EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR INTERNAL MARKET, INDUSTRY, ENTREPRENEURSHIP AND SMES
Single Market Policy, Regulation and Implementation
**Standards for Growth**

# Meeting of the EU27 Member States on cybersecurity and standardisation (Brussels, 25 June 2019)

# Minutes

## 1. WELCOME AND OPENING OF THE MEETING

The Commission opened the meeting by recalling the context and its scope. The meeting was organised bearing in mind the rules that currently apply to the debates on sensitive topics to go beyond the 31 October 2019.

The use of network and information systems by citizens, organisations and businesses across the Union is now pervasive, and digitisation and connectivity are becoming core features in an ever-growing number of products and services. However, increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats. In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and would foster mutually reinforcing objectives.

The scope of the meeting was twofold:

- to provide a comprehensive overview of recent policy and regulatory developments in relation to 5G and cybersecurity;
- to exchange views with the MS on standardisation needs and priorities to be taken into account in medium/long term policy development bearing in mind such developments.

The event was intended not to overlap with debates within other committees or groups, thus its focus was solely on standardisation-related aspects.

## 2. ADOPTION OF THE AGENDA OF THE MEETING

The agenda was unanimously adopted.

## 3. SETTING THE SCENE

### 3.1. Joint Communication "EU-China – A strategic outlook" and follow-up actions

The Commission outlined the main features of the Joint Communication, which assesses the multiple dimensions of EU-China relationship, and sets out 10 high-level actions in selected fields. A specific action (Action 9) calls to a common EU approach to the security of 5G networks in order to safeguard against potential serious security implications for critical digital infrastructure. The implementation of the action requires *inter alia* issuing a Commission Recommendation on cybersecurity of 5G networks [item 3.2 of the agenda], and the organisation of an exchange of view with the Member States on the standardisation implications of 5G network security. This meeting was organised in response to the latter.

### 3.2. Commission Recommendation "Cybersecurity of 5G networks" and the Cybersecurity Act

The Commission provided an overview of the main elements of the Commission Recommendation of 26 March 2019. Two strands of action are set in it, one at national level (risk assessment of the 5G network infrastructure, by 30 June 2019) and one at Union level (joint review of the Union-wide exposure to risks related to infrastructures underpinning the digital ecosystem, in particular 5G networks, by 1 October 2019 + toolbox of risk management measures, by 31 December 2019). The NIS Cooperation Group includes a specific work stream on 5G, and is in charge of the implementation of the Recommendation.

The Cybersecurity Act [Regulation (EU) 2019/881 of 17 April 2019] enters into force on 27 June 2019. It introduces, for the first time, EU wide rules for cybersecurity certification of products, processes and services. Moreover, it sets a new permanent mandate for the EU Agency for Cybersecurity (ENISA), as well as more resources allocated to the Agency to enable to fulfil its goals. The Stakeholder Cybersecurity Certification Group (SCCG) and the European Cybersecurity Certification Group (ECCG) are established as well.

### 3.3. State of play of cybersecurity certification according to the new regulatory measures

The Commission recalled that the Cybersecurity Act (Article 47) requires the Commission (with the assistance of SCCG) to publish a Union rolling work programme for European cybersecurity certification that shall identify strategic priorities for future European cybersecurity certification schemes. However, since the Rolling Work Programme has not been set up yet, proposals can be made earlier by the Commission or the Member States. The Committee on Standards may have views on relevant standards and technical specifications to be taken into account. The process may prove difficult due to the complexity of the matters to be addressed (e.g. software certification).

## 4. 5G NETWORKS IN EUROPE

### 4.1. Overview

The Commission recalled that the state of play of 5G in the EU countries can be found in the 5G Observatory Quarterly Report that has been published recently. The simultaneous launch of the service in the Member States is planned for 31 December 2020, while the coverage of major cities is expected by 2025. At a global level, USA and Korea have already launched the service. In Europe, Finland, Spain and Switzerland have set up 5G networks, however various actions are ongoing in other European countries. Outstanding issues concern the allocation of spectrum in the 3,5 GHz band (only 21,4% is assigned), and the development of standards that guarantee the low latency time (i.e. fast response) the is required by equipment/devices. Their development is still at an early stage, and will depend from the needs of the vertical sectors.

### 4.2. Exchange of views on the implementation in the Member States

There was no significant debate, only few questions for clarification were raised by the participants.

## 5. CURRENT CHALLENGES FOR CYBERSECURITY STANDARDISATION, INCLUDING 5G NETWORKS, AND SUITABLE POLICY INITIATIVES AT EU LEVEL

### 5.1. Cybersecurity standardisation in the 2019 Rolling Plan for ICT standardisation

The Commission provided an overview of the Rolling Plan for ICT standardisation, and on the specific actions on cybersecurity that are mentioned in the 2019 edition:

1) Developing standards for critical infrastructure protection

2) Assessing the standards required to support the European Cyber-security Certification Framework to ensure that standards are available for the core of any certification activity

3) Investigating the issue of malware on personal computers

4) Investigating options for collaboration to defeat and remedy attacks

5) Investigating requirements for secure protocols for networks of highly constrained devices and heavily constrained protocol interaction

6) Investigating the availability of standards as regards to the security and incident notification requirements (as defined in NIS Directive)

7) Developing a “guided” version of ISO/IEC 270xx series specifically addressed to SMEs

### 5.2. State of play of Huawei participation in European initiatives

While the debate about the security implications of China’s growing digital influence is grabbing headlines around the world, the question of China’s involvement in standardisation, particularly European standardisation, also deserves attention. China's stance towards international standards has changed from one of active adoption to one of active shaping, largely centred on developing Chinese standards and promoting them abroad. Chinese companies are also increasingly active in international standard-setting bodies such as ITU, ISO and IEC (particularly on 5G standards).

The Commission provided an overview of the Huawei involvement in standardisation activities at the global and European level, in H2020 projects and JRC activities. The subsequent debate confirmed that Huawei is ubiquitous and a very active player at the global and European levels.

### 5.3. Exchange of views

The debate gave the opportunity to the participants to discuss the forthcoming cybersecurity certification process, the referencing of cybersecurity/5G standardisation in the risk assessments that are being prepared by the Member States, the reciprocity of the Chinese system, and a possible measure in support of education in cybersecurity standardisation.

At the conclusion of the meeting the Commission thanked the participants for their contributions, and informed them that a further meeting is not planned yet since its organisation will depend from the results of the risk assessments.