Towards a European Cybersecurity Competence Network

Overview of the selected pilots

Gregory Blanc (IMT/Télécom SudParis)

3rd EUNITY Workshop
April 26th, 2019 – Kyoto

SU-ICT03-2018

- « Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity R&I Roadmap »
  - RIA call opened from Feb. 1st to May 29th, 2018
  - Overall budget 50M€
- 13 submitted proposals
  - 9 above threshold
  - Total requested budget : ~145M€
  - 4 pilots selected

Motivated by a Joint Communication to the European Parliament and the Council (JOIN(2017) 450 Final, Sept. 2017)

Overview of the selected Pilots

Acronym No.	Title (duration in months)	Coordinator (consortium size)	Total cost
CONCORDIA 803927	**Cyber security cOmpeteNce anD Innovation (48)**	**Universitaet der Bundeswehr Muenchen (42 partners)**	**16M€**
CYBERSEC4 EUROPE 830927	**Cyber Security Network of Competence Centres for Europe**	**Goethe University Frankfurt (43 partners)**	**16M€**
ECHO 830943	**European network of Cybersecurity centres and competence Hub for innovation and Operations**	**Ecole Royale Militaire Koninklijke Militaire School (30 partners)**	**16M€**
SPARTA 830892	**Strategie Programs for Advanced Research and Technology in Europe**	**CEA (44 partners)**	**16M€**

Building Cybersecurity Capabilities

- Per the Joint Communication 450 (Sept. 2017)

  « Building on the work of MS and the PPP reinforce EU cybersecurity capability through a network of cybersecurity competence centres with a European Cybersecurity Research and Competence Centre at its heart »

- A Competence Network and the Centre:
  – cybersecurity **technological** and **industrial** capacities necessary to secure **DSM**
  – **competitiveness** of EU's cybersecurity industry
  – cybersecurity to be a competitive advantage of **other EU industries**

Goals and beneficiaries

- Goals
  - Pool, share and give access to existing **expertise**
  - Co-invest and share costly **infrastructure**
  - Help deploy EU **products and solutions**
  - Ensure long-term strategic **cooperation** between industries, research communities and governments
  - Help overcome the **skills gap**
- For the benefit of:
  - Public Sector
  - Cybersecurity Industry
  - Scientists
  - Businesses incl. eHealth, e-Commerce, energy, smart mobility, finance, IoT, etc.

Technology & Innovation Ecosystem

- European Cybersecurity Competence Centre
  - Manage **funds** for cybersecurity under Horizon Europe
  - Help **coordinate** the Network and Community to drive cybersecurity technology agenda
  - Support joint **investment** from EU, MS and industries
- Network of National Coordination Centres
  - National capacity building, link with existing initiatives
  - Nominated by MS, it may receive funding and pass on financial support
- Cybersecurity Competence Community
  - Large, open, and diverse group of stakeholders
  - From research, private sector, public sector (incl. civilian and defence)

Competence Community

- **Support** the Centre and the Network in achieving their **mission** and **objectives**
- **Enhance** and **disseminate** cybersecurity **expertise** across the Union
- **Participate** in activities promoted by the Network and the Centre
- **Participate** in the Working Groups on specific activities
- **Promote** the outcomes of specific projects

National Coordination Centres

- Nominated by MS and notified to the EC
- Support to Competence Centre in achieving its mission
- Contact Point at national level, facilitates **participation of industries** and other actors
- Assess entities in the MS to **become part** of the Community
- Establish **synergies** with relevant activities at national and regional levels
- Identify and address **sector-specific** cybersecurity industrial **challenges**
- Implement specific actions incl. supporting **national ecosystems**
- Promote and disseminate **outcomes** of the work by the Network, Community and Centre

Competence Centre

- Facilitate and help **coordinate** the work of the Network
- **Implement** cybersecurity parts of Digital Europe and Horizon Europe **programmes**
- Enhance cybersecurity **capabilities**, **knowledge** and **infrastructures** at the service of industries, the public sector and the research communities
- Contribute to the **wide deployment** of state-of-the-art cybersecurity **products and solutions** across the economy
- Contribute to reducing **skills gaps** in the Union related to cybersecurity
- Contribute to the **reinforcement** of cybersecurity **research and development**

Competence Centre – Governance

- Governing board
  - 1 representative of each MS with cybersecurity knowledge and managerial skills
  - 5 representatives of the Commission
  - Renewable term of 4 years
  - Observers admitted (ENISA as permanent)
  - Elected executive director (4 years, renewable once)
- Voting rules
  - Union holds 50% of voting rights
  - Every participating MS = 1 vote
  - Decisions taken by a majority of at least 75% of all votes, representing at 75% of the total financial contributions to the Competence Centre
  - Chairperson takes part in the voting

Competence Centre – IAB

- Industrial and Advisory Board
  - 16 members appointed by the Governing Board among representatives of entities of the Community
  - Expertise in cybersecurity research, industrial development, professional services or deployment
  - Investment of cPPP experience
  - 3 years' renewable term
  - Commission and ENISA participate in the works of IAB
  - Meets twice a year
- Tasks
  - Advises on establishing Working Groups
  - Organises public consultations and provides input for drafting the work plan and multi-annual strategic plan

- Duration: from Jan. 2019 to Dec. 2022
- Objectives:
  1. A Cybersecurity Competence Network with CODE research center as coordinator and ENISA as secretary
  2. Using an open, agile and adaptive governance model and processes that combines the **agility** of a start-up with the **sustainability** of a large center
  3. Devise a cybersecurity **roadmap** to identify powerful **research paradigms**, to do hands-on **experimental validation**, **prototype** and solution **development**
  4. Develop next-generation cybersecurity solutions by taking a **holistic end-to-end data-driven** approach

- Objectives:
  5. **Scale up** existing research and innovation with CONCORDIAs **virtual lab** and **services**
  6. Identify **marketable** solutions and grow **pioneering** techniques towards fully developing their transformative potential
  7. Develop **sector-specific** (vertical) and **cross-sector** (horizontal) industrial pilots with building **incubators**
  8. Launch **Open Calls** to allow entrepreneurs and individuals to stress their solutions with the development

- Objectives:
  9. Set up an Advisory Board, comprised by leaders of industry, standardization, policy and politics
  10. Mediate between **multiple communities**
  11. Establish a **European Education Ecosystem** for Cybersecurity
  12. Provide **expertise** to European policy makers and industry

- Liaisons:
  - ENISA
  - EUROPOL
  - EDA
  - CCDCOE
- Verticals:
  - Telecom
  - Finance
  - Transportation/E-mobility
  - E-Health
  - Defence
- Web: concordia-h2020.eu
- Twitter: @concordiah2020

- Duration: from Jan. 2019 to Dec. 2022
- Objectives:
  - Provides EU with **all capabilities required** to secure and maintain a healthy, democratic society, living to European constitutional values and being a **world-leading** economy
  - Follows the intentions of **European legislation** that reflects and protects European societal, democratic and economic norms and principles
    - GDPR
    - eIDAS
    - PSD2
    - ePrivacy regulation
    - ENISA
    - Cybersecurity Act

- Implementation:
  1. **Governance**: leveraging experience from FIDIS or NESSOS networks of excellence and benchmarking from other governance structures (CERN, NIST), devise a proven, feasible and sustainable governance model for the Cybersecurity Competence Network
  2. **Cooperation**: enable novel and forward-looking modes of cooperation between stakeholders with complementary interests and skills from the public and private sectors, research, SMEs, industry, and academia, both European and global
  3. **Building future-oriented European capabilities**: increase the depth and breadth of usable cybersecurity skills in Europe as well as improve access to necessary facilities for research, development, experimentation and testing

- Implementation:
  4. **EU leadership in cybersecurity innovation**: demonstrate that European R&I can effectively create next-generation digital technologies as well as leading-edge products, solutions and services that have strong market potential
  5. **Support the complete industrial value chain**: reinforce European industry as well as address the security and resilience of the Digital Single Market by:
     - Reducing fragmentation to ensure that EU is a net exporter rather than importer of know-how
     - Demonstrating the impact on a broad range of use cases: health, smart cities, finance, e-commerce, transport, supply chain
- Web: cybersec4europe.eu
- Twitter : @CyberSec4Europe

- Duration: from Jan. 2019 to Dec. 2023
- Objectives: **organize and optimize currently fragmented cybersecurity efforts across EU**.
  - **Central Competence Hub** as focal point
  - ECHO **Multi-sector Assessment Framework**:
    - Analysis of challenges and opportunities derived from **sector-specific use cases**
    - Analysis of **transversal** cybersecurity needs
    - Development of inter-sector **Technology Roadmaps** involving horizontal cybersecurity disciplines

- Objectives:

  – Creation of an ECHO Cybersecurity **Certification Scheme**, aligned with ongoing EU efforts

  – Provision of an ECHO **Early Warning System**

  – Operation of an ECHO **Federation of Cyber Ranges**

  – Delivery of the ECHO **Cyberskills Framework**, with training materials and training events

  – Management of an expanding collection of **Partner Engagements**

- Web: echonetwork.eu
- Twitter: @ECHOcybersec

SPARTA

- Duration: from Jan. 2019 to Dec. 2022
- Objectives:
  - Create a networked governance for advanced cybersecurity research in Europe
  - Define and sustain an EU-wide roadmap at the cutting-edge of cybersecurity research and innovation
  - Build sustained collaborations with academic, industrial, governmental, and community stakeholders
  - Innovate to address transformative strategic challenges
  - Support cybersecurity design, testing, evaluation, and certification capabilities
  - Enhance awareness and training capabilities and develop cybersecurity skills
  - Demonstrate ethical sustainability

- T-SHARK – Full Spectrum Situational Awareness will expand the reach of **threat understanding**, from the current **investigation-level** definition, up to **strategic considerations**, down to **real-time events**
  - Decision-making tools
  - Common cybersecurity culture
  - Preparedness for possible disruptions and attacks
- CAPE – Continous Assessment in Polymorphous Environments will enhance **assessment** processes to be able to perform **continuously** over **HW/SW** lifecycles and under **changing** environments
  - Tools for continuous trust in sovereign and foreign-sourced components, systems and services

- HAII-T – High Assurance Intelligence Infrastructure Toolkit will manage the **heterogeneity** of the IoT by providing a **secure-by-design** infrastructure that can offer **end-to-end** security guarantees
  - Fully verified software stack which can serve in a variety of IoT devices
- SAFAIR – Secure and Fair AI Systems will evaluate the security of AI systems, produce approaches to make systems using AI more **robust** to attackers' manipulation, make AI systems more **reliable** and **resilient** through enhanced **explainability** and better **understanding** of threats
  - Methods and tools for analysis and assessment of security threats for AI systems

- Web: sparta.eu
- Twitter: @sparta_eu

Stay tuned !

- Twitter
  - @eunity_project
- Web
  - www.eunity-project.eu
- Contact points
  - EU coordination : herve.debar_at_telecom-sudparis.eu
  - JP contact point : youki-k_at_is.naist.jp