IEEE

EU Policy News Bulletin

ICT

November 2019

AT A GLANCE: EUROPEAN PARLIAMENT CONFIRMED THE NEXT INTERNAL MARKET COMMISSIONER - CROATIAN PRESIDENCY TO START IN JANUARY 2020 - INDUSTRIAL IOT AND CYBERSECURITY TOP PRIORITIES - ENISA THREAT LANDSCAPE FOR 5G NETWORKS - IS CERTIFICATION THE ANSWER TO RISK MITIGATION IN EUROPE?

Edition Content

EU INSTITUTIONS

EU INDUSTRIAL POLICY

CYBERSECURITY

GLOSSARY

AI: Artificial Intelligence, the simulation of human intelligence processes by machines, especially computer systems.

DG CNECT: The Directorate-General for Communications Networks, Content and Technology is the European Commission department responsible to develop a digital single market to generate smart, sustainable and inclusive growth in Europe.

ENISA: The European Union Agency for Cybersecurity, fully operational since 2005 and located in Athens, Greece.

EP: European Parliament, institutions of the European Union constituted of 751 Members of Parliament directly elected by European citizens.

GDPR: General Data Protection Regulation, it replaces the Data Protection Directive 95/46/EC and is designed to harmonise data privacy laws across Europe, protect and empower all EU citizens' data privacy and reshape the way organisations across the region approach data privacy.

IOT: Internet of Things is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

MEP: Member of the European Parliament, a co-legislator within the EU that is made up of representatives from political parties throughout Member States.

NIS DIRECTIVE: The Directive on security of network and information systems entered into force in August 2016. It provides legal measures to boost the overall level of cybersecurity in the EU.

The material contained in this newsletter may reflect the opinions of its authors and not necessarily IEEE.

Edition Content

EU INSTITUTIONS

European Parliament confirmed the next Internal Market Commissioner

Mr Thierry Breton, the French nominee for the position of Commissioner in charge of the Internal Market, was approved by the European Parliament committees on industry and internal market on 14 November.

©Shutterstock

If the Parliament plenary confirms the whole College of Commissioners on 27 November, the new European Commission, led by President Ursula von der Leyen, will be able to take office in December 2019.

During his hearing, Mr Breton outlined his political priorities and clarified his views on a wide range of topics including the regulation of online platforms, EU's technological sovereignty, AI, unfair competition from third countries, competition policy, data protection & data sharing, EU's industrial policy, public procurement or the regulation of cyberspace.

Repeatedly asked by MEPs how he would avoid conflicts of interest arising from his industrial background, Breton pledged to work independently and transparently and to not give "special treatment" to the companies he had previously worked for or was associated with, in line with Code of Conduct for European Commissioners. "I will be as independent as I was as a French minister", he said in an attempt to assuage some MEP's concerns.

Key points for IEEE were the following:

Technological sovereignty: Breton emphasised that EU needs to invest heavily in critical technologies like 5G, 6G, AI, cloud computing, blockchain or quantum computing to become a key industrial player in new technology. The battle with other regions in the world is not lost, he said, making the point that there are many technologies where the EU is leading the way, such as green technologies. He also said that the Commission is working on establishing a European Innovation Council with the aim to support technological innovation in Europe. He took the view that European data needs to be stored and processed in Europe to make sure it remains secure.

Artificial intelligence: Breton stressed that AI relies on three pillars: available data, computing power and algorithms. "I will be the Commissioner of data", he said.

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

Edition Content

EU INSTITUTIONS

EU INDUSTRIAL POLICY

CYBERSECURITY

He hinted that he was not necessarily in favour of new laws on AI in the new Commission's first 100 days in office, stressing it would be up to the entire College of Commissioners to decide on the issue and that he would back their decision.

Cyberspace: Breton pledged to regulate the structure and activities of cyberspace to ensure free access to Europe's single market. There needs to be a free access and fair distribution with a level playing field, he said.

Data protection & data sharing: Breton made the point that European citizens should be able to do what they want with their data. In the single market of data, especially industrial ones, some data needs to be kept by companies because it is key for R&D or innovation, while some data must be pooled or shared in an anonymised way because it can contribute to progress, he underlined.

Digital Services Act: Breton assured MEPs that the digital platforms' intermediary liability regime, as established by the e-Commerce Directive, will be preserved under the DSA, adding that the DSA could become a global standard like the GDPR to regulate online platforms' activities.

Industrial policy: Breton vowed to use a host of measures, from subsidies to trade defence and border taxes – to help companies face the digital and green transitions and to put forward an "ambitious industrial strategy".

Next steps:

- 27 November: The Plenary of the European Parliament is due to vote on the appointment of the new College of Commissioners as a whole

Early December: Von der Leyen's Commission is expected to enter into office(

Source: Interel)

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

The material contained in this newsletter may reflect the opinions of its authors and not necessarily IEEE.

Edition Content

EU INSTITUTIONS

EU INDUSTRIAL POLICY

CYBERSECURITY

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

Croatian Presidency to start in January 2020

©Shutterstock

On 7 November we attended the American Chamber of Commerce to the EU digital economy meeting with Viktor Sober, Minister Counsellor, Telecommunications and Information Society at the Croatian Permanent Representation to the EU, and Domagoj Maricic from the Croatian Post and Electronic Communications Agency. The overall feeling is that the Croatian Presidency will be driven by the European Commission and the subsequent German Presidency, with officials present not appearing to have a very ambitious work plan.

They listed their four presidency priorities as follows:

- Europe that is developing
- Europe that connects
- Europe that protects
- Influential EuropeMore specifically, on the legislative side, they will focus on 5G (security, smart cities); the cybersecurity competence centre community; connectivity (digital divide, digital skills); new issues (AI, blockchain); and finalising existing proposals (E-privacy).

Other policy issues include Cybersecurity, Artificial Intelligence (AI) and the Gaia-project. With regards to cybersecurity, it is expected that by October 2020 we will be seeing some activity on certification of 5G networks, based on the certification regime introduced in the Cybersecurity Act. There are currently many changes in the Commission's directorate for technology (DG CNECT) with senior officials moving, so there is a brief pause in activity. A clearer picture is expected to emerge in the next 2-3 months.

Concerning AI, a consultation is expected as soon as the new European Commission comes into office. An Impact Assessment could be presented end of February / early March 2020. It is also clear that the proposal will be a regulation.Finally, there is increasing interest in the "Gaia-X"- project, a Franco-German cloud initiative, which aims to set up an efficient, competitive, secure, trustworthy and decentralised data infrastructure for Germany and Europe. This new data infrastructure should

Edition Content

strengthen both the digital sovereignty of cloud services users and the scalability and competitive position of European cloud providers. The political pressure for a European cloud solution increased over the last months, as there is a perception of high dependence on foreign providers. The EU sees a need to foster this key technology in order to stay competitive against the USA and China.

(Source: Interel)

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

Edition Content

EU INSTITUTIONS

EU INDUSTRIAL POLICY

CYBERSECURITY

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

EU INDUSTRIAL POLICY

Industrial IoT and cybersecurity are top priorities

A European Commission expert group, the Strategic Forum on Important Projects of Common European Interest (IPCEI), has published its recommendations for a common vision for joint actions and investments between EU, Member States and industry, on key strategic value chains in Europe.

©Shutterstock

The following sectors were identified as strategic:

- Connected, clean and autonomous vehicles
- Smart health
- Low-CO2 emission industry
- Hydrogen technologies and systems
- Industrial Internet of Things
- CybersecuritySuggested actions include joint investments; consolidation of Single Market through regulations and standards; and development of new skills. In addition, experts call for an agile governance process to monitor technological and industrial developments, to identify emerging strategic value chains and to monitor and evaluate the progress of work on these value chains.

Industrial Internet of Things (IoT) is a subset of IoT focussing on specialised requirements of industrial applications in various industry segments such as manufacturing, oil and gas, transportation/mobility, energy, and utilities. Industrial IoT technologies are at the centre of the digital transformation of European industry and open plenty of opportunities in all industrial sectors. Recommendations revolve around the following topics:

- Secure and trusted data spaces
- Industrial cloud, edge and data infrastructures
- Tools for data exploitation and AI
- A future industrial 5G infrastructure that responds to industrial needs
- Digital industrial platforms driven by EU actors
- Cybersecurity
- Skills development - especially in advanced analytics and artificial intelligence
- Scale-up-existing initiatives
- A sector-based approachCybersecurity covers a wide range of topics, including

The material contained in this newsletter may reflect the opinions of its authors and not necessarily IEEE.

Edition Content

encryption, monitoring, identity management, authentication, endpoints (devices) and digital services. It encompasses hardware, software and services, The IPCEI's vision on EU cybersecurity revolves around the following topics: competitiveness, protection, independence, leadership. The main challenges for the European cybersecurity industry are identified as follows:

- In some sectors, the biggest players and service providers are non-European.
- European companies are also small, compared to the global giants.
- The skills gap: Europe will be competing for a limited talent pool. The skills gap for cybersecurity professionals working in the industry in Europe is predicted to be 350,000 by 2022 and globally 1.8 million.A large number of recommendations are made, grouped around two topics: coordinated investments in five specific areas; and related supporting recommendations (eight additional areas of actions, that would be required and useful to support the development of the Cybersecurity value chain.

The recommendations are consistent with previous intelligence on EU strategic priorities in the field of IoT (especially industrial IoT, where some EU companies still play a leading role) and cybersecurity, where the expressed goal has been achieving EU strategic autonomy and develop a competitive industry.

(Source: Commission and Interel)

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

The material contained in this newsletter may reflect the opinions of its authors and not necessarily IEEE.

Edition Content

CYBERSECURITY

ENISA threat landscape for 5G networks

ENISA, the European Union Agency for Cybersecurity published a **Threat Landscape for 5G Networks**, assessing the threats related to the fifth generation of mobile telecommunications networks (5G).

This technical report on 5G architecture completes the EU-wide **Coordinated Risk Assessment of 5G networks** published on 9 October 2019, which contained 10 high-level risk scenarios, based on the national risk assessments by EU Member States.

©Shutterstock

The ENISA 5G threat landscape contains:

A detailed architecture outlining the most important 5G infrastructure components through 9 detailed zoom-ins of the 5G architectural elements mentioned in the coordinated risk assessment. These include the security architecture, slice architecture, edge computing architecture, software defined networks architecture, physical architecture, and others.

Detailed threat assessments for the 5G infrastructure components. The assessed threats refine the threats reviewed in the coordinated risk assessment.

5G infrastructures possess a high degree of complexity due to the multiple features introduced by this technology. While 5G pilots are ongoing, standardisation work is also advancing as do vendor development activities towards migrations to 5G. In this still very dynamic environment, threat and risk assessments will need to be performed in an iterative manner to cover upcoming developments.

The developed 5G Risk Assessment and the 5G Threat Landscape are **initial steps** towards the longer maturity trajectory of 5G infrastructures, their deployment and adoption. They will need to be regularly updated in order to capture those changes appropriately. Certification of 5G components is perceived as a further trigger of threat and risk management activities.

The network and information systems (NIS) Cooperation group and the Member States with the support of ENISA will publish a 5G toolbox towards the end of 2019 to provide a number of different directions and options for the Member States to take. Certification of 5G architecture components is a likely action depending on the exact designation of tools under the toolbox initiative carried out. The scope of 5G certification schemes needs to be determined by the European Commission with input from the Member States and duly communicated to ENISA.

(Source: ENISA)

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

The material contained in this newsletter may reflect the opinions of its authors and not necessarily IEEE.

Edition Content

EU INSTITUTIONS

EU INDUSTRIAL POLICY

CYBERSECURITY

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

Is Certification the answer to risk mitigation in Europe?

An event titled "Is Certification the answer to risk mitigation in Europe?", sponsored by Huawei, took place on 19 November in Brussels. Speakers included an official from the Commission's directorate for technology (DG CNECT) and an official from the Croatian Permanent Representation to the EU (upcoming presidency of the Council of the EU), as well as an academic and a representative from GSMA, the mobile network operators trade association. Please note that none of the speakers' comments can be attributed since the event followed the Chatham rules.

A lot of the focus was on 5G and how such a complex system can be certified. Some participants called for more information exchange. It was also stressed that certification is a Single Market tool and just part of the solution, with public awareness another necessary component to make it successful.

The following points stood out:

We are observing a shift from security being a competitive advantage to it being a collaborative issue (e.g. exchange of information between stakeholders). Speakers supported common standards, as a way to enhance trust. However, a key challenge is the interpretation of security requirements for a complex product, which is time-consuming.

It was further highlighted that certification is not the answer to the entire cybersecurity question, but an important step, comparing it to energy efficiency labelling on appliances and climate change. Cybersecurity is a Member State's issue, with the Commission working to ensure the internal market is not distorted. Industry also appears to be taking certification efforts seriously.

The EU's top priority on 5G is to have a secure network running and operating. The ambition is for Europe to have a capacity that is not disrupted, whatever happens to other parts of the world. This does not mean that third country providers should be prevented from coming to Europe, but we must ensure we can still operate, whatever the situation is in other states.

The certification of 5G must be complemented with public awareness of what certification means and how they can use the various products. The goal is that a certificate issued by one country will have almost the same validity in all Member States, even if there are differences as to the level of assurance being implemented.

Speakers stressed that first we need to decide what certification is for and whether certificates are aimed at consumers or operators. We also need to consider how to bring together the various pieces of the puzzle (cyber act, common criteria, some existing schemes) and determine the levels of criticality, what needs basic, substantial, high etc. Certification must also be updated and we need to look at the common criteria for that.

Finally, it was said that the conversation should be about trust and resilience, not about security for security's sake.

(Source: Interel)