H2020 FRAMEWORK PROGRAMME
H2020-DS-SC7-2016 DS-05-2016
EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

A resume of the preliminary version of the Cybersecurity Research Analysis Report for the two regions: Research and Innovation Aspects

1) Opportunities of financing in Europe and Japan

The main financing mechanisms in the European region include:

- **European Programmes**:
  - Framework Programmes (now Horizon 2020), where legal entities participate in open competitions.
  - Connecting Europe Facility (CEF)- cybersecurity calls, where the applicants are one or more Member States, international organizations, joint undertakings, public or private undertakings.
- **European Union Agency for Network and Information Security (ENISA)** is the center of expertise for cyber security in Europe, established in 2004 and collaborates with Members States and private sector in order to deliver advice and solutions. The main areas in which ENISA focuses are: recommendations, actions supporting policy making and implementation and 'Hands On' work, where ENISA collaborates directly with operational teams throughout the EU.
- **EUREKA**: a framework programme with main aim: "*raising the productivity and competitiveness of European businesses through technology. Boosting national economies on the international market, and strengthening the basis for sustainable prosperity and employment*."
- **National financing mechanisms** - analysis using project partner's countries (France, Greece, Spain, Poland, Belgium) as a sample
- **Mixed** (national and international funds)
- **Other forms of financing mechanism:**
  - French Marie Sklodowska-Curie actions/grants & research infrastructures support
  - European Strategy Forum for Research Infrastructures (ESFRI)
  - European Structural and Investment Funds (ESIF)
  - PRIMA initiative (Euro-Mediterranean cooperation)
  - Euratom (European Atomic Energy Community) programs supporting projects connected to nuclear energy (potential cybersecurity aspects)

The main funding mechanisms in Japan include various funds provided by the government. Mainly these include:

- **The Ministry of Internal Affairs and Communications (MIC)** which is spending for the communication aspects of cybersecurity, including mobile networks, and the Strategic Information and Communications R&D Promotion Programme (SCOPE).
- Another source of funding is the **Ministry of Economy, Trade and Industry (METI),** which is mainly funding computing aspects of cybersecurity, including industrial control systems. Particularly there are two funding instruments:
    - **The New Energy and Industrial Technology Development Organization (NEDO**) and
    - **The Information-technology Promotion Agency (IPA).**
- **The Ministry of Education, Culture, Sports, Science and Technology (MEXT),** including the **Japan Society for the Promotion of Science (JSPS**), is primarily responsible for funding universities.
- Finally the **Cabinet Office (CAO)** is promoting inter-ministerial and intersectional R&D efforts, through the Cross-ministerial Strategic Innovation Promotion Program (SIP).

2) Main research areas and agendas

The main research directions in cybersecurity are defined in the Strategic research and Innovation agendas and the national cybersecurity strategies.

Strategies and Research and Innovation Agendas The European top-level strategic documents are consisted of:

- **Digital Single Market (DSM) Strategy**, mainly focusing on the introduction of a Common European Digital Market,
- **Cybersecurity strategy of the EU**, with five main priorities including: achievement of cyber resilience, drastic reduce of cybercrime, development of cyberdefence policy and capabilities related to the Common Security, and Defence Policy (CSDP), development of the industrial and technological resources for cybersecurity and finally establishment of a coherent international cyberspace policy for the European Union and promotion of core EU values.
  On 13 September 2017, the European Commission published the *Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*[1]*,* which sets three pillars in cybersecurity building EU resilience to cyber attacks, creating effective EU cyber deterrence and strengthening international cooperation on cybersecurity.
  Another interesting document in cybersecurity is *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry,*[2] which is perceived as an update of the Strategy.

The main goal of the Strategic Research and Innovation Agenda is to propose topics for calls of project proposals related to cybersecurity for the H2020 Work Programme 2018-2020. The main challenges of research and innovation are found in several ECSO documents, including the market fragmentation, the innovation led by imported ICT products, the need to mitigate cyber security dependencies from external sources and achieve strategic supply chain in the field, less funding to research and innovation available and often dispersed due to a lack of transnational approach European industrial policies not yet properly addressing specific cybersecurity issues, weak entrepreneurial culture and lack of venture capital and finally human factor and skills shortage.

[1] http://eur-lejuu.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450

[2] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52016DC0410

The main goals of the Research and Innovation Agenda are the protection of critical infrastructures and vertical sectors from cyber threats, the increment of the European digital autonomy, the allowance of security and trust of the whole supply chain, the investment in areas where Europe has a clear leadership or strategic needs, the leverage upon the potential of SMEs and finally the increment of competitiveness[3].

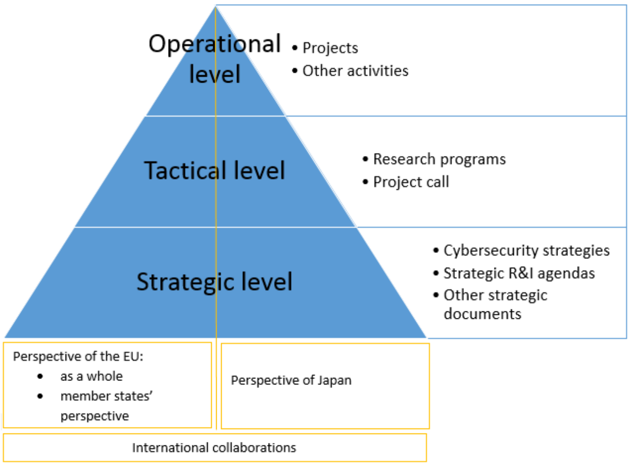

Figure 1 A schematic overview of the analysis

Overall strategy for the European cybersecurity market and industry The European cybersecurity market share is about 24%, which is less than the contribution of Europe to Global GDP (i.e. about 26%). Many activities should be performed to boost cybersecurity research. In order to implement the research and innovation strategy and to align technical with cooperation and coordination aspects, five major types of mechanisms/projects are recommended. These include Cyber Coordination (Coordination and Support Actions), Cyber Ecosystem, Cyber Pilots, Cyber Infrastructures and Technical projects. SRIA[4] defines the following seven main priorities:

- Ecosystem for Education, training, market growth and SME support
- Demonstrations for the society, economy, industry and vital services
- Collaborative intelligence to manage cyber threats and risks
- Remove trust barriers for data-driven applications and services
- Maintain a secure and trusted infrastructure in the long-term
- Intelligent approaches to eliminate security vulnerabilities in systems, services and applications
- Advanced Security Services[5]

The context of cybersecurity is also formed by several publications of the working groups of ECSO. ECSO WG5's Position Paper[6] describes the main gaps in European cyber education and professional training.

European project calls EU Research and Innovation Programme has dedicated 80 billion euros of fund over 7 years (2014 to 2020), through H2020, along with private investments. The main calls include the Information and Communication Technologies (ICT) , the Information and Communication Technologies, the Digitizing and transforming European industry and services: digital innovation hubs and platform, the Cybersecurity calls, the Joint Collaborations, the Innovation in SMEs (INNOSUP), the Secure Societies - Protecting Freedom And Security Of Europe And Its Citizens (DRS), as well as the individual national project calls.

3) The strong and weak points

Following the analysis of the questionnaires provided in our first workshop in Japan, along with observations and experience of all partners of the consortium, we provide an overview of strong and weak points for both regions.

[3] Strategic Research and Innovation Agenda, June 2017, https://www.ecsorg.eu/documents/publications/59e615c9dd8f1.pdf

[4] ibid3

[5] ibid3

[6] Position Paper, Gaps in European Cyber Education and Professional Training, WG5 – Education, training, awareness, cyber ranges, March 2018

Strengths There is a high level of awareness on both sides. There is a need to have reliable metrics in cyber hygiene, for the common base of discussion and mitigation. Therefore, strategic documents are very important. Although the use of IT has already progressed widely in various fields, the regulation and the government policy are still able to have a great effect on the activities of the private sector and the citizens. Because of that, promoting public-private cooperation in the use of IT, cybersecurity and privacy protection will be critical for wholesome economic growth. Where there is absolutely no need, services cannot be sold on the market. However, pursuing only needs, will not yield more advanced business markets, and making strategic documents even more relevant. Lately, research strategies require programs to involve companies interested in technologies, from the point of view of exploitation. Thanks to those companies, the industry needs to become input to research programs.

Weaknesses A very important problem is the ability and time needed to transfer the outcomes of research into technologies and products. The main obstacles include differences in focus between research and industry, as well as in needs, aims, and assumptions. Other obstacles are the law limitations in the regulations, the fragmented regulations across the different markets, the conflicts between theoretic model and reality, the limited resources, the different limitations and the time of adoption. Some of these obstacles are also confirmed by the SRIA document[7]. In order to reduce these obstacles, we indicate the following propositions:

- Industry involvement in research,
- Practical experience of the researchers,
- Good definition of mutual expectations between research and industry,
- Law harmonization, which can bring the effect of synergy, and because of that, research outcomes could be adopted and implemented more easily.

During the analysis, the lack of high-qualified personnel in the area of cybersecurity was highlighted. Specifically the working group focuses on the following issues[8]:

- Increase education and skills on cybersecurity products and safe use of IT tools in Member States for individual citizens and professionals,
- Develop cybersecurity training and exercise ecosystem leveraging upon cyber range environments,
- Support awareness-raising and basic hygiene skills

Also the analysis revealed the lack of coordination of research actions on various levels, as well as the lack of strong global cybersecurity enterprises and solutions originating in the EU and Japan.

Common interests between the EU and Japan During the first workshop, the EUNITY consortium gathered information from the attendees regarding several topics, including cyber threat intelligence, education, awareness and cyber range, education, awareness and cyber range, methods to enhance cybersecurity, security services, network security and cybersecurity in various domains (IoT, cloud, legal policies, social networks etc.)

The most important priorities of R&I are risk management and critical infrastructure protection, cybersecurity in various technologies, threat detection and threat intelligence, cryptology design, techniques and protocols network security, hardware and systems security and cybersecurity measures at the Tokyo Olympic Games in 2020.

The most important threats seem to be malware, APT, cyber terrorism, network threats, lack of integration/cooperation between CERTs, poor cyber literacy, cyber attacks for critical infrastructure, quantum cryptanalysis, specific threats against various technologies, data theft and social engineering. On the very important issue of collaborations between EU and Japan, the existing collaborations are:

- The Computer Security Incident Response Team in Japan (JPCERT/CC) has many bilateral MoUs with European national CSIRTs,

[7] European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private Partnership (cPPP), June 2016, http://ecs-org.eu/documents/ecs-cppp-sria.pdf

[8] https://www.ecs-org.eu/working-groups/wg5-education-awareness-training-cyber-ranges

- JPCERT/CC is a member of APCERT[9] ,
- Japan Institute for Promotion of Digital Economy and Community (JIPDEC) cooperates with ETSI (European Telecommunications Standards Institute)

The ICT areas that need collaboration between EU and Japan are NGN (Next Generation Network), IoT (Internet of Things) and cyber-physical systems, including drones, big data, HPC (High Performance Computing), AI (Artificial Intelligence) and ML (Machine Learning), computer science education, distributed OS, robotics, smart cities, NFV (Network Function Virtualization), VR/AR (Virtual/Augmented Reality), E-Health, interoperability between eID (government-issued digital certificate for citizen) in the perspective of EU and Japan (in regulation, policy and technical aspects). Specifically the areas in cybersecurity that need collaborations are education and awareness, standards and regulations and information sharing.

[9] https://www.apcert.org