar security threats
  - High situational awareness and strategic decision-making capability of potential future threats
  - Will put EU in leader position on complex cybersecurity threats intelligence
- Expected funding
  - **100**Mio euro and additional funding for development and establishment of common threat intelligence platform

Cyber Secured Hardware, Operating System and Middleware

Claudia Eckert, SPARTA (TU Munich, Fraunhofer AISEC)
Fabio Massacci, Cybersec4Europe (Uni Trento)

Ambition:

- Develop core technologies towards a trusted European single digital market: Enhance Europe's technological sovereignty to foster innovation
  - Why is it important?
  - What should be done?
  - How can it be done?
  - What can be achieved?
  - Who can do it?
  - How much funding is required?

Cyber Secured Hardware, Operating System and Middleware

Ambition:

- Develop core technologies towards a trusted European single digital market: Enhance Europe's technological sovereignty to foster innovation

Why is it important? Politically

- Digitization is built upon a hardware and software continuum
  - Domains: digital production, digital health, digital farming, smart energy
  - Non-EU manufacturers dominate the global hardware & OS market
  - Large fraction from Open Source Software easy to use but hardly verified
  - Strong dependency for EU enterprises, governments, citizens
    - Trusted? Shut down via activated kill switch? Information leakages through Backdoors!
- Innovation (e.g. AI) heavily depend on access to data
  - Non-EU hyperscaler platforms (AWS, Azure, Google) dominate the cloud market
  - Strong dependency for EU enterprises, governments, citizens
    - Trusted? Lock-in? Loss of control over own data? Leakage of business secrets?

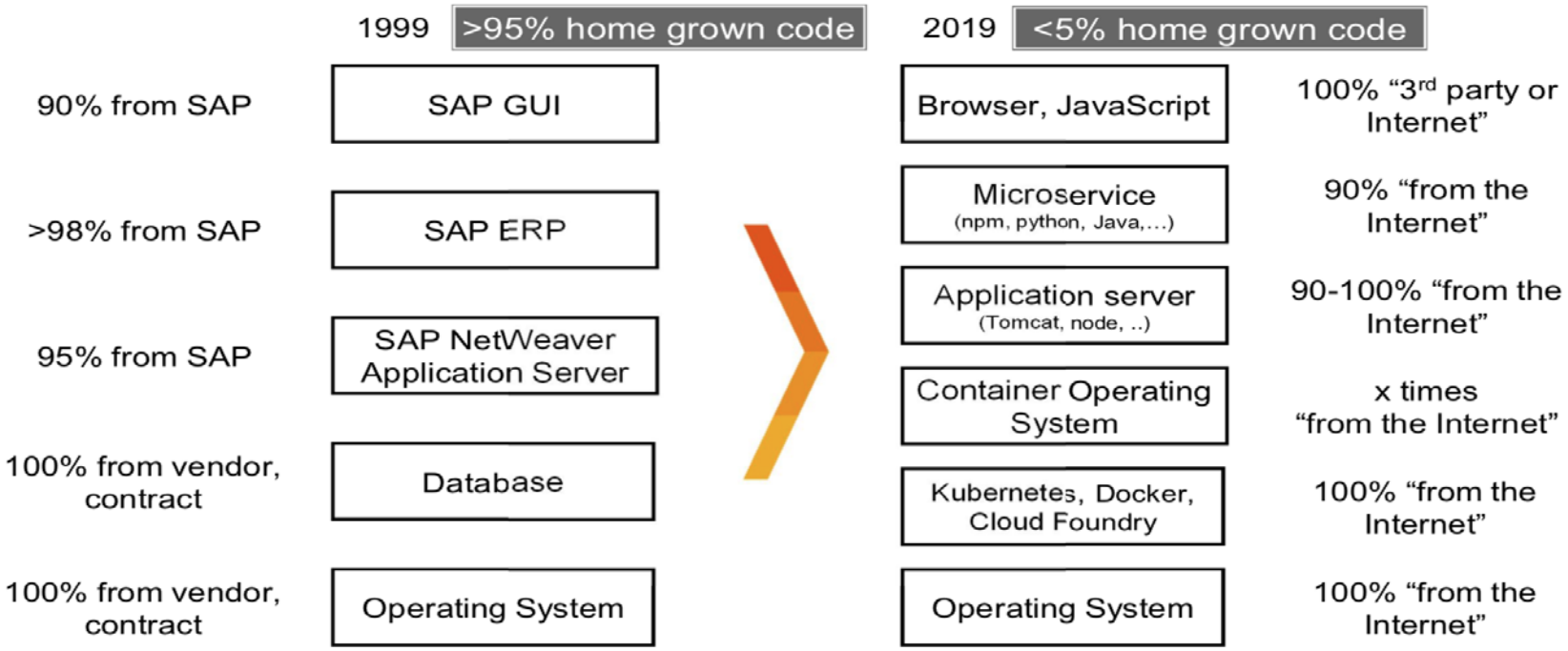
Cyber Secured Hardware, Operating System and Middleware

Ambition:

- Develop core technologies towards a trusted European single digital market: Enhance Europe's technological sovereignty to foster innovation

Why is it important? Technically

- There is no longer a "single" manufacturer, not even a "EU" manufacturer
- On the side the modern software stack hardware is worse



Cyber Secured Hardware, Operating System and Middleware

What should be done?

1. Provide technologies to build Trusted Products:
   - **What:** Provide trusted hardware with trusted (embedded) operating system for IoT
   - **Branding:** Trusted products made in EU to strengthen the market position of European firms
2. Provide technologies to Test Security of Products
   - **What:** Provide trusted tools to test the security of hardware and software components
   - **Branding:** Made Everywhere, Secured in Europe to strengthen certainty of EU supply chain
3. Provide technologies to build Trusted Data-Sharing Infrastructures
   - **What:** Provide trusted infrastructures with "virtual hyperscalers" based on existing Clouds
   - **Branding:** Data sovereignty preserving European values

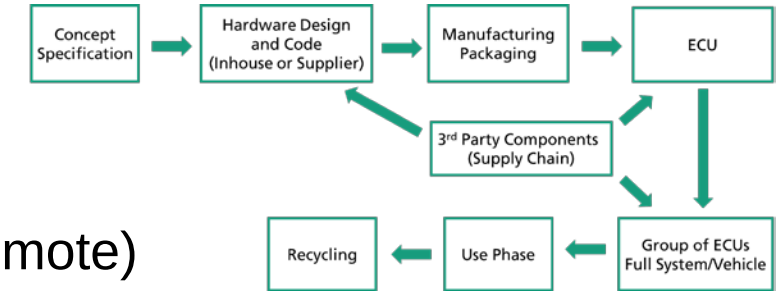
Benefits

- Trustworthy smart products will foster new business models
- Strengthen the role of Europe as the world de-facto security and privacy regulator
- Access to trustworthy data is key to foster innovations and services based on AI

Cyber Secured Hardware, Operating System and Middleware

How can it be done?

- Develop trusted hardware based on Open Source Hardware
  - Trusted Designs: code review, IP verification
  - Trusted Manufacturing and packaging: split manufacturing
- Develop Trusted platforms based on Open Source Software
  - Isolated container: trusted execution of applications
  - Attestation: check security status of OS at any time (from remote)
- Develop Trusted CI/CD & continuously updated artefact test toolchains based on Open Source SW
  - Protect the whole lifecycle of the hw/sw-component incl. its long term updates and evolution
  - Ensure trustworthiness of hw/sw platform over it's lifecycle irrespective of where it is made
- Develop and run a reference Trusted Data-Sharing Infrastructures leveraging on the above
  - Trusted connector, service brokers, App Stores
  - Trusted identity providers, clearing houses
- Leverage previous and just starting work: International Data Space (IDS), GAIA-X

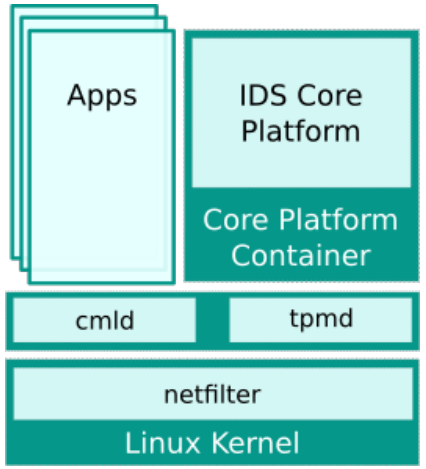


Cyber Secured Hardware, Operating System and Middleware

What can be achieved?

Trusted Products made in EU: Trusted Open Source hardware and software platforms

- No hardware Trojans, backdoors, or hidden functions.
- Highly integrated packages using cutting-edge technology
- Certified OS platforms with attestation services
- Tailored to customer needs: e.g. for IoT



Products Tested for Security in EU: Trusted Open Source chain of “assurance”

- Either it originates from a trustworthy supply chain or it meets its secure baseline
- Open software suite available to SMEs for final customer integrations

Trusted Data-Sharing Infrastructures: Secure Interoperability across clouds

- Trusted data ecosystems
- Certified connector components
- Identity Management

Cyber Secured Hardware, Operating System and Middleware

Who can do it: Belgium, Estonia, France, Italy, Germany, Spain, The Netherlands

- Trusted Hardware:
  - **Academia:** CEA, Fraunhofer, INRIA, imec, PoliTorino, TUM
  - **Industry:** Globalfoundries, G&D, Gemalto, Thales, ST Microelectronics
- Trusted Operating System platforms
  - **Academia:** Fraunhofer, INRIA, TUM, TUDresden, VU Amsterdam, UniMurcia
  - **Industry:** Hensoldt, Airbus, Genua, SUSE
- Trusted Security Testing Toolchain
  - **Academia:** CEA, CISPA, KULeuven, UniTrento, Imdea, Fraunhofer, TUM
  - **Industry:** SAP, xanitizer, Gemalto, RIPS
- Trusted Data-Sharing Infrastructures:
  - **Academia:** Fraunhofer, INRIA, TUM, UniMilano
  - **Industry:** SAP, Deutsche Telekom, Bosch, Atos, Vicomtech, Tecnalia, Cybernetica

Note: the listed partners are examples to show, that Europe has the capacity and power to do it!

Cyber Secured Hardware, Operating System and Middleware

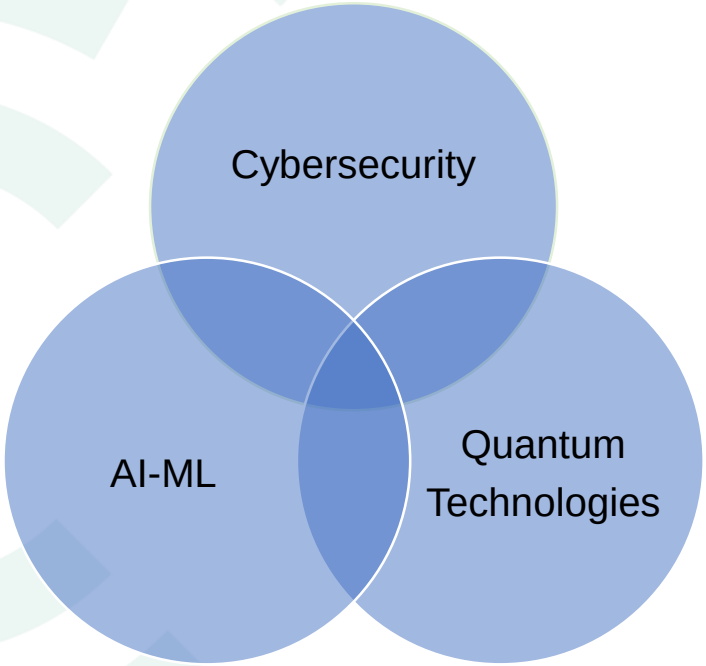
How much funding is required?

- Trusted Hardware: 80-100 Mio Euro (for up to 7 years)
- Trusted OS platforms: 40 Mio Euro (3 years)
- Testing tool chain HW/SW artifacts: 60 Mio Euro (3 years)
- Trusted Data Sharing Infrastructure: 80 Mio (2 years)

Quantum Technologies

- Gabi Dreo, RI CODE, CONCORDIA
- Helmut Leopold, AIT, OPENQKD
- Fabio Martinelli, CNR, SPARTA

Intro: Quantum Technologies, AI-ML, Cybersecurity



Quantum Computing
Quantum Communication
Quantum Simulation

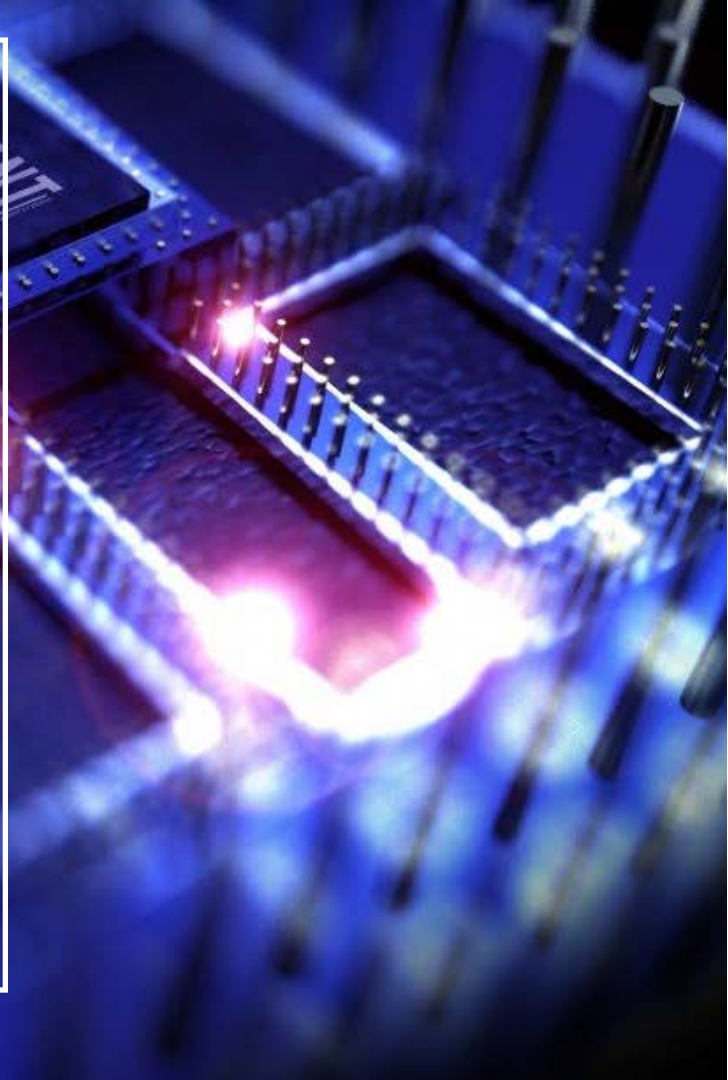
Europe Needs a Strong Cybersecurity Ecosystem and Trustworthy IT!

Europe Needs a European Quantum Internet, connecting quantum computers, simulators, and sensors via quantum networks!

Intro: Security is at Risk

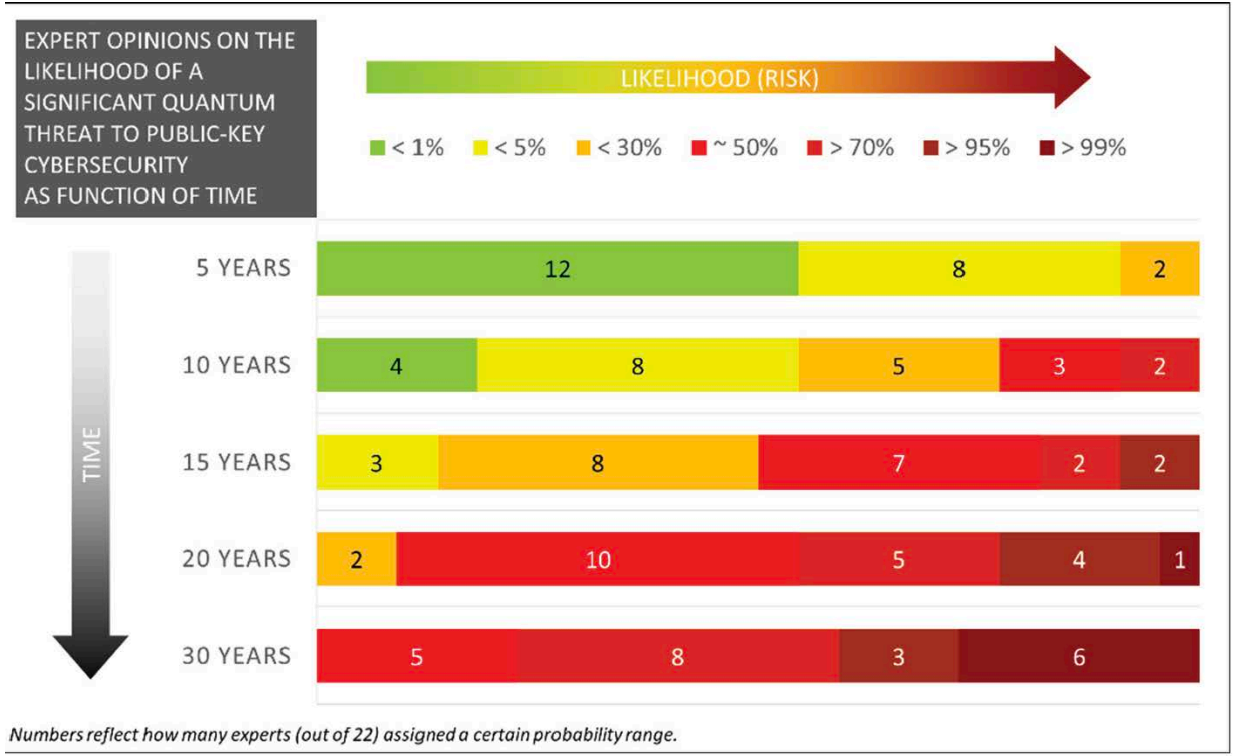
Quantum computers can break codes with astronomically fewer steps, posing a threat to the pillars of today’s cybersecurity defences

The bottom line is that whenever quantum computing arrives, we need to be ready for the security challenges it will present. And the time to start preparing is now.



Quantum Threat

Quantum Threat Timeline



Topics

1. **Quantum Computing**

   e.g. RI CODE with the IBM Q-Hub (1 of the 8 worldwide)

2. **Applied Post-Quantum Cryptography**

   The need to develop quantum computer resistant crypto algorithms and mirgration paths to transform architectures/software into QC resilient ones

3. **Adaptation, integration and migration of legacy ICT system for Quantum advent**

4. **Quantum Communication and Quantum Key Distribution**

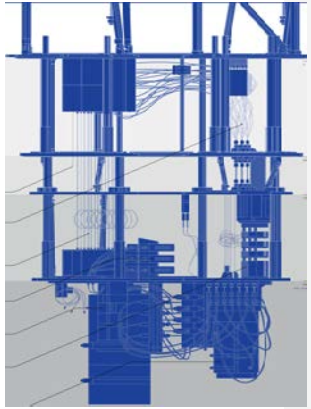
   e.g. EU Project https://artes.esa.int/news/esa-and-ec-sign-agreement-european-quantum-communications with 10 EU Member states

5. **Education and training of a new generation of practitioners and researchers in the field**

1. IBM Q Hub @ RI CODE

Cooperation Partners

- Leibniz Supercomputing Center
  - LMU
  - TU München
  - Hochschule München
- DLR
- Research center Jülich
- ZITiS
- Giesecke + Devrient
- secunet
- Siemens
- ...



IBM Q Hubs Worldwide

慶應義塾 Keio University
Universität der Bundeswehr München
The University of Melbourne
Oak Ridge National Laboratory
University of Oxford
INL International Iberian Nanotechnology Laboratory
NC State University
國立臺灣大學 National Taiwan University

1. Application of Quantum Computing (I)

Research: Quantum ML and Security:new risks, new opportunities

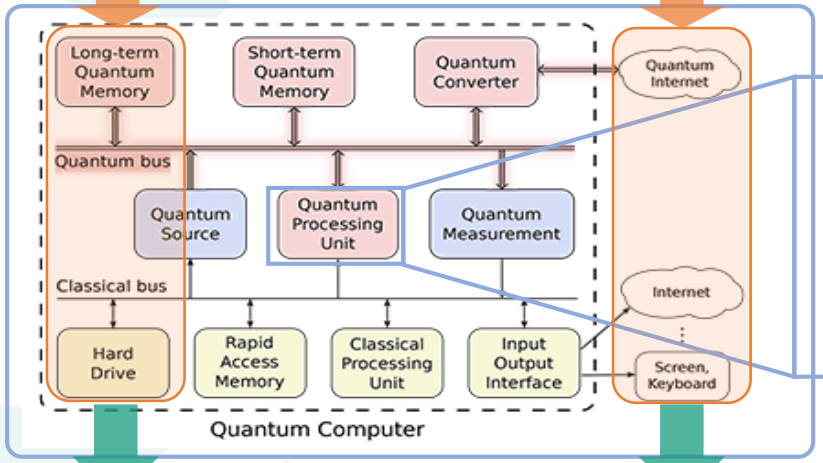
Security Threat

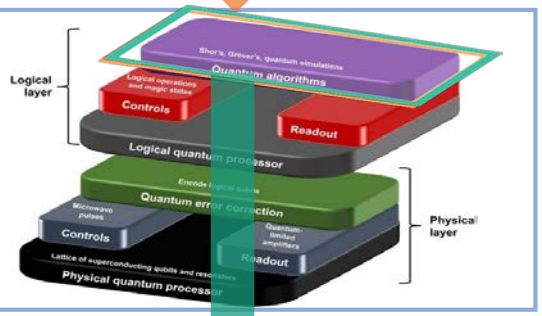
(Quantum) Poisoning Attacks

Information Leakage

Adversarial Attacks (Evasion, Inversion)

ML relevant QC Technology Stack





Defensive Technique

Sanitization, Access Protection & Detection

Privacy Preserving QML
Quantum Speedup of ML for Security: improved anomaly dectection, improved threat analytics

Robust QML Algorithms

2. Post-Quantum Cryptography

Vulnerable to a quantum attack are:

- Any cryptographic primitive based on Integer Factoring and Discrete Logarithms.
- This includes RSA, DSA, DH, ECDH, ECDSA and variants.
- Any security protocols that derive security from the primitives.
- Any products or security systems that derive security from the above protocols.

➢These Systems need to be replaced or hardened

Impacted but not broken:

- Primitives such as AES and SHA-3.

➢These Systems need longer keys

Quantum Safe Cryptography (post quantum / quantum resistent)

- Algorithms that run on todays *conventional* computers
- That are secure against a quantum adversary

2. Applied Post-Quantum Cryptography

How can we protect data and systems today against future quantum computers?

- Design of novel post-quantum protocols for privacy and digital identity protection
- Implementation of post-quantum algorithms on special hardware, i.e. high-speed FPGAs, constrained IoT, smart cards
- How can we establish migration paths from existing and running software to QC resilient software. Migration normally takes very long time, 10 years or more, we must start to develop solutions for European industry right now
- How should agile software and hardware architectures look like to securely exchange crypto modules with QC-resilient ones.
- How to adapt the used protocols accordingly

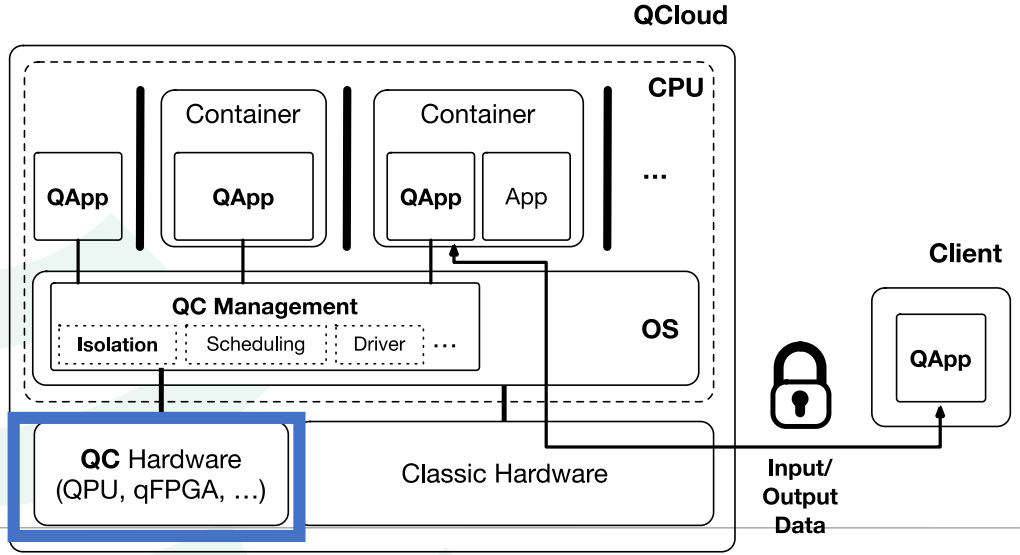
2. Post-Quantum Cryptography

- A lot of Research: e.g. the NIST PQC Project
- Post-Quantum Cryptography – competition for Key Encapsulation (KEM)/Encryption and Signatures
  - 2 (or 3) rounds
  - 1st round 82 submissions, 69 accepted,
  - 2nd round started (May 2019)
    26 candidate algorithms (17 encryption/KEM, 9 signatures)
  - 2017-2020
  - + 2 years for standard phase
  - See: www.nist.gov/pqcrypto

3. Adaptation of ICT to quantum advent and integration of quantum solutions with classical ones

Research questions :

- Designing new hybrid architectures
  - QC devices should be securely attachable to cloud platforms.
- How to protect sensitive business data on the QC devices (trusted QC Management)



4. Quantum communications

DIGIBYTE | 13 June 2019

The future is quantum: EU countries plan ultra-secure communication network

ESA and EC sign agreement on European quantum communications

4. Strategic Autonomy and Technology Leadership of Europe

- **Technologie – Leadership**
  - AI
  - Cyber Security
  - Quantum Technology

- Strategic Autonomy of Europe in the global Digital Space for Data Communication and Data storage
  - Data integrity & authenticity in all market segments
  - Security Technologies „made in Europe“
  - European Quantum Security Infrastructure – fibre + satellite

EU R&D Programm	**International Standardization with a European position ITU/ETSI/ISO/ …**	**EU Infrastructure Programm Satellite + Fibre**	**European Application Trials/Demos: EU Project OPENQKD**	**EU Industry Invest Programm**

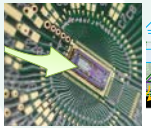
QCI Vision

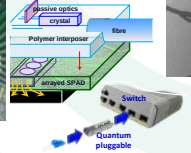
4. Quantum Communication R&D + OPENQKD

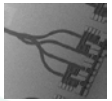
EU SAGA Programm

UNIQORN	CiViQ	QIA	QRANGE	esa
Miniaturization on the chip smaller, cheaper, and highly integrated	Development of high performance QKD components and systems for telecom networks	QIA Quantum Internet Alliance – Entanglement based Quantum Internet	Quantum random number generators	

ESA ARTES Skylight Project **QUARTZ**







OPENQKD – Infrastructure Trials and Use Cases in Europe

Euro **QCI** Quantum Communication Infrastructure 2019-2029
DE, ES, IT, NL, LU, MT, BE, PT, HU, PL, …

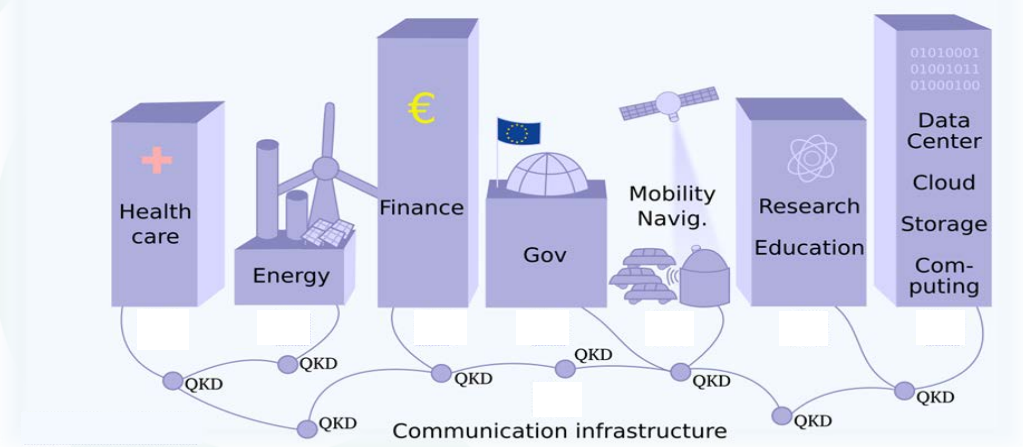
National programs:

- Germany
- France
- Italy
- Netherlands
- Sweden
- ….

4. OPENQKD
Comprehensive European Initiative for Trialing and Demonstration of QKD (38 partners)

- **European** leading academic and RTOs with strong background in quantum communication technologies
- Network equipment vendors
- Network operators and service providers
- Security product and application providers
- Business and **governmental end-users**
- Certification and standardization agencies

4. OPENQKD Application Areas
Secure Data Pillars of our modern society



- Securing Government Communication
- Securing sensitive medical data
- Secure cloud storage
- Securing Smart Grids
- Securing Banking transactions
- Securing Time signal reference distribution

eGovernment	Critical Infrastructures	Industry 4.0	IIoT

Privacy	Data Authenticity	Data Integrity	Data Souvereignity

5. Education and training for a new generation of practitioners and researchers

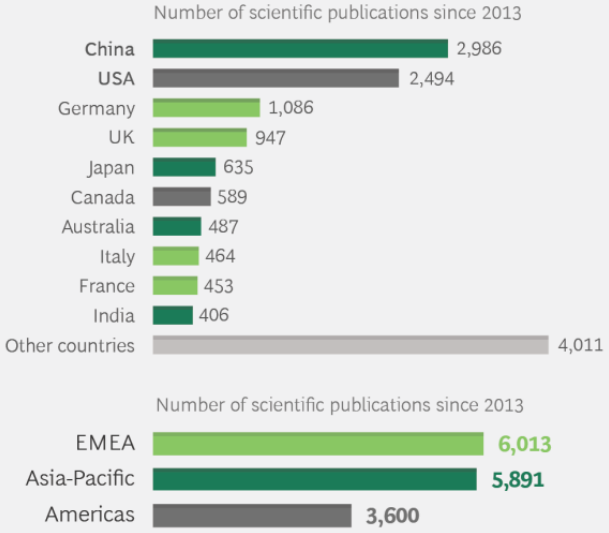
The challenge:

- There is the need and the opportunity to make growth a genration of scientists with knowldge in classical security as well as on quantum solutions
- Currently the scientific community as quite separate
- There is the need to integrate multi-disciplinary expertise

Backup Material

EXHIBIT 5 | China Leads in Publications on Quantum Computing, But the US Is More Integrated Internationally

China leads by country
EMEA leads by region



US has strongest institutional collaborations[1]

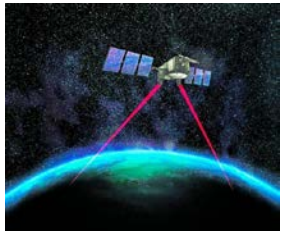
	China	US	Germany	UK	Japan	Canada	Australia	Italy	France	India
China	1,529									
USA	224	894								
Germany	102	240	309							
UK	116	288	187	248						
Japan	116	210	124	102	239					
Canada	194	187	82	70	35	221				
Australia	59	80	54	68	35	66	121			
Italy	25	64	124	135	14	26	22	271		
France	28	96	111	116	95	19	35	88	173	
India	10	19	20	6	7	10	7	1	7	156

Sources: Web of Science; BCG Center for Innovation Analytics.
Note: Analysis based on approximately 10,000 scientific publications related to quantum computing submitted from 2013 to mid-2018; EMEA=Europe, Middle East, Africa
[1]Where two or more universities from the same country were affiliated with the same publication, they were counted as one internal collaboration.

QKD Infrastructure – fibre + satellite

Enabling highly secure key distribution on a global scale

QKD
Key distribution via satellite



ESA ARTES Skylight
Project **QUARTZ**

EU SAGA Programm

QKD
Key distribution via optical fibre networks in Europe

National programs:

- Germany
- France
- Netherlands
- Sweden
- ….

QKD
Applications / Use Cases / Trials

EU Project OpenQKD

1. APPLICATION OF QUANTUM COMPUTING (I)

Research

Optimization of Quantum Computing

- Definition of problems (use cases) that can be solved by Quantum Computing
- Research in AI-ML in Cybersecurity, Deep Learning with Quantum Computing, ...
- Usage of Quantum Computing in Geoinformatics and other sectors
- Improved predictive security: using QC to compute ML models and gain complete new results (due to new computation paradigms) to improve security.
- Adversarial learning for ML with QC: which new kinds of attacks must be addressed how to design QC resilient AI systems
- Apply existing quantum machine learning techniques to land cover classification

Standard and certification tools

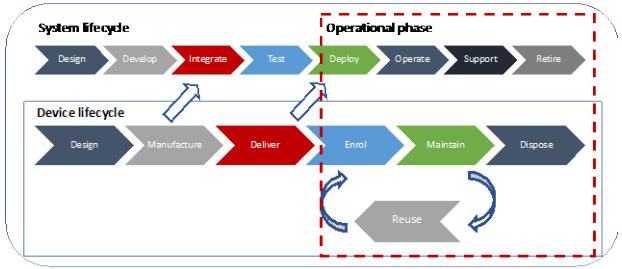
Antonio Skarmeta, UMU <skarmeta@um.es>

Shahid Raza, SICS <shahid.raza@ri.se>

Roberto Cascella, ECSO <roberto.cascella@ecs-org.eu>

Setting the scene – Why certification and standardisation tools are important?

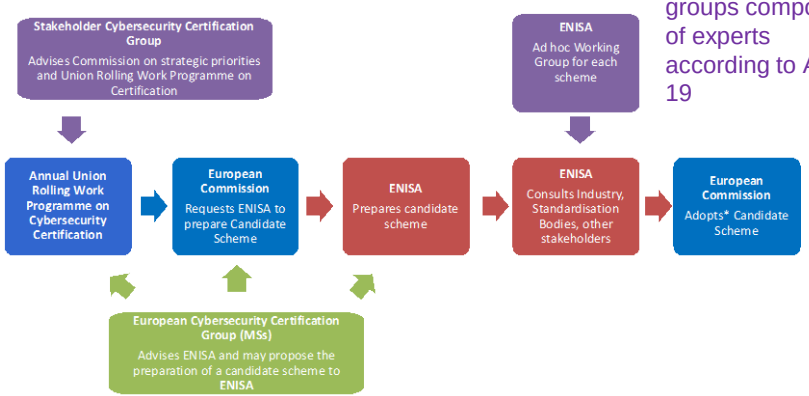
What about the time and space dimension?



Complexity is dramatically increasing!

Source of the figure concept: , ISO/IEC 30141, Information technology – Internet of Things reference architecture (IoT RA)

The context – European Cybersecurity Certification Framework



Ad hoc working groups composed of experts according to Article 19

Source of the image:
https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/1%20Gonzalez.pdf

- Improve the conditions for the functioning of the internal market by **increasing the level of cybersecurity** within the Union
- **Enable a harmonised approach at EU level** of European cybersecurity certification schemes, in view of creating a digital single market for **ICT products, services and processes**
- Simplify procedures, reduce the time and cost of deployment of IT product and services
- Define a mechanism to attest that the ICT products, processes and services that have been evaluated to comply with specified security requirements
- Increase trust and give users more confidence in ICT products and services

Some joint initiatives under EC umbrella

- Standards
  - Rolling Plan for ICT standardisation 2020 under definition (ECSO participates) → Coordinated actions for standardisation

- Cloud security certification
  - Recommendations for the implementation of the CSP Certification scheme (ECSO joined their workshop)

- JRC Pilot project on IACS – ERNCIP project – <u>ongoing</u>
  - Recommendations for the implementation of the Industrial and Automation Control Systems components Cybersecurity Certification scheme (ECSO participates)

Certification and standards – What industry worries about (examples)

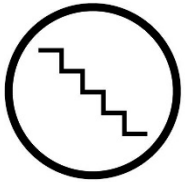
Too slow and too unpredictable

Not flexible enough

Lack of harmonization

Too expensive

Too much formalisms



lack of agility

Undetected cheaters in the supply chain

Static certificates

Pure checklist evaluations

complex composite certifications

*Challenges of the Industry document of ECSO WG1

The way forward – What the industry expects

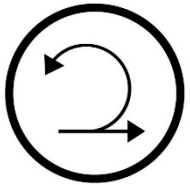
Fast and predictable

High level of flexibility

Full harmonization

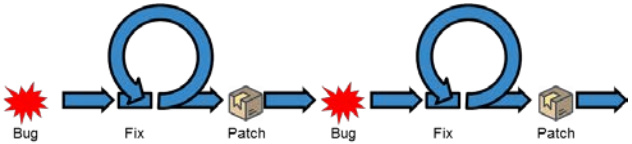
Efficiency

Pragmatism



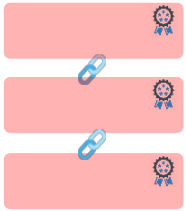
Agility

Detecting cheaters in the supply chain



Patching and updates

Ethical hacking



Lean modular composite certifications

ECSO work already available…. ➔ to foster trust in digitalization and promote innovation

ECSO Meta-Scheme Approach helps to harmonise the minimum security requirements, define a unified levelling across verticals, and provide a common way to define the scope and required security claim

- https://www.ecs-org.eu/documents/publications/5a3112ec2c891.pdf

It can act as a methodological tool to structure the landscape, "glue" together the existing schemes and specify additional steps

ECSO Assessment options explains how to benefit from the right mix of security assessments, and what constraints to be aware of

- https://www.ecs-org.eu/documents/publications/5d6fbbd00cfe7.pdf

It provides insights to organisations that are building their cybersecurity capabilities and need to choose how to assess security

ECSO State of the Art Syllabus provides a cartography of existing certification schemes and standards (products & components; ICT services; service providers & organisations; security professionals)

➔ 290 standards & certification schemes

We are updating the SOTA:
Have your say and contact us
<wg1_secretariat@ecs-org.eu>

Develop capabilities and capacities for an integrated cross-border and cross-sector certification approach

- **Challenges**
  - Trust of evidence in cybersecurity assessment
  - Impact of emerging technologies, such as 5G and IoT, and softwarisation enlarging the attack
  - Time dimension and need to address the whole lifecycle
  - Time to market and cost factors are critical especially for SMEs
  - Lack of common tools and testing environments
  - Skills and training to assess and operate product/services/systems
  - Needs for capacity building in conformity assessment bodies in accordance to Cybersecurity Act
- **Potential benefits**
  - Increase of end users' trust in EU products and competitiveness across Member States.
  - A stronger, more innovative and more competitive EU cybersecurity industry, fostering technological autonomy
  - EU industry better prepared for the threats to ICT systems
  - Common approaches across vertical sectors, and tools and platforms for SMEs entering the ICT market for a faster adoption of best practices in the related industry, enforcing the security at early stages
  - An aligned vision on cybersecurity will foster the implementation of EU cybersecurity legislation

Standards and certification for cyber resilient infrastructures – continuous assessment

- **Benefits and why this is needed**
  - Lack of a common European regulation and certification framework in cybersecurity
  - Integration of smart devices and IoT in infrastructures
  - Certification process is very slow comparing with the device updating requirements
- **How to implement it**
  - Develop automated tools and methodologies to deal with the heterogeneity of current standards and certificate schemes, facilitating the comparability and avoiding multi-certification
  - Design and establish a platform for sharing cybersecurity certification information, in order to increase trust and transparency among stakeholders, including manufacturers and end users from different Member States. Important for the reuse of evidence
  - Tools for partial and continuous assessment and lean re-certification of systems
  - Tools for management of evolving threats due to the integration of IoT with legacy systems
  - Develop skills for professionals and operators of infrastructures
  - Fostering consensus among industry, operators and policy makers to identify a common set of requirements to be considered to assess key domains
  - Development of Digital Twin capabilities for continuous assessment and integration of new solutions
- **Impact that can be achieved**
  - Increased confidence in the functioning of a critical sector, based on the development of more robust and secure products
  - Management of the supply chain and integration into critical infrastructure. Reuse of certificate evidence to speed up the certification process
  - Harmonized vision of cybersecurity requirements and risks and traceability of security evaluation and assessment along the supply chain
- **How much funding is required?**
  - 100Mio Euro (3 years) and additional funding for mapping sector specific requirements

Vulnerability disclosure and handling processes

- **Benefits and why this is needed**
  - Reach higher automation and improvement of security during product/service/software lifecycle
  - Concrete instruments to embed secure by design principles via a risk assessment and management approach
  - Existent non-European approaches (NIST National Vulnerability Database and CVE MITRE)
  - Ensure continuous assessment (time dimension)
- **How to implement it**
  - Creation of a *federation of different European database* for known cybersecurity vulnerabilities: trusted party to maintain accurate information and access control policies to limit vulnerabilities exploitation. Some individual efforts already exists (ex. CEF VARIoT project
  - Definition of coordinated Common Vulnerability Disclosure programmes (ex. https://zerodisclo.com)
  - Analysis of current best practices, standards, and certification schemes whether they include that include vulnerability management and alignment with global industry best practices and international standards
  - Define how to assess the risk and metrics for each vulnerabilities and automated mitigations of vulnerabilities
  - Implement a push notification system to protect and mitigate risks in products affected by critical vulnerabilities
  - Create bug bounty programmes (ex https://firebounty.com)
  - Cyber-secure modelling via digital twin simulated environment (es. AIT initiative
- **Impact that can be achieved**
  - Increased security of products/services/systems by drawing attention to the need to update and patch.
  - End-user will benefit more secure products
  - Definition of patches and updates management process to prevent cyber threats exploiting known vulnerabilities
  - Life-cycle management of security
- **Expected funding**
  - 50Mio Euro (3 years) and additional funding for bug bounty programs or technology/sector specific DB

Develop tools to automate evaluation compliance and checking during the lifecycle

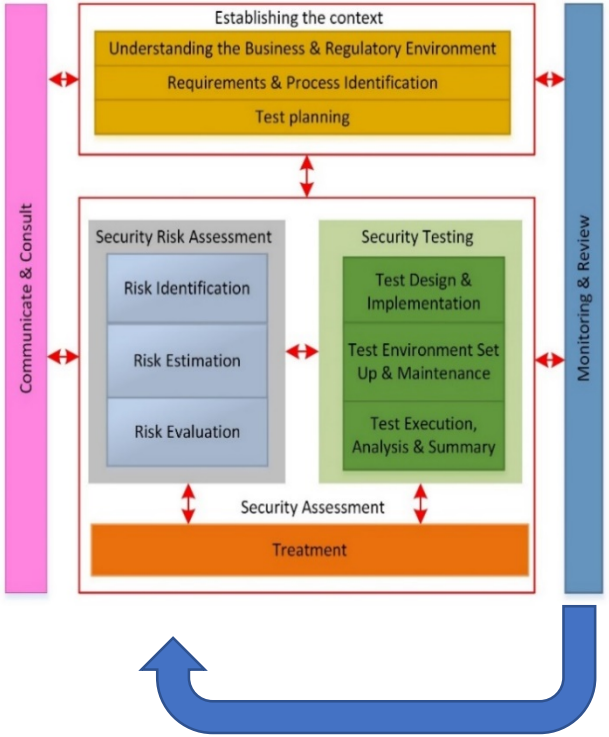
- **Benefits and why this is needed**
  - Current certification schemes need to consider the dynamic nature of cybersecurity in real life scenarios
  - New vulnerabilities/threats and updates/patching demand for continuous evaluation (certification) during lifecycle (Cybersecurity Act, Article 51)
  - Reduce the time to markets of products and, even more critical, of software and services where the release cycle is shorter

- **How to implement it**
  - Tools for automated compliance checking, threat identification, system assessment and certification compatibility (static) / Most of current tools focus on dynamic analysis of software
  - AI-based tools for continuous evaluation of security functionalities, impact of updates, real-time assessment, patching and lean re-assessment ➔ automatic identification of vulnerability and patches (dynamic) / cooperation with AI initiatives
  - Use of automated tools for security assessment and testing under a standard-based methodology (e.g., based on ETSI ETSI EG 203 251 V1.1.1) and tools for analysis of security certification reports (CC EAL, FIPS140-2)
  - Define a common taxonomy across sectors and tools to maintain cyber security in cross-sectorial systems (initial effort in some sectors such as manufacturing Semi40 and Arrowhead Tools)
  - Simulated environments for threat management: cyber range to train professionals and digital twins to test security functionalities and patches
  - Open tools and testing certification labs to easy SME access to the precertification of products
  - Develop skills for ethical hackers and professionals and bug bounty skills

Develop tools to automate evaluation compliance and checking during the lifecycle

- **Impact that can be achieved**
  - Better adoption of certification process in the EU industry to increase users' trust in their products
  - Management of the supply chain, cybersecurity evidence of products, services and systems for certification
  - Raised the bar of the security baseline by stimulating competition and better services to the market
  - Provide mechanisms to SMEs and companies to internally assess and evaluate products, supported by financial incentives
  - Tools to support the life-cycle management of security increasing easy access to SME
  - Connection to the Cyber Secured Hardware, Operating System and Middleware challenge

- **Expected funding**
  - 80Mio Euro (3 years) and additional funding for mapping sector specific requirements



EU security information sharing framework among Member States

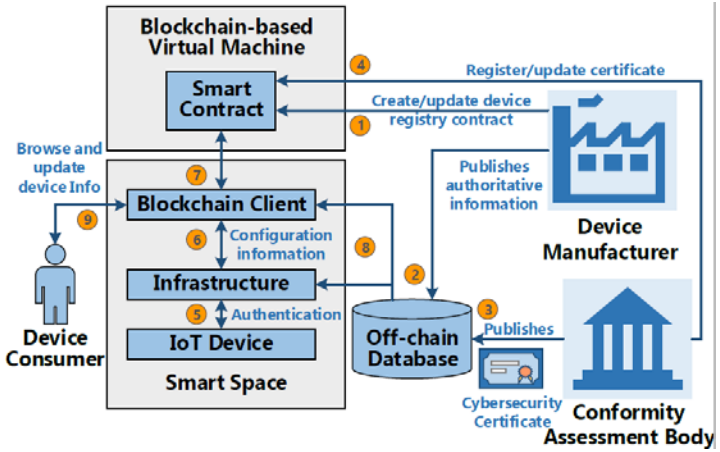
- **Why is it important**
  - Emerging technologies such as 5G or IoT are fostering a hyperconnected world, which implies that vulnerabilities are more frequent and borderless
  - Multiple certification schemes and standards are used in different Member States to certify ICT and are not mutually recognized. Multiple certification schemes will coexist.
  - Sharing mechanisms are explicitly mentioned and encouraged by NIST and Cybersecurity Act
- **What should be done?**
  - Developing a EU sharing approach through the integration of MS platforms to manage the information about ICT products, services and process related with security configuration, updates, vulnerabilities, certificates and relation with other components.
  - Support open testing platform
  - Security information disclosure and handling processes
- **How can it be done?**
  - Developing a EU sharing approach through the integration of MS platforms to manage the information about ICT products, services and process
  - Blockchain [1] as a potential solution involving different ICT stakeholders
  - Fostering the cooperation with ENISA, certification assessment bodies, national authorities and manufacturers

[1] Ricardo Neisse, José L. Hernández-Ramos, Sara N. Matheu, Gianmarco Baldini and Antonio Skarmeta. "**Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices**" in IEEE *CSCN* 2019

EU security information sharing framework among Member States

- **What can be achieved?**
  - Integrated approach to transparently reflect the security level of an ICT component and the dependencies with other products
  - Increasing alignment with Cybersecurity Act (Article 4, 6) on cybersecurity information sharing
  - More trusted self-assessment process (Cybersecurity Act, Article 53)
  - Connection to Cyber Range and Threat Intelligence challenge

- **Who can do it?**
  - Involvement of ENISA, certification assessment bodies, national authorities and manufacturers. Including EU initiatives on blockchain (Blockchain Observatory & Forum, European Blockchain Partnership (EBP), International Association of Trusted Blockchain Applications (INATBA))
  - RTO: ECSO, RISE, UMU, UPS, CYBER, VTT, NTNU, UMA
  - Industry: ATOS, CONCEPTIVITY, NEC, Orange, SGS, Thales, ENG, Siemens
  - Industrial sector: banking, telcos



- **How much funding is required?**
  - 50Mio Euro (3 years) and additional funding for bug bounty programs or technology/sector specific DB

https://ec.europa.eu/digital-single-market/en/blockchain-technologies

Creation of cybersecurity behavioral profiles to reflect the intended behavior and usage of an ICT product, service or process in the value chain

- **Why is it important**
  - To reduce the attack surface across ICT systems and reducing propagation of vulnerabilities and attacks
  - Alignment with Cybersecurity Act (Article 55) on the need for supplementary cybersecurity information

- **What should be done?**
  - Fostering cooperation with/among manufacturers to encourage adoption of standards for defining profiles
  - Integration with the cybersecurity certification process to identity and mitigate potential suspicious behavior
  - Create an EU vulnerability database

- **How can it be done?**
  - Based on a standardized behavior specification, for example the recent IETF MUD standard, which has received an increasing attention (e.g., NIST [2])
  - MUD profiles can be generated from the certification process to obtain an evidence based set of rules describing the expected behavior of the ICT product.
  - MUD enforcement can be performed through Software Defined Networks (SDN) and Network Function virtualization (NFV)
  - Involvement of manufacturers across the EU is crucial

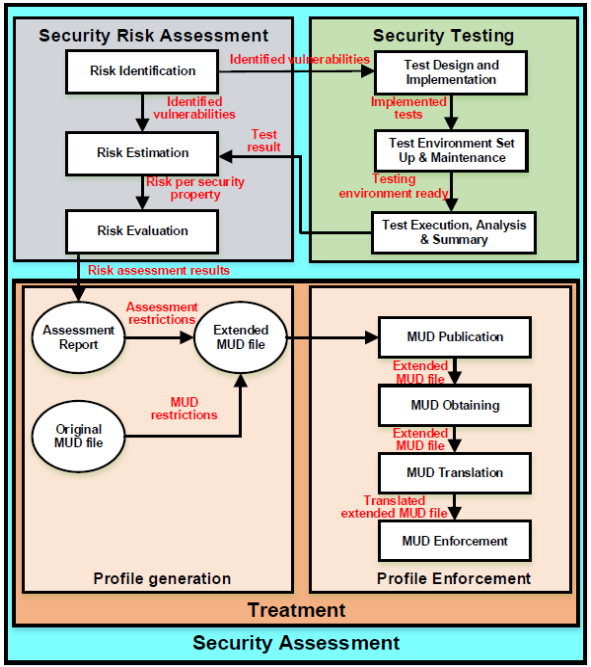
[2] NIST SPECIAL PUBLICATION 1800-15A. **Securing Small-Business and Home Internet of Things (IoT) Devices Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD).** November 2019

Creation of cybersecurity behavioral profiles to reflect the intended behavior and usage of an ICT product, service or process in the value chain

- **What can be achieved?**
  - Reduction of the attack surface and propagation of vulnerabilities
  - Increasing trust of manufactured ICT products, process or services across the EU
  - Increasing capacity to detect and react against potential cybersecurity attacks or vulnerabilities
  - The adoption of standard technologies (e.g., MUD) by manufacturers via incentives to reduce effort in certification process
  - Accelerate the adoption of certification tools

- **Who can do it?**
  - The adoption of standard technologies (e.g., MUD) by manufacturers is crucial
  - RTO: UT, BRNO, UMU, CYBER, UNITN, VTT, RISE, UPS, CEA
  - Industry: IoTivity, Industrial Internet Consortium, Philips, Thales, SGS, ENG, Schneider
  - Certification and standardization agencies

- **How much funding is required?**
  - 40 Mio Euro (2 years)



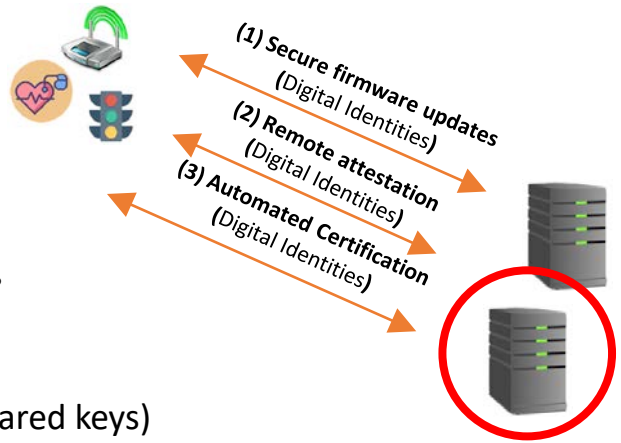
Automated Certification for IoT – Digital TRUST for Digital Systems

Why is it important

- Cybersecurity breaches are frequent not only because humans are the weakest links, rather technical cybersecurity solutions demand human involvement
- Many IoT devices have no software update mechanism. Others are only certified for their factory-installed firmware where ***software update breaks certification***

What to do?

- Update → Attest/Audit → (Re-) Certify



How to do (Device-side)?

1. Automated ways to bring digital identifies to IoT
2. Software updates for IoT – no proprietary solution
3. Trusted hardware with *trusted execution environment* and *secure storage*
4. Remote audit and attestation

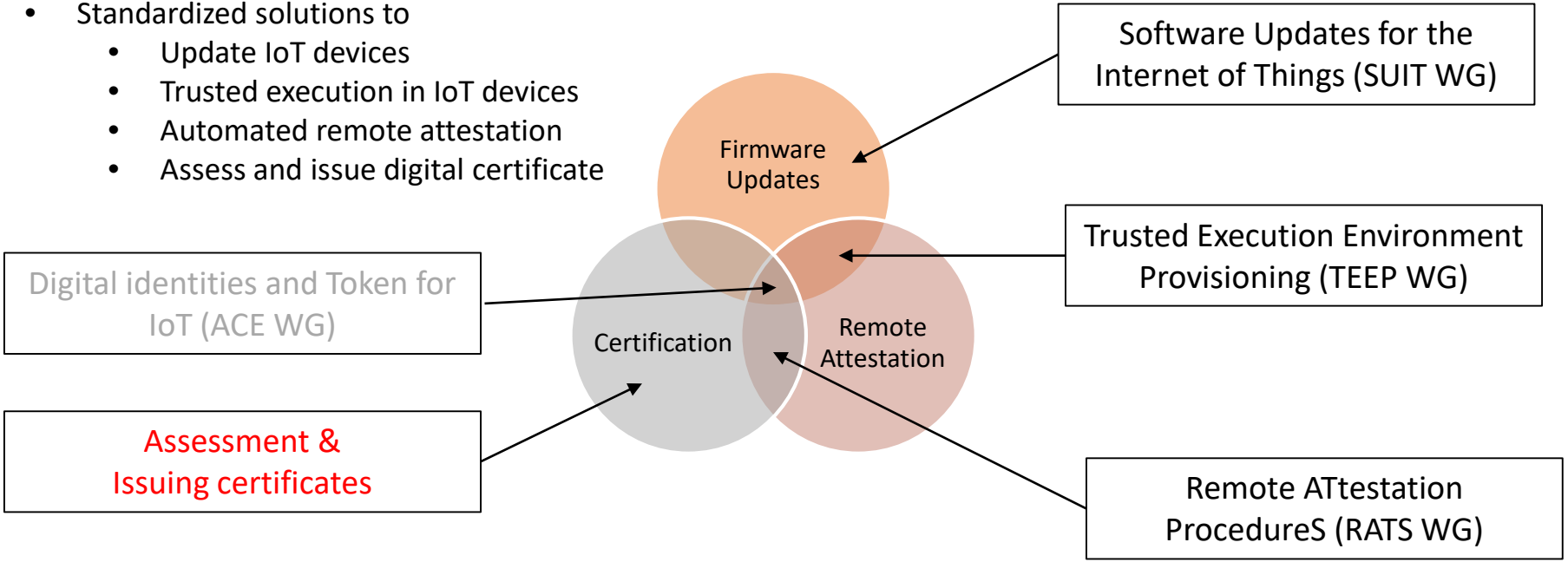
What can be achieved?

- PKI for IoT: Zero-touch security for IoT devices (no PINs/Passwords/pre-shared keys) with no trusted entities on the way – Pure End-to-End security
  - Enrolment already standardized (IETF ACE)
  - Cost-effective, lightweight digital certificates/identities

Automated Certification for IoT – Do we already have standardization forums?

What can be achieved (continue…)?

- Standardized solutions to
  - Update IoT devices
  - Trusted execution in IoT devices
  - Automated remote attestation
  - Assess and issue digital certificate



Automated Certification for IoT – Do we already have standardization forums?

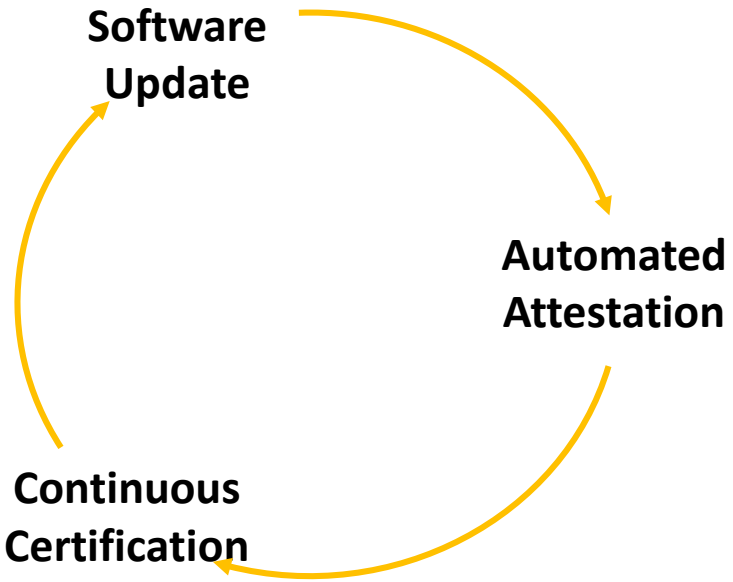
Who can do it?

RTO: TU Domstadt, RISE, UMU, NTNU, VTT, CEA, CERTH
Industry: Cyber Services, Ericsson, Nexus, SGS, IBM, NXP, Thales, infineon
Potentials CABs: RISE, SGS, EUROSMART, Applus+, Riscure

How much funding is required?

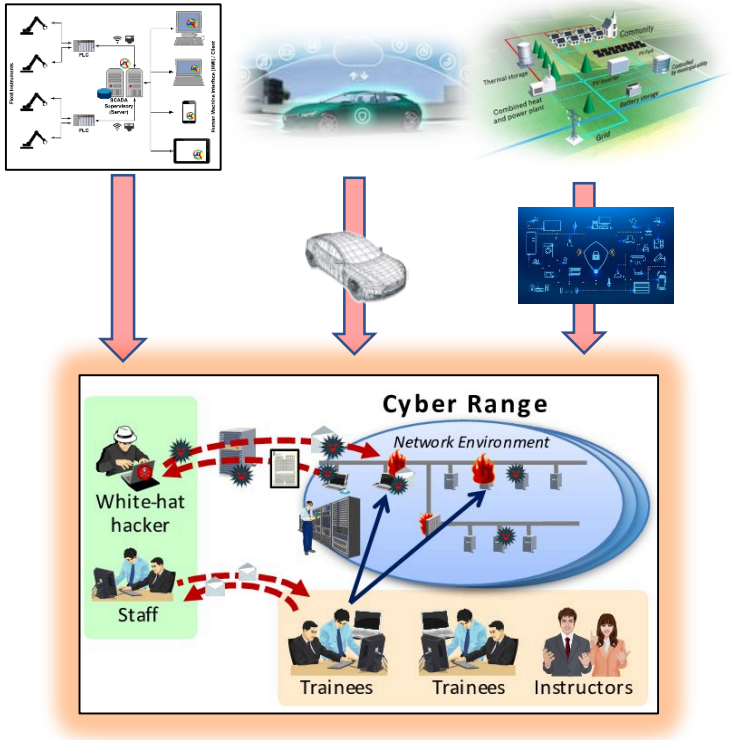
10 Mio Euro (3 years)

*Single digital certificate(identity) for both **authentication** and **assurance***
(Automated proof of certification)



Cyber Range as a Certification Assessment Tool

- Automated ethical hacking
- Standalone vs. full cyber environment assessment
- Automated attacks (red/blue teams)
- Realtime access to vulnerability databases
- Digital certification leads to ***digital trust***
  - No human error/favouritism/kickbacks



Who can do it?

RTO: RISE, JAMK, NTNU, Uni. Maribor, CODE, FOI, …
Industry: RHEA, Cyber Services, SGS, Thales, Air Bus, (plus vertical)
Potentials CABs: RISE, SGS, EUROSMART, Applus+, Riscure

How much funding is required?

15 Mio Euro (3 years)

*RISE Sweden is a **certification body,** owns a **cyber range,** and a leading IoT security research and standardization group*