BUSINESS PLAN

CEN/CENELEC JTC 13
Cybersecurity and data protection

EXECUTIVE SUMMARY

Cybersecurity and data protection are rapidly growing and changing technical and application domains. The threats and requirements are increasing dramatically with the progress of digitalization and the rising number of critical assets digitalized and accessible online. Therefore protection is expected from citizens but also industry and even government.

CEN/CENELEC JTC13 intends to

- Become the European standardisation focal point for Cybersecurity and Data protection
- Be recognized at European and International level as a provider of best in class standards (EN, TS, TR)
- Be identified as a strategic partner of,

    1. The European commission (DG CONNECT, GROW, HOME etc.) and the European Parliament – ITRE/ LIBE/ IMCO;
    2. Institutions, Agencies and bodies within the EU system, being involved in the Cybersecurity & Privacy policy and law making, such as ENISA, BEREC, Council – Horizontal party on cyber issues, NIS Cooperation Group, EEAS/INTCEN, EDPS/EDPB, EDA, Europol/EC3
    3. Other European bodies/entities/consortia, public private partnerships or private, such as ECSO, the Cybersecurity Competence Centre/Network, ANEC/BEUC, EDRi, Digital Europe, Eurosmart, EU funded projects/initiatives (H2020. CEF etc.);
    4. EU MSs' National administrations and bodies/entities involved in the Cybersecurity & Privacy policy and law making, such as National Cybersecurity Authorities, DPAs etc.

And therefore adopt a strategy consistent with these objectives. It will also cooperate with all the partners in standardisation field both from international (ISO, IEC, ITU) and European (ETSI) point of view, as well as other National Standardization bodies relevant to JTC13 SCOPE, on international level (e.g. NIST, JISC, SAC etc.).

It will act in order to avoid duplication of efforts and inconsistency between standards.

1 BUSINESS ENVIRONMENT OF THE CEN/CENELEC/JTC 13

1.1 Description of the Business Environment

The following political, economic, technical, regulatory, legal, societal and/or international dynamics describe the business environment of the industry sector, products, materials, disciplines or practices related to the scope of this CEN/CENELEC /JTC, and they may significantly influence the content of the resulting standards and how the relevant standards development processes are conducted:

Cybersecurity is becoming a strategic issue both due to societal demand from citizens but also from governments and businesses to preserve their sovereignty. Due to the general digitalization of the world cybersecurity is becoming a must for all parts of the community and the industry. At the same time the relation between cybersecurity and privacy is non-trivial, as depending on the technology and the application scenario both can support each other but also sometimes compete.

Some domains are in exponential growth: for example, IoT (Internet of Things) is claiming to reach 40 billion of devices deployed in the world in 2023. The cyber risk for this equipment is huge. For these markets the cost of cybersecurity must be affordable and consistent with user needs. The

Cybersecurity must cover all the domains: products, solutions, services, processes, people and organization. The need is huge!

Europe is at the leading edge in technology to support cybersecurity and data protection, thanks to the European legislators' regulation work: eIDAS, GDPR, NIS, Cyber Act, e-privacy regulation (in the works), EECC and a number of vertical sectors' legislations.

The EU Cybersecurity Act (CSA), which entered into force in June 2019, intends to establish a European cybersecurity certification framework for ICT products, services and processes. ENISA is participating in this new framework by preparing candidate certification schemes on the request from the European Commission or the European Cybersecurity Coordination Group (representation of Member States).

Standardisation will play an important role in the framework, as the CSA states the following:

- There is a need for closer international cooperation to improve cybersecurity standards, including the need for definitions of common norms of behaviour, the adoption of codes of conduct, the use of international standards, and information sharing, promoting swifter international collaboration in response to network and information security issues and promoting a common global approach to such issues.
- The European cybersecurity certification schemes should be non-discriminatory and based on European or international standards, unless those standards are ineffective or inappropriate to fulfil the Union's legitimate objectives in that regard.
- The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto
- A European cybersecurity certification scheme shall include at least the following elements:
  - References to international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements.
  - To support EU regulations standardisation is necessary in order to guarantee interoperability harmonisation of cybersecurity functions.

Many bodies are developing standards relevant to cybersecurity, for example ISO/IEC JTC 1/SC 27 which intends to cover the complete scope of IT security (ISMS (Information security management systems), cryptography, security evaluation, specific technical controls, privacy, identity management, biometrics). ISO/IEC JTC 1/SC 27 is developing horizontal standards but some other vertical domains are also developing cybersecurity standards, for example ISO TC 22/WG 11 in automotive sectors. This must be carefully managed in order to limit the vertical domains to the very minimum necessary.

2 BENEFITS EXPECTED FROM THE WORK OF THE CEN/CENELEC/JTC 13

Standardisation bodies have different scopes and governance. We can identify:

- **International level SDOs**: ISO, IEC, ITU, under UN governance are recognized by the standardisation community as international standard organisation (SDO). These organisations are potentially addressing all domains. The members are registered national bodies (NB) and the principle chosen is one member one vote. That is to say that each state has the same weight in vote whatever the size of the country could be. These SDO are mostly working on a consensus basis, voting is an exceptional case. The Published standards are generally not free.
- **European level**: In Europe there are three recognized by the EU standardization bodies: CEN, CENELEC, and ETSI. These ESOs (European standardization organizations) are partly funded by European Union.
  - CEN and CENELEC function similarly to ISO and IEC, the membership is also assured through national bodies. CEN and CENELEC have a more and more integrated functioning through the CCMC (CEN CENELEC Management Centre). The published standards are generally not free.
  - ETSI has a different governance organization from CEN and CENELEC. Membership is assured via individual registration by companies and other bodies from EU Member States and also globally. The membership fee is paid on a voluntary basis on top of a minimal cost and the number of votes is proportional to the annual fee cost. There are regulations and governance mechanisms to avoid a majority shared by only a few members. There is also a national representation for the European matters (like European standards ballots).
  - One important point is that ETSI standards and all technical reports and technical specifications are available **free of charge.** This eases acceptance of the standards worldwide.
  - In order to authorize exchange and transfer of standards between International and European SDO's, mechanisms of transposition have been put in place (the Dresden, Frankfurt and Vienna agreements), authorizing to transpose standards from one standardisation body to another without restarting all work from scratch. It is possible, for example, to transpose an IS (International standard) to an EN (European standard) to be referred in European regulations, or to transpose an EN to an IS in order to make it applicable worldwide.
  - The Vienna Agreement, signed in 1991, was drawn up with the aim of preventing duplication of efforts and reducing time when preparing standards. As a result, new standards projects are jointly planned between CEN and ISO. Wherever appropriate, priority is

given to the cooperation with ISO, provided that international standards meet European legislative and market requirements, and that non-European global players also implement these standards.

- CENELEC enjoys close cooperation with its international counterpart, the International Electrotechnical Commission (IEC). In order to facilitate a consensus-finding process between European and international standards development activities in the electrical sector, CENELEC and IEC formalized the framework of their cooperation through the signature in 1996 of an 'agreement on common planning of new work and parallel voting', known as the Dresden Agreement.
- After 20 years of a fruitful partnership this has resulted in a very high level of technical alignment (close to 80% of CENELEC standards are identical to or based on IEC publications). CENELEC and IEC have reconfirmed their longstanding cooperation on 17 October 2016, by signing the Frankfurt Agreement. Building on the experience of both partners, this new agreement preserves the spirit and approach conveyed by the Dresden Agreement, in particular the strategic commitment of CENELEC to support the primacy of international standardization. It includes several updates aiming at simplifying the parallel voting processes and increasing the traceability of international standards adopted in Europe thanks to a new referencing system.

- **Ad hoc standardisation bodies:** In addition to the official international or European standardization bodies, there are other entities/consortia working in specific and focused domains, for example industrial fora like 3GPP, CSA, Fido Alliance, Global platform, GSMA, IEEE, IETF, AIOTI, one M2M, TCG, OASIS etc.
  - These industrial bodies have different functioning depending on their scope, participation and coverage, but they intend to cover specific requirements from industry and claim to be more efficient than traditional SDO. Nevertheless, they don’t have the official recognition international SDOs have. These SDOs, however, have defined specific procedures to import perceived de facto standards from these organisations, like PAS (publicly available specifications), or so-called fast track mechanisms. This approach proved to be very useful, as a good example we can note ISO/IEC 27000, which was created as BS 7799 and transposed later after a first unsuccessful try to ISO/IEC standard using a fast track procedure.
  - We can note also that national standardisation bodies are producing high value standards, like for example the US NIST – National Institute of Standards and Technology. One of NIST standards, the FIPS 140-2, has been taken as a basis to develop ISO/IEC 19790 – Cryptographic module evaluation. This ISO/IEC standard became afterward the reference for the rev 3 of FIPS 140.

- **Overlaps in standards**: Cybersecurity standardisation activities take place in international, national, and industry-based forums. Within Europe the three European Standards Organizations, CEN, CENELEC, and ETSI cooperate to try to minimize the amount of duplication of standards. Many groups have liaisons and cooperation agreements within each other. Unfortunately, a common understanding between these groups has often proved to be difficult.
- There are many examples of duplication of work between standards organizations. Without mentioning concrete examples, we can state that it can lead to at least duplication of efforts, and in the worst case in the inconsistent sets of standards, which is harmful for industry, as potential users of the standard. In addition, the relation of cybersecurity groups with other security domains (societal security, physical security etc.) is not sufficiently addressed.
- We can note the recent creation (2019) within CEN and CENELEC of a Security sectorial forum in order to address this gap. This forum has identified 14 primarily relevant standardisation bodies for security within CEN and CENELEC, for which improved collaboration is necessary and not limited to:
    - CEN/CLC/JTC 4 Services for fire safety and security systems
    - CEN/CLC/JTC 8 Privacy management in products and services now included as JTC13/WG5
    - **CEN/CLC/JTC 13 Cyber security and data protection**
    - CEN/TC 72 Fire detection and fire alarm systems
    - CLC/TC 79 Alarm systems
    - CEN/TC 79 Respiratory protective devices
    - CEN/TC 162 Protective clothing including hand and arm protection and lifejackets
    - CEN/TC 164 Water Supply
    - CEN/TC 192 Fire and rescue service equipment
    - CEN/TC 234 Gas Infrastructure
    - CEN/TC 263 Secure storage of cash, valuables and data media
    - CEN/TC 325 Crime prevention through building, facility and area design
    - CEN/TC 391 Societal and citizen security
    - CEN/TC 439 Private security services

3 PARTICIPATION TO THE CEN/CENELEC/JTC 13

All the CEN national members are entitled to nominate delegates to CEN Technical Committees and experts to Working Groups, ensuring a balance of all interested parties. Participation as observers of recognized European or international organizations is also possible under certain conditions. To participate in the activities of this CEN/TC, please contact the national standards organization in your country.

4 OBJECTIVES OF THE CEN/CENELEC/JTC AND STRATEGIES FOR THEIR ACHIEVEMENT

4.1 Defined objectives of the CEN/CENELEC/JTC 13

- Provide support to EU regulations (eIDAS, GDPR, NIS, Cyber Act, e-privacy, ….) and a number of vertical legislations should the European Commission submits a request
- Interface to ISO/IEC via Vienna and Dresden agreement
- Partnership with international and national standardisation organizations and industrial fora. Cooperate with all the partners in standardisation field both from international (ISO, IEC, ITU) and European (ETSI) point of view, as well as other National Standardization bodies relevant to our work, on international level (e.g. NIST, JISC, SAC etc.).
- Provide horizontal standards for vertical applications domains (transport, healthcare, smart cities, automotive, IOT, …) :
    - Information security management systems
    - Cryptography
    - Security evaluation and certification
    - Privacy
- Contribution to ICT rolling plan, EU standardisation strategy, EU rolling working plan (RWP) of the Cybersecurity Act.
- Develop standards in accordance with the Cybersecurity Act provisions, recital 54 (international cooperation) and recitals 49 and 66 (interoperable solutions) and in particular liaise with SCCG (Stakeholders Cybersecurity Coordination group) through CEN BT and CENELEC BT representative. WG1 (chairman advisory group) will act as mirror committee of SCCG for JTC13.
- Be identified as a strategic partner for,

    1. The European commission (DG CONNECT, GROW, HOME etc.) and the European Parliament – ITRE/ LIBE/ IMCO;
    2. Institutions, Agencies and bodies within the EU system, being involved in the Cybersecurity & Privacy policy and law making, such as ENISA, BEREC, Council – Horizontal party on cyber issues, European Parliament – ITRE/ IMCO, NIS Cooperation Group, EEAS/INTCEN, EDPS/EDPB, EDA, Europol/EC3
    3. Other European bodies/entities/consortia, public private partnerships or private, such as ECSO, the Cybersecurity Competence Centre/Network, ANEC/BEUC, EDRi, Digital Europe, Eurosmart, EU funded projects/initiatives (H2020. CEF etc.);
    4. EU MSs' National administrations and bodies/entities involved in the Cybersecurity & Privacy policy and law making, such as National Cybersecurity Authorities, DPAs etc.

4.2 Identified strategies to achieve the CEN/CENELEC/JTC 13 defined objectives.

- Set up an efficient organisational structure: 6 dedicated Working groups, plenary meetings, 3 sessions per year
- Manage active liaison with all relevant bodies : ISO/IEC, ETSI TC Cyber, CEN CENELEC security sector forum, sectorial TCs, …
- Interface with ECSO (WG1, WG6) and Horizon Europe projects
- Liaise and collaborate directly with the wide spectrum of stakeholders in the Cybersecurity public policy ecosystem, as identified above by communicating its intention (coordinated by the strategy committee?
- Involve the best European experts
- Organisation of annual event with the support of CCMC, ENISA
- Participation to Conferences at European and international level
- Implement a communication strategy, with the support of CCMC, to promote our activities and reach stakeholders as widely as possible, including the public.
- Build and formalize effective liaisons with International SDOs and non-European National SDOs with a pioneering activity and politico-economic significance for Europe (e.g. NIST, JISC, SAC etc.)

4.3 Environmental aspects

This is not relevant for JTC13

5 FACTORS AFFECTING COMPLETION AND IMPLEMENTATION OF THE CEN/CENELEC/JTC13 WORK PROGRAMME

To achieve the objectives of the CEN/CENELEC/JTC 13 it is necessary to,

- Engage all the parties in the work and in particular experts with long lasting expertise

- Work in an open-minded spirit of collaboration in order to take the best of all initiatives. The Cybersecurity and data protection is more than necessary, it is vital.

- Adopt a bottom up approach. Leverage relations on a National level, to establish an effective communication and synergies, as to promote the work of the TC and be identified an important catalyst and incubator of effective solutions and innovation in the cybersecurity terrain.