Council of the
European Union

Brussels, 6 March 2018
(OR. en)

6827/18

Interinstitutional File:
2017/0225 (COD)

COPEN 57
COPS 61
COSI 44
CYBER 42
IND 68
JAI 195
JAIEX 18
POLMIL 20
RELEX 195
TELECOM 58
CSC 69
CSCI 32
CODEC 328

COVER NOTE

From:	European Economic and Social Committee
To:	Delegations
Subject:	Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification - Opinion

Delegations will find below the Opinion of the European Economic and Social Committee on the abovementioned subject.

European Economic and Social Committee

TEN/646
Cybersecurity Act

OPINION

European Economic and Social Committee

Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')
[COM(2017) 477 final/2 2017/0225 (COD)]

Rapporteur: **Alberto MAZZOLA**
Co-rapporteur: **Antonio LONGO**

Consultation	European Parliament, 23/10/2017 Council of the European Union, 25/10/2017
Legal basis	Article 114 of the Treaty on the Functioning of the European Union
Section responsible	Section for Transport, Energy, Infrastructure and the Information Society
Adopted in section	05/02/2018
Adopted at plenary	14/02/2018
Plenary session No	532
Outcome of vote (for/against/abstentions)	206/1/2

1. Conclusions and recommendations

1.1 The EESC considers that ENISA's new permanent mandate as proposed by the Commission will significantly contribute to enhancing the resilience of European systems. However, the accompanying provisional budget and resources allocated to ENISA will not be sufficient for the agency to fulfil its mandate.

1.2 The EESC recommends to all Member States to establish a clear and equivalent counterpart to ENISA, as most of them have not done it yet.

1.3 The EESC also feels that, in terms of capacity building, ENISA should prioritise actions to support e-government[1]. EU/worldwide digital identity for persons, organisations and objects is key, and preventing and combating ID theft and online fraud should be a priority.

1.4 The EESC recommends that ENISA should provide regular reports on the cyber-readiness of Member States, primarily focusing on sectors identified in Annex II to the NIS Directive. A yearly European cyber exercise should assess the readiness of Member States and the effectiveness of the European cyber crisis response mechanism, and should produce recommendations.

1.5 The EESC supports the proposal to create a cybersecurity competence network. This network would be sustained by a Cybersecurity Research and Competence Centre (CRCC). This network could support European digital sovereignty by developing a competitive European industrial base for key technology capabilities based on the work done by the contractual Public-Private Partnership (cPPP), which should evolve into a Tripartite Joint Undertaking.

1.6 The human factor constitutes one of the most important causes of cyber accidents. For the EESC there is a need to build a strong cyber skills base and improve cyber hygiene also through awareness campaigns among individuals and businesses. The EESC supports the creation of an EU-certified curriculum for high schools and professionals.

1.7 The EESC believes that a European Digital Single Market also needs a homogeneous interpretation of the rules for Cybersecurity, including mutual recognition between Member States, and that a certification framework and certification schemes for the different sectors could provide a common baseline. However, different approaches must be provided for different sectors due to the way they function. Therefore the EESC believes that sectoral EU Agencies (EASA, ERA, EMA, etc.) should be involved in the process and in some cases, with the agreement of ENISA to guarantee coherence, delegated to draw up cybersecurity schemes. Minimum European standards for IT security should be adopted in cooperation with CEN/CENELEC/ETSI.

1.8 The envisaged European Cybersecurity Certification Group supported by ENISA should be made up of national certification supervisory bodies, private sector stakeholders, including operators from various applications, and scientific and civil society actors.

[1] Digital Single Market/Mid-term review.

1.9 The EESC takes the view that the agency should monitor the performance and decision-making of national certification supervisory authorities through audits and inspections, on behalf of the Commission and that responsibilities and sanctions for non-respect of standards should be defined in the Regulation.

1.10 The EESC believes that certification activities cannot exclude a proper labelling system, to be applied also to imported products to reinforce consumers trust.

1.11 Europe should scale up investments converging different EU funds, national funds and private-sector investments towards strategic objectives in strong public-private cooperation, also through the creation of an EU Cybersecurity Fund for Innovation and R&D in the current and future Research Framework Programme. Furthermore, Europe should create a fund for deployment for the Cybersecurity, opening a new window in the current and future Connecting Europe Facility as well in the next EFSI 3.0.

1.12 The EESC believes a minimum security level is necessary for "ordinary" "Internet of People" (IoP) devices. In this case, certification is a key method of providing a higher level of security. Internet of Things (IoT) security should be a priority.

2. Cybersecurity present framework

2.1 Cybersecurity is critical to both prosperity and national security, as well as to the very functioning of our democracies, freedoms and values. "Cybersecurity is an ecosystem where laws, organisations, skills, cooperation and technical implementation need to be in harmony to be most effective", states the UN's Global Cybersecurity Index, adding that cybersecurity is "becoming more and more relevant in the minds of countries' decision makers".

2.2 The need for a secure ecosystem is becoming crucial due to the Internet revolution. This revolution has not only redefined business-to-consumer (B2C) industries such as media, retail and financial services; it is also reshaping manufacturing, energy, agriculture, transport and other industrial sectors of the economy that, together, account for nearly two-thirds of the global gross domestic product, as well as utilities' infrastructure and people's interactions with public administration.

2.3 The Digital Single Market Strategy is built around improving access to goods, services and content, creating the appropriate legal framework for digital networks and services, and reaping the benefits of a data-based economy. It has been estimated that the strategy could contribute EUR 415 billion per year to the EU economy. The cybersecurity skills gap for professionals working in the private sector in Europe is predicted to be 350 000 by 2022[2].

2.4 A 2014 study estimated that the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around EUR 55 billion) in 2013[3].

[2] OJ JOIN/2017/0450 final.

[3] Commission Staff Working Document – Impact Assessment, accompanying the Proposal for a Regulation of the European Parliament and of the Council, Part 1/6, p. 21, Brussels, 13/9/17.

2.5 According to Special Eurobarometer 464a on "Europeans' attitudes towards cyber security", 73% of Internet users are concerned that their online personal information might not be kept secure by websites and 65% that it might not be kept secure by public authorities. Most respondents are concerned about being the victims of various forms of cybercrime, and especially about malicious software on their devices (69%), identity theft (69%) and bank card and online banking fraud (66%)[4].

2.6 So far, no legal framework has been able to cope with the pace of digital innovation, and a number of legal texts are contributing item by item to establishing an appropriate framework: the revision of the Telecoms Code, the General Data Protection Regulation (GDPR), the Directive on network and information systems security (NIS Directive), the Regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS Regulation), the EU-US Privacy Shield, the Directive on non-cash payment frauds, and so on.

2.7 There are many different organisations further to ENISA, the "EU Cybersecurity Agency", dealing with cybersecurity issues: Europol; Cert-EU (Computer Emergency Response Team of the European Union); the EU Intelligence and Situation Centre (EU INTCEN); European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA); Information Sharing and Analysis Centres (ISACs); the European Cyber Security Organisation (ECSO); the European Defence Agency (EDA); the NATO Cooperative Cyber Defence Centre of Excellence; and the UN GGE (United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security).

2.8 Security by design is key to providing high quality goods and services: smart devices are not that smart if they are not secured, and the same is true of smart cars, smart cities and smart hospitals – they all require built-in security for devices, systems, architectures and services.

2.9 On 19-20 October 2017, the European Council asked for the adoption of a common approach to EU cybersecurity following the proposed reform package, calling for "a common approach to cybersecurity: the digital world requires trust, and trust can only be achieved if we ensure more proactive security by design in all digital policies, provide adequate security certification of products and services, and increase our capacity to prevent, deter, detect and respond to cyberattacks"[5].

2.10 In its resolution of 17 May 2017, the European Parliament "emphasises the need for end-to-end security across the whole financial services value chain; points to the large and diverse risks posed by cyberattacks, targeting our financial markets infrastructure, the Internet of Things, currencies and data; […] calls on the ESAs to regularly review existing operational standards covering ICT risks of financial institutions; calls furthermore for ESA guidelines on the supervision of Members States' cyber risks; stresses the importance of technological know-how in the ESAs"[6].

[4] Special Eurobarometer 464a – Wave EB87.4 – Europeans' attitudes towards cyber security, September 2017.

[5] European Council Conclusions of 19 October 2017.

[6] EP Resolution 17.05.2017 - A8-0176/2017.

2.11 The EESC has had several previous opportunities to tackle the issue[7], including, during the Tallinn Summit, the conference on the Future development of e-Government[8], and has set up a permanent study group on the Digital Agenda

3. The Commission proposals

3.1 The Cybersecurity Package includes a joint communication reviewing the previous European cybersecurity strategy (2013), as well as a Cybersecurity Act focusing on ENISA's new mandate and a proposed certification framework.

3.2 The strategy is structured around three main sections: resilience, deterrence and international cooperation. The deterrence part focuses mainly on cybercrime issues, including the Budapest Convention, and the international cooperation part looks at cyber defence, cyber diplomacy and cooperation with NATO.

3.3 The proposal sets out new initiatives such as:

- building a stronger EU cybersecurity agency;
- introducing an EU-wide cybersecurity certification scheme;
- swiftly implementing the NIS Directive.

3.4 The resilience part proposes cybersecurity-related actions addressing in particular: market issues, the NIS Directive, rapid emergency response, the development of EU competence, education, training – in cyber skills and cyber hygiene – and awareness).

3.5 In parallel, the Cybersecurity Act proposes the creation of an EU cybersecurity certification framework for ICT products and services.

3.6 The Cybersecurity Act also proposes an enhanced role for ENISA as the EU agency for cybersecurity, granting the agency a permanent mandate. On top of its current responsibilities, ENISA is expected to cover new supporting and coordination tasks related to support for the implementation of the NIS Directive, the EU Cybersecurity Strategy, Blueprint, capacity building, knowledge and information, awareness raising, market-related tasks such as support for standardisation and certification, research and innovation, pan-European cybersecurity exercises, and the secretariat of the Computer Security Incident Response Team (CSIRT) Network.

[7] Digital Single Market/Mid-term review.OJ C 75, 10.3.2017, p. 124, OJ C 246, 28.7.2017, p. 8, OJ C 345, 13.10.2017, p. 52, OJ C 288, 31.8.2017, p. 62, OJ C 271, 19.9.2013, p. 133.

[8] EESC Press Release N° 31/2017 Civil Society debates E-government and cybersecurity with incoming Estonian Presidency: http://api.eesc.europa.eu/documents/eesc-2017-03031-00-00-cp-tra-en.docx.

4. General observations – Overview

4.1 Context: Resilience

4.1.1 Single Cybersecurity Market

Duty of care: The development of the proposed principle of "duty of care" mentioned in the Joint Communication for the use of secure development lifecycle processes is an interesting concept to be developed with EU industry, which could lead to a comprehensive approach for EU legal compliance. Security by default should be considered for future evolution.

Liability: Certification will help to make it easier to attribute liability in the event of a dispute.

4.1.2 NIS Directive: energy, transport, banking/finance, health, water, digital infrastructure, e-commerce.

For the EESC, the full and efficient implementation of the NIS Directive is essential in order to ensure the resilience of national critical sectors.

The EESC believes that information sharing between public and private actors should be strengthened through sectoral Information Sharing and Analysis Centres (ISACs). An appropriate mechanism to securely share trusted information within an ISAC and between CSIRTs and ISACs should be developed, based on an evaluation/analysis of the mechanism currently in use.

4.1.3 Rapid Emergency Response

The "Blueprint" approach would provide an effective process for an operational response at EU and Member-State level to a large-scale incident. The Committee underlines the need to involve the private sector; operators of essential services in the operational response mechanism should also be taken into consideration, as they could provide valuable information on threats and/or support in detection of and response to threats and large-scale crises.

The Joint Communication proposes mainstreaming cyber incidents into the EU's crisis management mechanisms. While the EESC understands the need for a collective response and solidarity in the event of an attack, a better understanding is needed of how this could be applied as cyber threats usually propagate across countries. Tools used in national emergencies could be only partially shared in the case of a local need.

4.1.4 Developing EU Competence

For the EU to be truly competitive on the global stage and to build a solid technological base, it is essential to create a coherent, long-term framework encompassing all the stages of the cybersecurity value chain. In this respect, fostering cooperation between European regional ecosystems is key to developing a European cybersecurity value chain. The EESC welcomes the proposal to create a cybersecurity competence network.

This network could support European digital sovereignty by developing a competitive European industrial base and reducing dependency on know-how developed outside the EU for key technology capabilities, provide technical exercises, workshops and even essential cyber hygiene training for professionals and non-professionals, and also – based on the work done by the cPPP – foster the development of a network of national public-private organisations to support the development of a market in Europe. "Advancing cPPP should lead to its optimisation, adaptation or expansion" (EE-BG-AT Trio Presidency Cybersecurity Work Programme) through the establishment of a Tripartite (Commission, Member States, Enterprises) Joint Undertaking.

To be effective and achieve its proposed objectives at European level, the network should rely on a well-defined governance system.

This network would be supported by a Cybersecurity Research and Competence Centre (CRCC) at European level, linking existing national competence centres across the EU. The CRCC would not only coordinate and manage research as in other joint undertakings, but also allow for the effective development of a European cybersecurity ecosystem that would support the implementation and deployment of EU innovation.

4.2 **Context: Deterrence**

4.2.1 Fighting cybercrime is a top priority at national and European level requiring a strong political commitment. Deterrence activities should be carried out based on a strong partnership between the public and private sectors, establishing efficient information sharing and expertise at both national and European level. The possibility of expanding Europol's activities in cyber forensics and monitoring could be envisaged.

4.3 **Context: International Cooperation**

4.3.1 Building and maintaining trusted cooperation with third countries through cyber diplomacy and business partnerships is key to strengthening Europe's capacity to prevent, deter and respond to large-scale cyber-attacks. Europe should foster its cooperation with the US, China, Israel, India and Japan. Modernisation of EU export controls should avoid violations of human rights or misuse of technologies against the EU's own security, but should also ensure that EU industry is not penalised with respect to third country offers. An ad-hoc strategy for accession countries should be envisaged to prepare for the exchange of sensitive cross-border data, including the possibility to participate, as observers, in some activities of ENISA countries – these should be ranked according to their willingness to fight cybercrime and a blacklist might be envisaged.

4.3.2 The EESC welcomes the introduction of cyber defence in the envisaged second phase of a possible future EU cybersecurity competence centre. For this reason, in the interim, Europe could look at the development of dual-use competences, including leveraging on the European Defence Fund and the planned creation, by 2018, of a cyber defence training and education platform. Considering the mutually recognised potential and threats, the EESC deems it necessary to develop EU-NATO cooperation, and European industry should also closely follow developments in EU-NATO cooperation on enhanced interoperability of cybersecurity standards and other forms of cooperation in the context of the EU's approach to cyber defence.

4.4 **EU Certification Framework**

4.4.1 The EESC believes that Europe needs to face the challenge of cybersecurity fragmentation through homogeneous interpretation of the rules, including mutual recognition between Member States under a unified umbrella to facilitate the protection of a Digital Single Market. A certification framework could provide a common baseline (with specific regulations on higher levels, where needed), assuring synergies across vertical sectors and reducing the present fragmentation.

4.4.2 The EESC welcomes the creation of an EU cybersecurity certification framework and certification schemes for the different sectors, based upon adequate requirements and in cooperation with the main stakeholders. However, time to market and certification costs, as well as quality and security, are key elements that must be considered. Certification schemes will be set up to increase security according to present needs and threat knowledge: the flexibility and evolution capability of these schemes should be considered to allow for needed updates. Different approaches must be provided for different sectors due to the way they function. Therefore the EESC believes that sectoral EU Agencies (EASA, EBA, ERA, EMA, etc.) should be involved in the process and in some cases, with the agreement of ENISA to avoid duplication and lack of coherence, delegated to elaborate cybersecurity schemes.

4.4.3 For the Committee it is important to base the certification framework on commonly defined European cybersecurity and ICT standards that are, as far as possible, internationally recognised. Considering the timeframe and national prerogatives, minimum European standards for IT security should be adopted in cooperation with CEN/CENELEC/ETSI. Professional standards should be considered positively but should not be legally binding or hinder competition.

4.4.4 There is a clear need to associate liabilities with the different levels of assurance based on the impact of threats. Opening dialogue with insurance companies could benefit the adoption of effective cybersecurity requirements according to the sector of application. In the EESC's view, companies looking for "assurance level high" should be supported and incentivised, especially for life critical devices and systems.

4.4.5 Given the time that has elapsed since the adoption of Directive 85/374/EEC[9], and in view of current technological developments, the EESC calls on the Commission to look into the relevance of including in the scope of the directive some of the scenarios set out in this proposal for a regulation, in order to make for safer products with a high level of protection.

4.4.6 The EESC deems that the envisaged European Cybersecurity Certification Group supported by ENISA should be made up of national certification supervisory bodies, private sector stakeholders and operators from various application domains to ensure the development of comprehensive certification schemes. In addition, cooperation should be envisaged between this group and sector-representative associations from the EU/EEA (e.g. cPPP, banking, transport, energy, federations, etc.), via the appointment of experts. This Group should be able to consider European achievements in certification (mainly based on the SO-GIS Mutual Recognition Agreement (MRA), national schemes and proprietary ones) and aim to preserve European competitive advantages.

[9] OJ L 210 of 7.8.1985, p. 29.

4.4.7 The EESC proposes that this group of stakeholders should be given responsibility for jointly preparing certification schemes, together with the European Commission. Sectoral requirements should also be defined through consensual agreement between public and private (users and suppliers) stakeholders.

4.4.8 Moreover, the group should regularly review the certification schemes, considering the requirements of each sector, and adapt the schemes when necessary.

4.4.9 The EESC supports the phasing out of national certification schemes when a European scheme is introduced, as proposed in Article 49 of the Regulation. A single market cannot work with different and competing national rules. To this end, the EESC suggests taking a census of all national schemes.

4.4.10 The EESC suggests that the Commission launch an action to promote cybersecurity certification and certificates in the EU and support their recognition in all international trade agreements.

4.5 **ENISA**

4.5.1 The EESC considers that ENISA's new permanent mandate as proposed by the Commission will significantly contribute to enhancing the resilience of European systems. However, the accompanying provisional budget and resources allocated to the reformed ENISA may not be sufficient for the agency to fulfil its mandate.

4.5.2 EESC encourages all Member States to establish a clear and similar counterpart to ENISA, as most of them have not done it yet. A structured programme to second national experts (SNEs) to ENISA should be promoted to support exchange of best practices and strengthen trust. The Committee also recommends that the Commission ensure that the present good practices and effective measures existing in the Member States are collected and shared.

4.5.3 The EESC also feels that, in terms of capacity building ENISA should prioritise actions to support e-government[10]. EU/worldwide digital identity for persons, organisations, companies and objects is key, and preventing and combating ID theft and online fraud as well countering industrial intellectual property theft should be a priority.

4.5.4 ENISA should also provide regular reports on the cyber-readiness of Member States, primarily focusing on sectors identified in Annex II to the NIS Directive. A yearly European cyber exercise should assess the readiness of Member States and the effectiveness of the European cyber crisis response mechanism, and should produce recommendations.

4.5.5 The EESC is worried that resources are too limited, in terms of operational cooperation, including the CSIRTs network.

4.5.6 In terms of tasks related to the market, the EESC considers that boosting cooperation with Member States and setting up a formal network of Cybersecurity Agencies would help to support cooperation

[10] Digital Single Market/Mid-term review.

among stakeholders[11]. Time to market is very short and it is critical for EU companies to be able to compete in this field, and ENISA must be able to react in tune with this. The EESC considers that, like other EU agencies, ENISA could in future, apply a system of fees and charges. The EESC is concerned that competition for competences between EU and national agencies could, as has occurred in other fields, delay the proper establishment of the EU regulatory framework and damage the EU single market.

4.5.7 The EESC notes that tasks relating to R&I and to international cooperation are currently minimal.

4.5.8 The EESC considers that cybersecurity should be a regular discussion point during the regular Justice and Home Affairs (JHA) Agencies joint meetings and that ENISA and Europol should cooperate regularly.

4.5.9 As the cyberworld is very innovative, standards need to be carefully considered to avoid hindrance to innovation, which requires a dynamic framework; both forward and backward compatibility should be guaranteed as far as possible, in order to protect both citizens and companies' investments.

4.5.10 Due to the importance of national certification supervisory authorities, the EESC suggests that this Regulation should already establish a formal network of authorities empowered to solve cross-border issues with the support of ENISA. The network could at a later stage evolve into a single agency.

4.5.11 Trust is fundamental, but ENISA may not issue decisions nor audit reports. The EESC takes the view that the agency should monitor the performance and decision-making of national certification supervisory authorities through audits and inspections, on behalf of the Commission.

4.5.12 Participation in the ENISA management board should be extended, as observers, to industry and consumer organisations.

4.6 Industry, SMEs, funding/investments and innovative business models

4.6.1 Industry and investments

To increase the global competitiveness of EU companies operating in the ICT field, actions must be geared towards better supporting the growth and competitiveness of the ICT industry, including of SMEs.

Europe should scale up investments converging different EU funds, national funds and private-sector investments towards strategic objectives in strong public-private cooperation. The level of investment in critical domains should be increased and supported by the creation of an EU Cybersecurity Fund for Innovation and R&D in the current and future Research Framework Programme. Furthermore, Europe should create a fund for deployment for the Cybersecurity, opening a new window in the current and future Connecting Europe Facility as well in the next EFSI 3.0.

[11] OJ C 75, 10.3.2017, p. 124.

Incentives should be created for EU Member States to purchase European solutions when possible and select European suppliers if available, especially for sensitive applications. Europe should support the growth of European cyber champions that can compete on a global market.

4.6.2 SMEs

Due to the fragmentation of the market, there is a need for more clarity on client demand, in order to better address the market. Without a structured demand, SMEs and start-ups cannot grow at a rapid pace. In this context the establishment of European a cybersecurity SME hub would be positive.

Cybersecurity technology is changing rapidly and SMEs, thanks to their agility, can provide the cutting-edge solutions needed to remain competitive. Compared to third countries, the EU is still looking for an appropriate business model for SMEs.

Start-ups and SME-specific schemes could be devised to support the cost of certification to counteract the great difficulty in raising funds for their technological and commercial development.

4.7 The human factor: education and protection

4.7.1 The EESC notes that the Commission's proposal does not take sufficient account of people as drivers of digital processes, either as beneficiaries or as a cause of major cyber incidents.

4.7.2 There is a need to build a strong cyber skills base and improve cyber hygiene and awareness among individuals and businesses. To achieve this result, dedicated investment, time to train high-level instructors and effective awareness campaigns should be considered. The implementation of these three lines of action requires the involvement of national and regional authorities (responsible for establishing and investing in effective educational programmes) and of businesses and SMEs in a collective approach.

4.7.3 The creation of a possible EU-certified curriculum for high schools and professionals, with the active involvement of ENISA and its national counterparts, should be envisaged. Moreover, gender equality must be considered when developing educational programmes to improve employment levels in cybersecurity.

4.7.4 The EESC believes that the certification process must include a proper labelling system both for hardware and software, as is the case with many other products (e.g. energy products). This instrument will have the triple advantage of reducing costs to businesses, overcoming existing market fragmentation caused by different certification systems adopted at national level, and facilitating consumer understanding of the quality and features of the item purchased. In this regard, it is important that products imported from third countries are subject to the same certification and labelling mechanisms. Lastly, the EESC believes that the introduction of an ad hoc logo could be an effective way of informing consumers and users immediately about the reliability of purchased products or trading sites, or sites where sensitive data is transmitted.

4.7.5 ENISA should lead an essential multi-level information and awareness raising exercise, in order to increase knowledge of "secure" cyber behaviour and users' trust in the internet. To this end, business associations, consumer associations and other digital services bodies must be involved.

4.7.6 In addition to the Cybersecurity Act, as has already been proposed in Opinion INT/828, the EESC considers it crucial to launch at the earliest opportunity a major Europe-wide programme for digital education and training, providing everyone with the tools they need to cope with the transition. Whilst it is aware of the specific national remit in this area, the EESC hopes that the programme will start in schools, building on teachers' knowledge, adapting curricula and teaching methods to digital technologies (including e-learning) and providing all pupils with high-quality training. The programme will naturally include provision for lifelong learning with the aim of adjusting or updating all workers' skills[12].

5. Specific comments

5.1 Emerging technologies and solutions: the case of Internet of Things (IoT)

The number of connected devices is constantly increasing and is expected to reach a multiple of the number of people living on earth, due to the digitalisation of components, systems and solutions, and enhanced connectivity. This trend creates new opportunities for cyber offenders, especially because IoT devices are often not as well protected as traditional devices.

European security standards across different verticals using IoT devices can reduce development effort, time and budget for all industry participants in the value chain of connected products.

Some form of minimum security level through IDAM (Identity & Access Management), patching and device management is likely to be necessary for "ordinary" "Internet of People" (IoP) devices. As certification is a key method of providing a higher level of security, more emphasis should be given to Internet of Things (IoT) security in the new EU certification approach.

Brussels, 14 February 2018.

Georges Dassis
The president of the European Economic and Social Committee

____

[12] Digital Single Market/Mid-term review.