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

The goal of this report is to give a quick glance at the picture of the cybersecurity and privacy in Europe and Japan, as it is more analytically shown in the respective deliverable 3.1 of EUNITY. This report is analyzing the cybersecurity priorities in both EU and Japan, in order to produce an overview on the status and priorities of cybersecurity and privacy research and innovation activities in Europe and Japan. The report elicits the legal and regulatory landscape, with special attention to the GDPR and focuses on the cybersecurity strategy of EU and NIS. Some of the issues that the deliverable describes include the finance mechanisms of research and innovation in cybersecurity, in both regions, and the current role and activity of different units (SMEs, research institutions, CSIRTs, LEAs, etc.) in research and innovation. We provide an overview of the main research directions in the field, we identify the strong and weak points in the both regions to indicate the topics of common interest, where there are opportunities for cooperation and the topics where some aspects are covered asymmetrically, allowing greater synergy. Also we analyze long-term research programs at the national and international level, in order to find thematic parallels between the EU and Japan, which may create opportunities for either co-financing of joint EU-Japan projects, or at least synchronization of efforts enabling cooperation.
The purpose of the analysis is only to indicate the most visible similarities and differences. Figure 1, below, shows the dataflow that produced deliverable D3.1.

Legal and Policy Aspects

The European Landscape The rise of modern technologies and new forms of human and digital interactions, has brought into light the weaknesses of the existing legislation, which turned to be perceived by many as fragmented[1] and outdated. This "obsolete" state of play was accompanied by the increasing number of cyber threats that European stakeholders are facing[2] in both public and private sectors: growing security and privacy risks have become a landmark blocker for the achievement of a competitive and secure digital single market. As a consequence was the formation of GDPR after many societal discussions[3] and political decisions as shown in Table 1 Summary of the data subject's rights as enriched by GDPR.

[1] Cuijpers, Colette and Koops, Bert-Jaap, How Fragmentation in European Law Undermines Consumer Protection: The Case of Location-Based Services (July 19, 2010). European Law Review, Vol. 33, pp. 880-897, 2008. Available at SSRN: https://ssrn.com/abstract=1645524

[2] Ehrenfeld, J. (2017). WannaCry, Cybersecurity and Health Information Technology: A Time to Act. Journal of Medical Systems, 41(7),1.

[3] Kuner, C. (2005). Privacy, Security and Transparency: Challenges for Data Protection Law in a New Europe. European Business Law Review, 16(1), 1-8.

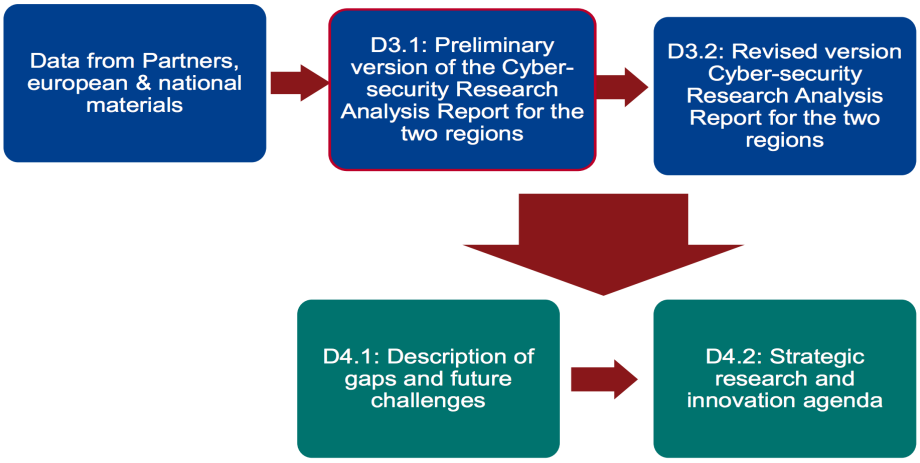

Figure 1Dataflow

The Japanese Landscape The first recognition of the right to privacy, in Japan, comes with the jurisprudence in the Utage no Ato case[4], where, based on an interpretation of the Civil Code, the Tokyo District Court stated that "*The right to privacy is recognized as the legal protection of the right so as not to be disclosed of private life*"[5]. The Act on Personal Information after its official announcement in 2003 came eventually into effect in 2005. The current privacy law got finalized in 2017 and as Harada states, "*One of the main objectives of the amended Act is to create a framework that recognizes and addresses the fact that transfers of personal data occur on a global scale*"[6]. The personal information is defined as information that is identifiable of the individuals by names, birthdate and the other descriptions including documents, drawings, electromagnetic records or voices, motions and other means. Personal identifiers are letters, numbers, marks and the other codes which fall in (i) characteristics of the part of body for the purpose of use of electronic machines, which is identifiable for the individual or (ii) the individual user or purchaser designated, written or recorded in the service use or the sales.
Similarly to what we describe as "*special categories of personal data*", it is explained how personal information which include race, religious beliefs, social statuses, medical records, criminal offences, events related to victims or criminal offences are indeed sensitive data which require special care in order to avoid the injurious discrimination, biases and potentially subsequent disadvantages. The Japanese law regarding anonymization provides a definition for anonymous data as personal information, which does not enable one to identify an individual.

Cybersecurity: Japan and the European Union: comparative aspects on privacy and data protection

List of initiatives:

- Set of Guidelines on Information Security Policies, (July 2000)
- Common Standards for Information Security Measures for Government Agencies (2005-2014)
- Policy Council (May 2014)
- Special Action Plan on Cyber-terrorism Countermeasures for Critical Infrastructures (2000)
- The Basic Policy (2014) and its revision by Strategic Headquarters (2015)
- Establishment of IT Security Office (2000)
- National Information Security Center & Information Security Policy Council created (2005).

Concerning the law, the Cybersecurity Strategic Headquarters mandates for the first time, reporting from government bodies, agencies and NIS. The Cybersecurity Strategy becomes a more accountable process. Cybersecurity is defined within the realm of the Japanese law as:

[4] Miyashita, H. (2011). The evolving concept of data privacy in Japanese law. International Data Privacy Law, 1(4), 229-238. http://dx.doi.org/10.1093/idpl/ipr019
[5]Judgment of Tokyo District Court, 28 September 1964, Hanrei-jiho vol. 385, p. 12
[6]M. Harada, Japan: Personal data protection. (2017). International Financial Law Review, Retrieved from https://search.proquest.com/docview/1872090298?accountid=17215

"consideration, maintenance and management of needed measures to prevent the leakage, destruction or damaging of information reported or transmitted or received by electronic way, magnetic way or other ways that human cannot recognize, or to manage safety control of that information, or to ensure safety and reliability of information systems or information and communication networks".

A basic difference between NIS and the Basic Act is that is sets the Citizen as an Active Stakeholder In the European NIS directive we notice that the goal is to coordinate efforts towards the security of European Information system, and not to mention the responsibilities that the citizens share towards this goal. However, in the Basic Act, the citizen remains an active participant in the level of awareness of cybersecurity, which actually mirrors the general claim by the expert community in cybersecurity, that this topic should be grasped in the societal level.

ART.	RIGHT	Brief description
12,13 and 14	Right to Information	In light of an improved transparency of data processing, data subjects have the right to request (free of charge) for what purposes and by whom exactly (third parties included) their data are processed.
15	Right to Access	The request may also pertain a copy of such data (see above) that must be provided electronically, in an easily readable format and without undue delay.
16	Right to Rectification	If personal data is inaccurate or incomplete, the data subject has the right to ask for them to be rectified.
17	Right to Erasure (Right to "be forgotten")	Data subjects have the right (under qualified circumstances) for their data to be erased from the controllers' dataset.[7]
18	Right to Restriction of Processing	Controllers are bound by the right of the data subject to ask for their personal information to be suspended from the processing.
20	Right to Data Portability	Data subjects have the right for their data to be transferred from one controller to another (or directly to the data subjects themselves) in an automatic and easily readable format.
21	Right to Object	Right to contest the processing of personal data by controllers.
22	Right not to be Subject to Automated Decisions	Data subjects have the right not to be subject to decisions based on solely automated means (including profiling), which leads to legal effects for the individuals.

Table 1 Summary of the data subject's rights as enriched by GDPR

Regarding information sharing and incident reporting the Japanese government has shown the willingness to deal with cybersecurity incidents in large events, proactively. Regarding the Olympic games in 2020, the senior official addressed in Japan Times[8], regarding cybersecurity cooperation: "*Ahead of the 2020 Olympic Games in Tokyo, the government sees cooperation as necessary to better prepare for growing cybersecurity threats, recover from such damage and probe the causes.*" Regarding information sharing, the Basic act does not provide any coherent provisions. Japan has signed a number of agreements on information sharing in regard to cybersecurity threat intelligence:

1. Japan-UK Joint declaration on Security cooperation, Tokyo 2017
2. Japan – India Cyber Dialogues, which lasts since 2012 and is at its Second Edition (2017)[9]
3. The Japan- ASEAN cybersecurity dialogues, which are rolled out in a number of different policy initiatives since 2009[10]
4. Japan's first access to the US's DHS's Automated Indicator Sharing (AIS)[11]

[7] C-131/12 - Google Spain and Google: Judgment of the Court (Grand Chamber), 13 May 2014 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González - Request for a preliminary ruling from the Audiencia Nacional

[8] The Japan Times, 48 infrastructure entities to get cybersecurity cooperation requests, 2015

[9] Joint Press Release Second Japan-India Cyber Dialogue, New Delhi, 2017

[10] 1Mihoko Matsubara, Japan's Cybersecurity Capacity-Building Support for ASEAN – Shifting From What to Do to How to Do It, PaloAlto Networks, 26.07.2017

[11] Morgan Chalfant, US, Japan deepen cyber information