Edition Content

EU INSTITUTIONS
New Internal Market Commissioner-designate still to be confirmed by the European Parliament P.2

EU DIGITAL POLICY PRIORITIES
Artificial Intelligence legislative framework in 100 days P.4

CYBERSECURITY
ENISA-Europol conference on Cybersecurity and the Internet of Things P.5

BLOCKCHAIN
Reports on regulatory framework of Blockchain and use in finance, trade and public services P.7

GLOSSARY

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

**CEO:** The chief executive officer, the highest-ranking person in a company or other institution, ultimately responsible for taking managerial decisions.

**DG:** European Commission Directorate-General. Department in charge of a certain EU policy area.

**ENISA:** The European Union Agency for Cybersecurity is an agency of the EU. It is fully operational since 1st September 2005.

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

**EUROPOL:** The European Union Agency for Law Enforcement Cooperation is the law enforcement agency of the EU formed in 1998 to handle criminal intelligence and combat serious international organised crime and terrorism through cooperation between competent authorities of EU member states.

**GDPR:** General Data Protection Regulation, it replaces the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, protect and empower all EU citizens’ data privacy and reshape the way organizations 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.

**WEF:** The World Economic Forum, based in Cologny-Geneva, Switzerland, is an Non-Governmental Organization, founded in 1971, with a membership of 1,000 multinational corporations, on whose behalf it lobbies, primarily for deregulation.
EU INSTITUTIONS

New Internal Market Commissioner-designate still to be confirmed by the European Parliament

The Commissioner-designate for the Internal Market, who would also be responsible for the Digital Single Market, the French Sylvie Goulard, a close ally of President Macron, was reject by the European Parliament at the beginning of October. This was due to ongoing investigations on her concerning alleged misuse of EU funds related to her parliamentary assistant’s work. Concerns were also raised about the extent of her portfolio, which included internal market, digital issues, industrial policy, defense and space. Despite a second hearing to plead her case, she failed to convince Members of the European Parliament (MEPs) of her suitability.

This rejection was perceived as a major humiliation by the French Government, which took two weeks before suggesting a new candidate suitable for the role. The new French Commissioner-designate, Thierry Breton, aged 64, is a very successful businessman and former French Finance, Economy and Industry Minister under President Jacques Chirac in 2005-2007. He is currently CEO of Atos since 2007 and was formerly CEO of France Telecom and Thomson (now Technopolis). He pro free market and business friendly, and was an early backer of Macron’s presidential candidacy in 2017. He has the great advantage of combining technical expertise (being a computer engineer by training), political experience and business knowledge.

However, Breton is very vocal about the need for more EU digital sovereignty, which is also one of the Commission President-elect’s main priorities. Earlier this year, he compared sovereignty over the “information space” to sovereignty over land, sea and air at a Senate hearing. He also voiced strong views on data localization, and said “European data needs to stay in Europe and remain under EU law”. His nomination is, therefore, very coherent with the orientation the Commission wants to give to EU digital policy.

Breton also argues that Europe “need[s] a digital policy and a real industrial policy at European level.” At the same time, he is sharply critical of the EU’s competition laws, arguing that “the politics of competition has laid down the law and sometimes has caused industrial disasters. It is therefore necessary that the new Commission...
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**
New Internal Market Commissioner-designate still to be confirmed by the European Parliament  
P.2

**EU DIGITAL POLICY PRIORITIES**
Artificial Intelligence legislative framework in 100 days  
P.4

**CYBERSECURITY**
ENISA-Europol conference on Cybersecurity and the Internet of Things  
P.5

**BLOCKCHAIN**
Reports on regulatory framework of Blockchain and use in finance, trade and public services  
P.7

promotes the development of major European players that will allow the entire industry of yesterday to play on a level playing field with that of tomorrow” he said during an interview. This view might put him at odds with his future superior, the incoming Executive Vice-President for Digital, Margrethe Vestager.

The new Commissioner-designate for the Internal Market will have to face a Parliamentary hearing in the course of November before being confirmed. President Macron’s priority is now to keep the large portfolio he obtained in the negotiations with the Commission President-elect and to avoid a second rejection by the European Parliament.

Following the rejection of three Commissioner candidates, from France, Romania and Hungary, the prospect of the new Commission taking office on 1 November as scheduled fell apart. A 1 December start date for the Commission is now considered more likely.

(Source: Interel)
EU DIGITAL POLICY PRIORITIES

Artificial Intelligence legislative framework in 100 days

The Commission-President elect, Ursula von der Leyen, in her political manifesto vowed to draft a regulatory framework on Artificial Intelligence (AI), that will be prepared in the first 100 days of her mandate. She also wants to ensure the multiannual financial framework prioritises investments in AI.

In her confirmation hearing in the European Parliament, Margrethe Vestager, Executive Vice President-designate for a Europe fit for the Digital Age and Commissioner-designate for Competition, gave more information on how this legislative framework will look like but said she didn’t know whether the Commission would propose a regulation or a directive.

The framework is set to draw on the existing work of the High-level Expert Group on AI, which recently drafted policy recommendations and ethics guidelines. While they recommend “regulating algorithmic systems with common horizontal requirements in European law”, the Group also stated that “unnecessarily prescriptive regulation should be avoided.” Vestager specified that different options will be explored ranging from self and co-regulatory measures to third party verification systems. She specifically highlighted the need to facilitate data sharing and access to data.

The EU’s aim is to set strong global standards on AI, privacy, liability, data and blockchain, as was done with the EU General Data Protection Regulation (GDPR). Asked about how the EU can be a leader in AI, Vestager responded it can only be the case if the EU instils trust in AI among citizens by enforcing strong ethical standards and by ensuring that algorithmic systems are not discriminatory with regard to biased datasets. She made the point that the EU will lose the battle with China and the US if it focuses on allowing companies to collect as much data as possible and invest significant amounts of money. She pointed to healthcare, environment and mobility as industries where Europe excels, and where the EU can deploy AI to a greater purpose.

She committed to set up a new public private partnership in AI to develop a roadmap for EU leadership in AI technology. Finally, she plans to ensure public awareness actions to improve citizens understanding of AI applications.

(Source: Interel)
The 3rd ENISA - Europol Internet of Things (IoT) Security Conference was held on 24 and 25 October 2019 and focused on the cybersecurity of the Internet of Things and emerging technologies, such as Artificial Intelligence (AI). The conference provided a platform for all relevant stakeholders to exchange insights, discuss pertinent topics and challenges, and identify good practices, security measures and solutions.

Overall, the emerging ecosystem will be predominantly made up of the interplay between AI-IoT-5G-cloud. Therefore, ENISA calls for a baseline IoT security, covering smart homes; industry 4.0; smart cities; smart airports; smart hospitals; smart cars. Research by IBM has shown that 69% of enterprises have more IoT devices on their networks than traditional endpoints. However, traditional security practices are not designed for IoT. AI can be used to help secure devices where it is not possible to install an agent (e.g. AI looks at a device make, model, vulnerabilities etc. and raises flags). Moreover, security will also become more challenging due to devices taken outside corporate networks. Most of motivation for attacks comes from monetary gain (47%) and Intellectual Property theft (30%). The rest are personal information theft, ransomware, cryptocurrency and destruction.

IoT main challenges include:

- Large attack surface and widespread deployment (stressed by a number of speakers);
- Security for safety (esp. for critical sectors);
- Interoperability, increased connectivity and cascading effects;
- Security and privacy by design not a top priority;
- Lack of expertise;
- Applying security updates;
- Lack of secure development practices;
- Fragmentation of new practices and standards;
- Unclear liabilities;

IoT security presents challenges due to scalability, heterogeneity, dynamic nature. Moreover, hardening the network itself is no longer sufficient, as attacks can come from connected devices. An additional observation was that privacy and security go in hand in hand; it is not possible to have one without the other. IoT devices should...
hence follow principles of proportionality, data minimization and transparency, while enabling the use of security techniques to assist with accuracy, integrity and confidentiality. They should not collect more data than necessary and protect whatever data they collect.

According to the World Economic Forum (WEF) the threat profile associated with the IoT is: lateral movement; theft of payment devices; surveillance abuse; physical attacks (currently on the rise due to the physical-digital convergence); blackmail. Another key issue is the second half of humanity coming online with low cost, not necessarily smart, devices. The focus will be on banking, weather information for farming and participation in health schemes. There are already issues with the more educated population, so this population will present additional challenges.

Regulators were urged to “make it easy” when considering regulation; it was stressed that “we are better together”, but this does not mean everyone should be saying the same thing. Instead, we should make sure that every different “size” we use reflects best practice.

Finally, security needs to be “baked in” to devices. Security first (designed at the start); fit for purpose (right-sized for application); resilience (through operating life) need to be emphasised. The current EU regulatory framework is insufficient, as the Cybersecurity Act, GDPR and Radio Equipment Directive include some provisions, but significant gaps still exist.

(Source: Interel)
EU INSTUTITIONS
New Internal Market Commissioner-designate still to be confirmed by the European Parliament  P.2

EU DIGITAL POLICY PRIORITIES
Artificial Intelligence legislative framework in 100 days  P.4

CYBERSECURITY
ENISA-Europol conference on Cybersecurity and the Internet of Things  P.5

BLOCKCHAIN
Reports on regulatory framework of Blockchain and use in finance, trade and public services  P.7

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

BLOCKCHAIN
Reports on regulatory framework of Blockchain and use in finance, trade and public services

The Joint Research Centre of the European Commission has published the “Blockchain Now And Tomorrow” report, which looks at the potential of the technology for the economy, industry and society, covering various sectors. It look into the state of blockchain technology by identifying ongoing and upcoming transformations in a range of sectors and setting out an anticipatory approach for further exploration. It also attempts to look beyond the hype and address controversies, taking a look at possible applications. The report notes that blockchain is “one of the technologies which is anticipated to have a profound impact over the next 10-15 years”.

Sectors covered by the report include financial systems (for example, reducing the costs across the lifecycle of a financial product); industry, trade and markets (e.g. traceability and quality control, supply chain management); government and public sector (e-IDs, tailored services for citizens, workflow automation and shared databases).

In addition, the European Union Blockchain Observatory and Forum has published a report exploring the legal issues pertaining to blockchain technology, particularly those around its decentralized nature and the implications of different types of smart contracts.

The main legal challenges arise form blockchain’s fundamental characteristics, such as decentralisation, pseudonymity / anonymity, immutability and automation. One challenge arising from this, for example, is ascertaining who the actors in the network are, where they are located, and what exactly their actions have been. That can make it challenging to assign responsibility or determine jurisdiction in the case of disputes. This, in turn, has repercussions for liability, determining which law is particular to which situation, regulatory monitoring, enforcement of rules etc.

The report states that none of the challenges outlined are insurmountable and proposes a twin track approach:

- Evolution of legal and regulatory “tools” to assist authorities with some of the novel aspects of blockchain technology;
- Natural evolution of the legal and regulatory framework to take account of blockchain.

Finally, the report urges regulators to provide guiding principles to attract private-
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.