Fonds européen de développement régional (FEDER)
Europäischer Fonds für regionale Entwicklung (EFRE)

Report 7.1.1: European rules for the security of energy data

Bushra Canaan, Djaffar Ould Abdeslam

Université de Haute-Alsace (UHA), Institut de Recherche en Informatique, Mathématiques, Automatique et Signal (IRIMAS)

Report 7.1.1: Detailed report on the European rules for the security of energy data

This series of reports of the WP7 Reporting on the future of Smart Grids/Energy Grids. It discusses technological issues associated with the deployment of Smart Grids, analyses implications for policymakers, citizens and society, industry and operators, as well as regulatory and financial conditions.

In this report we provide a brief review on the latest legislations, measures and initiatives adopted by the EU in terms of cyber security. With a special focus on smart grids to support electricity security during a period of rising digitalisation and decentralisation (Distributed Resources Control and meters).

1. Background and research gap

Intro

Critical sectors such as transport, energy, health and finance have become increasingly dependent on digital technologies to run their core business. While digitalisation brings enormous opportunities and provides solutions for many of the challenges Europe is facing, not least during the COVID-19 crisis, it also exposes the economy and society to cyber threats[1].

Utilities and other infrastructure have become increasingly attractive targets for bad actors, whether for financial or political gain. Attempts to breach systems grow, especially for systems that control vital infrastructure such as the electric grid.

Through the last few decades, the energy sector has witnessed a radical shift in the course of several paramount yet interconnected aspects. For instance, Energy markets were never the same after its liberalization by means of the modern regulations that enabled monopolies unbundling and introduced competition. Same thing goes on for organizational aspects, where decentralized energy systems have reinforced the role of end consumers, imposing a decentralized planning scheme instead of the conventional hierarchy planning adopted by centralized systems. On the other hand, the tangible progress among smart communication technologies and application also raised the bar when it comes to operational aspects [2] .

As necessary as it may seem to upgrade the network into the future smart grid by applying the latest technological trends, it is accompanied by quite a few expenses that cannot be underestimated[3].From a technical point of view, the entangled Energy systems are one of the most complexed strategic infrastructures in this digitalization era, steering the wheel of both economic and social events.

A new regulatory framework is necessary to ensure the most effective type and level of incentives to stimulate the investments required by the transition towards Smart Grids, while ensuring a level playing field in the sector[4].

This report starts with the identification and discussion of the technological issues and challenges associated to the deployment of smart grids, then analyses constrains and implications for citizens and society, for industry and operators, as well as the regulatory and financial framework conditions. It finally illustrates the current policy perspective and presents a series of policy-relevant conclusion.

Energy security in the increasing presence of DER- renewables

The electricity sector is on a clear pathway: more renewables, more distributed energy, more electric vehicles. According to industry forecasts, by 2030 consumers would invest more money in distribution-edge devices—solar PV, batteries, charging stations, electric vehicles, and smart controls, than electric utilities would invest in power generation and electricity grids. Collectively, these devices could serve the same function as centralized thermal power plants.

However, because they are naturally decentralized and distributed, they are rarely employed to their full capacity, making safe digitization, coordination, control, tracking, and financial settlement with each device expensive and often cyber-insecure. Furthermore, given the market interests of each individual device vendor, combining devices into a single grid participant is problematic.

Although its benefits are well known, policymakers have traditionally found it difficult to tap into the immense resource of energy efficiency since it is scattered among millions of households, appliances, businesses, and cars. When faced with a choice between collecting tiny amounts of cost-effective energy savings from thousands of hard-to-reach energy customers and building a costly new power plant to supply more energy services, policymakers may prefer the latter, despite the larger cost, simply because it is easier[5].

Smart Meters and Data Security

Smart Meters (SM) at the endpoint of distribution networks liaise with consumers and lends them an open window to interact with the utility. In an ideal scenario, smart segments must effectively communicate via Advanced Metering Infrastructure (AMI) to reach the perfect balance.

Since its first appearance in 1872 [6], the concept of electricity meter has remarkably evolved. Conventionally, electricity meters used to provide information only about electricity consumption, while intelligent meters are supposed to support a wide range of applications rather than just metering [7].

Despite its relatively low starting point, Smart Metering deployments are currently especially successful in Europe, largely due to the legislation of many countries promoting, or even forcing, the replacement of old metering devices with SMs. In fact, legislation for electricity SMs is in place in the majority of the member states of the European Union, providing a legal framework for deployment and/or regulating specific matters such as a timeline of the rollout or setting technical specifications for the meters[7].

According to the European Commission, member states have committed to deploy 200 million *SMs* by 2020 (Electric Directive 2009/72/EC). This implies that more than 70% of end users will be covered by Smart Grid technology.

The *European Smart Meters Industry Group* (ESMIG) has reduced the minimum features of an *SM* to the following four [8]:

- Remote reading
- Bidirectional communication
- Support of advanced tariff systems and billing applications
- Remote energy supply control.

On the other hand, the absence of human interventions is a key feature of advanced metering plug and play mode, which is very desirable but unfortunately, at its earliest phases, comes with relatively high-risk. Counting; The exposure to different kinds of communication systems, including internet, in addition to the needed adaptability to work with different billing applications that are probably open-sourced. Not to mention the double ownership making smart meters the most vulnerable component of the smart grid.

Impact on the electrical systems depends on the select functionality assigned to the smart meter. Of course, the availability of the entire service of a smart meter is still considered to leave the worst impact on systems, but data communicated via smart meters which provide considerably detailed information about consumers' consumption behaviour or habits are the biggest new concerns. Confidentiality data can be exported in many grievous ways such as optimizing the attacker's understanding of the compromised target so that he can make a more severe attack, extort the service providers, or even sell to unauthorized parties [9].

Energy providers, on the other hand, had their own share of concerns: the manipulation of data at the user end either due to the intentional act by the consumers themselves or cyber-attacks could be used in energy theft and billing manipulation, resulting in revenue loss[10]. For this reason, authenticated software should be implemented, not only on inside the meters, but also on the access side for a granted sound operation[11].

Several EU countries have met or exceeded their goal for 2021 and have moved on to the second round of upgrading. Some countries, on the other hand, are lagging behind, with some even abandoning the commitment entirely.

But still, approving complex rollouts like those suggested by the European Commission takes time. The various European parliaments need to validate the suggestions and vote in favour, with some countries inevitably voting against.

Smart meters in Germany

The pioneering position achieved recently by the German's renewable energy sector, still suffers from the lack of deployment of smart grid technologies, especially when it comes to smart meters. Unlike some of its Western European counterparts who had found themselves in a less dramatic circumstances concerning the legislation set by the European commission.

Under the instruction of EU Directive 2009/72/EC, the German Ministry for Economics has contracted with EY (formerly Ernst & Young) to accomplish a cost-benefit analysis of the nationwide rollout of a smart meter in 2013. The study has revealed a negative cost-benefit ratio which means that adopting the expeditiously implementation of smart meters will be insufficient from an economical point of view, since it will be unaffordable for most of the German consumers.

The discrepancy between the results of EY report and what has the EU Directive 2009/72/EC stipulated regarding the necessity of having a positive economic assessment in the member nations that pursue 80% smart meter penetration by 2020, has placed Germany and six other member states (Belgium, Czech Republic, Latvia, Lithuania, Portugal, and Slovakia) in an inconvenient situation with the opponents to the proliferation of smart meters.

By July 2016, the prolonged and constant debates have started to pay off through passing Energy Turnaround Act (Messstellenbetriebsgesetz – MsbG) which revolve around the Digitisation of Energy sector and prescribes the use of intelligent metering systems consisting of smart meters and smart meter gateways (SMGW: the central communication component of such a Smart Metering System). Based on this enactment, the long-run of smart meters rollout had been scheduled to start in 2017. These updates have paved the way for the next stage of launching the Energiewende, the German plan for energy transition pursuing the goal of providing 80% of its energy demand via renewables by 2050 resulting in low carbon emission, environmentally sound, reliable, and affordable energy supply.

The rollout characteristics in addition to stakeholders share in the project were also specified in the light of the previous legislation provisions. For example, It was expect that smart meters by 2017 will be installed among consumers that have an average annual consumption exceeds 10,000 kWh, in the purpose of decreasing this amount to 6,000 kWh in 2020. This will affect up to 15% of electricity consumers. In other words, around 50 million metering endpoints and 7.5 million smart meters across the nation.

However, things got out of track where it has been decided against a nationwide rollout of smart meters. Due to a lawsuit initiated by a corporation in Aachen, the Higher Administrative Court of North Rhine-Westphalia temporarily halted the rollout. The reason for this is that the legal criteria would almost certainly not be met.

That is that Rolling out smart meters on a nationwide level is an ambitious and complex operation. Effective communication strategies are needed to help consumers understand their rights and how they'll benefit from smart technology. Regulatory measures are needed, as are stakeholder incentives to ensure smart metering products and services are developed quickly. Data privacy and cyber security frameworks also need to be evaluated to ensure compliance with legal obligations.

Even though that the legislation allows the third-party service providers to assist Germany's grid operators in installing and running the smart meters but only a very small percentage of smart meters (around 3%) are operated by non-regulated competitive companies.

Concerning households with smaller consumption rates, the option of installing smart meters is still on the table with the utilities offering this technology with only 40€ per year which is the cost price cap.

The (MsbG) law stipulates that the procedures of fully replacing old meters with smart ones can reach until 2032. However, for the reasons of extrapolating further extends of the smart meters' rollout, some samples of both consumers and operators will have to complete their part before the end of 2024.

In each phase of replacement, technical and economic feasibility must be re-evaluated. For example, economic criteria based on the several measures like the meter's age, level of consumption and charge fees which may vary causing installation time frame debasement. Not to mention problems related to the technological development of data security tools and legislation.

After all, Germany has made its way through the smart meter rollout replacing the EU-Commission strategies with more appropriate but also more limited deployment schedule that comply with EY recommendations.

Smart meters in France (Linky)

Enedis (ex ERDF), the power grid operator for most of France, is responsible for installing the new Linky meters. After an initial pilot phase that took place in 2010 (in which over 250 000 Linky meters were deployed in Lyon and the Indre-et-Loire regions), a national deployment campaign began in December 2015. Over 28 million Linky meters was scheduled to be installed in the programme in 2021.

In total, 35 million household smart meters and 700,000 data concentrators will be installed across France as part of the deployment. This includes system integration, installation, meters, and data concentrators, is one of the largest projects of its kind, with a total cost of € 4,5 billion and is expected to save consumers € 50 per year on average.

Despite the COVID-19 disruptions, in December 2020 assessment affirms that France is on schedule to meet its 80 percent rollout objective by the end of 2021. A target that was reached in December 2021.

The leader multinational corporation in the smart metering solutions industry Landis+Gyr created a custom solution that was justified by the project's size and provided quality performance that beyond expectations. Enedis funded the original development and collaborated with a limited group of vendors, including Landis+Gyr, to build a detailed and rigorous supplier selection process.

The issues of access to data and respect for privacy are the subject of particular attention in all countries with the National Commission for Information Technology and Freedom (CNIL) in France or other equivalent agencies in Europe, such as the Agencia Española de Proteccion de Datos (AEPD) in Spain or the Virtuelles Datenschutzbüro in Germany.

In more detail, and as far as smart meters are concerned, all the metering information is encrypted at the meter level. Only a consumption index is sent to the distribution network operator. Information on the load curve is only sent to the energy supplier with the customer's express consent.

Even though, the CNIL in France insists on that load curves should not be collected systematically, but only when this is justified by the need to maintain the network or when the user expressly requests it in order to benefit from particular services.

Still, the Linky meter faces fierce opposition since its launch. Thousands of people across France have been refusing the mandatory installation of the Linky meters. Some blame it on a lack of transparency in electricity consumption cases of overcharging while others denounce harmful effects on health, in particular concerning electromagnetic hypersensitivity.

For almost two years, a commune in Seine-et-Marne has been at war against Enedis and Linky meters. The town hall had issued an order stipulating that no meter can be installed without the consent of the user. However, this measure has just been rejected by an administrative court after that, the national health and safety agency, Anses in 2017 confirmed that there was very little chance that the devices could cause harm. Whereas the level of exposure to electromagnetic waves is very low compared to those emitted from other household devices, like lamps and screens. People who refuse the installation of a Linky smart meter at their property in France after January 2023 will face paying an extra €50 per year, which has been confirmed, with up to 3.8 million people affected.

The figure comes after a public consultation and report into the issue by la Commission de régulation de l'énergie (CRE) energy commission.

The extra fee was justified due to the fact that technicians from electricity national grid managing firm Enedis will still have to check the "old generation" meters on-site, rather than have the readings automatically sent via the new system.

Although 90% of households are already estimated to have the smart meters installed, the extra fees could affect up to 3.8 million people. This was the number who still had not had the new meter installed by December 31, 2021, provided by the CRE.

2. Research goal and questions

Cyberattacks and cybercrime are increasing in number and sophistication across Europe. This trend is set to grow further in the future, given that 22.3 billion devices worldwide are expected to be linked to the Internet of Things by 2024.

This technological sovereignty needs to be founded on the resilience of all connected services and products. All the four cybercommunities – those concerned with the internal market, with law enforcement, diplomacy and defence – need to work more closely towards a shared awareness of threats. They should be ready to respond collectively when an attack materializes, so that the EU can be greater than the sum of its parts.

3. Research hypotheses

For modern society, a reliable energy infrastructure is essential. Electricity, gas, and oil are required not just for our daily activities, but also for the operation of key infrastructure such as transportation, telecommunications, healthcare, banking, and defence.

The European Union (EU) boasts one of the world's most stable electricity systems and a high level of energy security, thanks to its oil and gas reserves. However, a number of existing and emerging phenomena, particularly in the electrical industry, offer new threats to energy supply security.

As the energy system becomes more digitalized, hostile actors will have more opportunity to attack it, particularly through cyber-attacks, which might be combined with physical harm and social engineering. It also raises the possibility of unintentional disturbance. As a number of cases outside the EU have revealed, hackers are growing more adept and are already examining and exploiting vulnerabilities in the energy system.

Knowing that Much of the EU’s critical infrastructure is operated through industrial control systems (ICS)173, the scope of cyber-attacks discovered in control Systems (ICS) has revealed the level of sophistication Industrial Con of attackers[12].

The smart grid interconnection with the Internet exposes the grid to new types of risks, including Advanced Persistent Threats (APT), Distributed-Denial-of-Service (DDoS), botnets and zero-days. Stuxnet, Duqu, Red October, or Black Energy are just few examples of modern threats that appeared since 2010 [13].

The Cyber-physical systems (CPS) are prone to cyber-attacks on their data management and network layer as occurred in the cyber-attacks on Ukraine power distribution companies ,German steel mill , Maroochy water breach and various other industrial security incidents based on BlackEnergy and Stuxnet [14]

As for market security, most deregulated electricity markets consist of a day-ahead market and a real-time market. In the day-ahead market, the load is forecasted, and an optimization problem is solved to minimize the cost. The optimization problem’s outcome would be the predicted power generated at each bus (economic dispatch), which is used to define the locational marginal price (LMP) at each bus. The LMP is the buy/sell cost of power at different locations within electricity markets. Since False Data Injection FDI cyber-attacks can affect load forecasting, the day-ahead market is vulnerable to such attacks [15].

The real-time market uses the state estimation to estimate the power generated and power load at each bus, which is used to calculate the power flow through each line (for instance, optimal power flow can be used). Based on each line’s calculated power, the congestion pattern is achieved (if the estimated power in each line exceeds the maximum power limit, the line is congested). In the real-time market, real-time LMP is determined based on the calculated power. It can be seen that the state estimation is involved in congestion pattern calculations and loads and generation estimation. Thus, the FDI cyber-attacks that change the estimated state has impacts on the real-time market[16][17]

Other important services that rely on power may be harmed as a result of the outage. An insurance company, for example, has projected that a malware attack on power facilities in the north-eastern United States might result in economic damages of roughly USD 250 billion as a result of the consequences. Direct damage to assets and infrastructure, a drop in sales revenue for energy supply firms, a loss of sales revenue for businesses, and supply chain disruption are just a few examples. (Cyberattacks on London's power infrastructure may cost between GBP 21 and GBP 111 million per day.

Because of real-time requirements, a mix of advanced and legacy technologies, and the cascading effects of disruptions. The cybersecurity of the energy system, particularly the electricity grid, requires a dedicated sectoral approach. Experts believe there is a rising need for greater knowledge and information exchange, standardisation and certification, cybersecurity skill development, and legislation.

4. Methodology (description of collected data)

This research was conducted based on a detailed and systematic analysis of all available reference documentation communicated through the EU commission's official website, press releases, academic review papers and reports.

Existing Europe's cybersecurity legislation which outlines the framework for EU action to protect EU citizens and businesses from cyber threats, promote secure information systems and protect a global, open, free, and secure cyberspace has been collected, examined and summarized. In order to provide an overview of the EU's complex cybersecurity policy landscape and identify the main challenges to effective policy delivery.

We relied basically on a documentary review of publicly available information in official documents, position papers and third-party studies. In addition to screening the policy intervention incentives that promoted the progress made by the EU, we also accompanied this output with a brief reflection on the technological challenges and anticipated security gaps in the energy sector.

5. Results

NIS Directive

The first EU-wide legislation on cybersecurity, the Directive on Security of Network and Information Systems (the 'NIS Directive'), entered into force in 2016 after 3 years of negotiations. It marked a step change in cybersecurity as for the first time a common approach to increase the level of security of network and information systems across the Union was established. This law therefore constitutes the primary anchor for the EU cybersecurity architecture [18].

The objective of the Directive is to achieve evenly high level of security of network and information systems across the EU, through:

- Improved cybersecurity capabilities at national level;
- Increased EU-level cooperation;
- Risk management and incident reporting obligations for operators of essential services and digital service providers.

A challenge that applies to all stakeholders is to understand the overlap between legislations and consistently apply it throughout the Union. While the General Data Protection Regulation (GDPR) focuses on the rights of the data subjects and the obligations of relevant actors in processing activities, the NIS Directive concerns the national critical infrastructure of Member States and focuses on the main economic sectors.

The first challenge of the NIS Directive is that this is the first complete effort of the European Union to harmonise the cyber-security of critical infrastructure by increasing the common level of security in all Member State.

To date 25 EU Member States have notified full transposition of the Directive (all apart from LU-BE-HU). Prima facie checks have not revealed major gaps in the national transposition. The Directive requires Member States to get equipped with at least a minimum set of capabilities (a national strategy, national competent authority/ies, a national Computer Security Incident Response Team/ CSIRT). It also requires Member States to ensure that operators in critical sectors, as well as digital service providers, take appropriate security measures and notify significant incidents affecting their network and information systems to the national authorities.

In addition, Member States benefit from the work of the two cooperation fora established by the Directive, the NIS Cooperation Group (The Group) and the network of national Computer Security Incident Response Teams (CSIRTs Network)[19].

The CSIRTs Network provides a forum where members can cooperate, exchange information and build trust. Members will be able to improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents.

As part of the cybersecurity package adopted in September 2017, the Commission issued the Communication "Making the Most of the Directive on Security of Network and Information Systems" to assist Member States with guidance and best practice examples as well as to ensure a harmonised transposition of the new rules [20] .

After the entry into force of the NIS Directive, the European institutions have continued their legislative efforts on the security of networks and information systems through the European Commission’s priority to present to the European legislators a comprehensive package of measures to strengthen cyber security in the European Union.

One of the most important measures consists of a proposal for a Regulation which aims to create a European framework for the certification of cyber security of ICT products and digital services, as well as to strengthen the role of the European Agency for Network and Information Security (“ENISA”): the so-called Cybersecurity Act[21].

The Cybersecurity Act, which came into force in June 2019, can be divided into two parts: in the first part, the role and mandate of ENISA are specified, whilst, in the second part, a European system of certification of the cybersecurity of devices connected to the Internet and other digital products and services is introduced. Since this is a regulation, once adopted and entered into force, the Cybersecurity Act will be immediately applicable in all Member States, as was the case for the GDPR.

More precisely, the Cybersecurity Act introduces an EU wide ICT security certification system for digital products and services. This specific objective will attempt to solve the problem of the numerous existing certification schemes in some Member States but not recognized in other Member States. The Cybersecurity Act will provide an overall framework with a set of rules that will govern the European ICT certification schemes for specific categories of products and services – to ensure that those future certification schemes will be validly recognized in all Member States of Europe[21].

Under this mandate, ENISA could perform functions to support the internal market and cover a cybersecurity ‘market observatory’ to analyse the trends of the cybersecurity market and then reflect that in the EU policy development in the ICT standardization[21].

ENISA would also be involved in the EU Cybersecurity Blueprint, in order to coordinate responses to large-scale cross-border cybersecurity incidents and crises at the EU level. This blueprint will be applicable only to cybersecurity incidents with extensive effects on two or more Member States and with political significance on the EU political level[21].

Latest updates and regulations

In December 2020, the European Commission and the European External Action Service (EEAS) presented a new EU cybersecurity strategy. The aim of this strategy is to strengthen Europe’s resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The new strategy contains concrete proposals for deploying regulatory, investment and policy instruments.

On 22 March 2021, the Council adopted conclusions on the cybersecurity strategy, underlining that cybersecurity is essential for building a resilient, green and digital Europe. EU ministers set as a key objective achieving strategic autonomy while preserving an open economy. This includes reinforcing the ability to make autonomous choices in the area of cybersecurity, with the aim to strengthen the EU's digital leadership and strategic capacities.[1]

The strategy covers the security of essential services such as hospitals, energy grids, railways and the ever-increasing number of connected objects in our homes, offices and factories. The strategy aims to build collective capabilities to respond to major cyberattacks. It also outlines plans to work with partners around the world to ensure international security and stability in cyberspace. Moreover, it outlines how a Joint Cyber Unit can ensure the most effective response to cyber threats using the collective resources and expertise available to Member States and the EU[22].

The EU is committed to supporting this strategy through an unprecedented level of investment in the EU's digital transition over the next seven years. This would quadruple previous levels of investment. It demonstrates the EU’s commitment to its new technological and industrial policy and the recovery agenda [22]

The Recommendation on the Establishment of a Joint Cyber Unit is a critical step in completing the European cybersecurity crisis management architecture. It contributes to a secure digital economy and society as a concrete deliverable of the EU Cybersecurity Strategy and the EU Security Union Strategy.

The Joint Cyber Unit proposed today intends to pool the EU's and Member States' resources and skills in order to effectively prevent, deter, and respond to large-scale cyber incidents and crises. Too often, cybersecurity communities, such as civilian, law enforcement, diplomatic, and cyber defence communities, as well as corporate sector partners, work in silos. They will have a virtual and physical platform of cooperation with the Joint Cyber Unit: relevant EU institutions, authorities, and agencies, in collaboration with Member States, will gradually develop a European platform for solidarity and help in the face of large-scale cyberattacks.

The following table provides a detailed timeline for all measures taken by the Eu council concerning the cybersecurity legislations.

Date	Measure	Description
9/06/2016	Council agrees on next steps to fight criminal activities in cyberspace	The EU justice ministers examined ways to improve criminal justice in cyberspace in greater depth. They agreed on two sets of conclusions, one of which outlines specific steps to increase cooperation and the other of which includes a deadline for further action[23]. • Conclusions on improving criminal justice in cyberspace. • Conclusions on the European judicial cybercrime network.
24/10/2017	EU ministers agree on cybersecurity action plan	The Council agreed to create an action plan for EU cybersecurity reform. Ministers emphasized the importance of cyber security for European residents and enterprises[24].
20/12/2017	EU institutions strengthen cooperation to counter cyber-attacks	In the fight against cyber-attacks, EU institutions have taken a significant step forward in their cooperation. A permanent Computer Emergency Response Team (CERT-EU) covering all EU institutions, bodies, and agencies was established through an inter-institutional agreement. CERT-EU will ensure that the EU's reaction to cyber-attacks on its institutions is synchronized[25].
16/04/2018	Malicious cyber activities: Council adopts conclusions	The Council approved conclusions on hostile cyber actions, emphasizing the significance of a global, open, free, stable, and secure cyberspace that fully respects human rights and basic freedoms, as well as the rule of law. The Council voiced grave concern regarding non-EU states and non-state actors' enhanced capabilities and willingness to pursue their goals through destructive cyber actions. The EU will continue to improve its cyber-security capabilities[26].
13/09/2018	Cybersecurity Act: Council starts negotiations with European Parliament	The Council and the European Parliament have begun talks with the goal of obtaining an agreement on the Cybersecurity Act by the end of the year. On the 8th of June, a general approach to this proposition was agreed. By establishing an EU-wide certification structure for ICT products, services, and procedures, the Cybersecurity Act aims to improve cyber resilience. The current EU Agency for Network and Information Security would also be upgraded (ENISA)[27].
18/10/2018	European Council calls for measures to build strong cybersecurity in the EU	EU leaders have asked for the EU's deterrence, resilience, and reaction to hybrid, cyber, and chemical, biological, radiological, and nuclear (CBRN) threats to be strengthened further. They did so in response to cyber-attacks on The Hague-based Organisation for the Prohibition of Chemical Weapons (OPCW).

		The European Council also demanded that all cybersecurity recommendations be finalized "before the end of the legislative session" - in April 2019[28].
19/11/2018	Cyber defense: Council updates policy framework	In order to boost their cyber defense capabilities, EU member states are actively cooperating. The Council adopted an enhanced version of the EU cyber defense policy framework to achieve this goal. Since the initial framework was adopted in 2014, the update allows the EU to take into account changing security challenges. It defines priority areas for cyber defense and explains who is responsible for what. The European Council, at its most recent meeting on October 18, 2018, advocated for measures to strengthen cybersecurity in the EU. Restrictive measures capable of responding to and deterring cyber-attacks were specifically mentioned by EU leaders[29].
19/12/2018	Cybersecurity Act: EU ambassadors approve proposed regulation	With the passage of the proposed Cybersecurity Act, the European Union will be able to implement an EU-wide cybersecurity certification program and establish a permanent EU cybersecurity agency. On December 10, the presidency and the European Parliament reached a provisional agreement on the new law. Consumers will soon have access to EU-wide cybersecurity certification for Internet-connected devices, allowing them to make better informed decisions and making it easier for businesses to advertise their smart products across Europe[30].
13/03/2019	Pooling cybersecurity expertise: Council to start negotiations with European Parliament	The Council presidency was given permission by EU ambassadors to begin discussions with the European Parliament about pooling cybersecurity knowledge. The focus of the talks will be on two projects: building the European Cybersecurity Industrial, Technology and Research Centre, a top-tier knowledge source for cybersecurity; and establishing a network of national coordination centers[31].
9/04/2019	Council adopts Cybersecurity Act	The Council adopted the rule known as the Cybersecurity Act on April 9, 2019, which introduces: a set of certification processes that operate across the EU The current European Union Agency for Network and Information Security will be replaced with an EU cybersecurity agency (ENISA).
17/05/2019	Cyber-attacks: Council is now able to impose sanctions	The Council developed a framework that enables the EU to apply targeted restrictive measures in order to discourage and respond to cyber-attacks that represent a threat to the EU or its member states from the outside. For the first time, this ruling permits the EU to penalise individuals or entities who:

		are involved in other ways are responsible for cyber-attacks or attempted cyber-attacks give financial, technical, or material support for such attacks Sanctions may also be levied on those who are connected to them. This framework also applies to cyber-attacks against non-EU countries or international organizations where restrictive measures are deemed necessary to meet the Common Foreign and Security Policy's objectives (CFSP)[32].
03/12/2019	Significance and security risks of 5G technology: Council adopts conclusions	The ramifications on the European economy and the need to address security concerns were discussed in the Council's 5G conclusions. The EU ministers emphasized that 5G networks will be critical infrastructure for the continued operation of critical societal and economic services [33].
5/06/2020	Mandate on cybersecurity centers and state of play of 5G networks	A fresh mandate for discussions with the European Parliament on the proposed regulation has been agreed creating the European Cybersecurity Competence Centre and the Network of Coordination Centers on June 3, 2020. The Croatian presidency will then contact the Parliament's chief negotiator to discuss the idea of holding a trilogue meeting. The presidency also discussed the status of the EU toolbox for 5G network security implementation[34].
9/06/2020	Council conclusions: shaping Europe's digital future	The Council accepted conclusions on a wide variety of problems linked to the EU digital strategy's implementation. The essay emphasizes the importance of digital transformation in combating the pandemic and in the post-COVID-19 recovery. In terms of cybersecurity, EU ministers want to increase the EU's response capabilities and ensure the integrity, security, and resilience of digital infrastructure, communication networks, and services as cyber threats and crimes grow in number and sophistication. The EU also believes that a coordinated strategy is necessary to avoid cybersecurity threats and ensure a secure 5G deployment[35].
30/07/2020	EU imposes the first ever sanctions against cyber-attacks	Six persons and three entities were found to be culpable for or participating in numerous cyber-attacks, and the Council decided to impose restrictive measures against them. The measures include a travel ban and an asset freeze, as well as a prohibition on EU persons and businesses making cash accessible to anyone on the list[36].
2/12/2020	Cybersecurity of connected devices – Council adopts conclusions	The Council accepted conclusions that acknowledge the expanding usage of internet-connected consumer and industrial items, as well as the additional risks to privacy, information security, and cybersecurity that this poses. The findings emphasize the need of determining the long-term need for horizontal legislation to handle all essential aspects of connected device cybersecurity, including as availability, integrity, and confidentiality.

		The Internet of Things (IoT), which consists of machines, sensors, and networks, will play a critical role in creating Europe's digital future, as will their security[37].
9/12/2020	Bucharest will host the seat of the new European Cybersecurity Competence Centre	Representatives from the governments of EU member states chose Bucharest (Romania) as the potential home of the new European Cybersecurity Industrial, Technology, and Research Competence Centre. The Cybersecurity Competence Centre will strengthen the EU's coordination of cybersecurity research and innovation. It will also be the EU's primary tool for pooling funds for cybersecurity research, technology, and industrial development[38].
11/12/2020	Provisional agreement on the EU Cybersecurity Competence Centre	Representatives from the governments of EU member states chose Bucharest (Romania) as the potential home of the new European Cybersecurity Industrial, Technology, and Research Competence Centre. The Cybersecurity Competence Centre will strengthen the EU's coordination of cybersecurity research and innovation. It will also be the EU's primary tool for pooling funds for cybersecurity research, technology, and industrial development[39].
15/12/2020	Council calls for strengthening resilience and countering hybrid threats, including disinformation	The Council adopted conclusions that urge for more robust EU responses to hybrid threats, such as disinformation, as well as increased resilience. New technologies and crises, such as the current epidemic, provide possibilities for hostile actors to expand their interference efforts, according to the Council. Apart from the crisis itself, these present an extra difficulty for member states and EU institutions. The EU and its member states are more vulnerable to hybrid threats as a result of the COVID-19 pandemic, according to the Council. Increased disinformation dissemination and manipulative interference are examples of such threats. To combat such dangers, which include hostile cyber activity, disinformation, and threats to economic security, a comprehensive approach combining effective cooperation and coordination is required[40].
22/03/2021	Council adopts conclusions on the EU's cybersecurity strategy	Conclusions on the EU's cybersecurity policy for the digital decade were accepted by the Council. The European Commission and the EU High Representative for Foreign Affairs and Security Policy presented this plan in December 2020. It lays forth the foundation for EU action to protect EU individuals and enterprises from cyber threats, promote secure information systems, and safeguard a global, open, free, and secure cyberspace. Security is critical for establishing a resilient, green, and digital Europe, according to the results. They made obtaining strategic autonomy while maintaining an open economy a priority. This involves bolstering the EU's ability to make autonomous cybersecurity decisions, with the goal of bolstering the EU's digital leadership and strategic capabilities[41].

20/04/2021	Bucharest-based Cybersecurity Competence Centre gets green light from Council	The EU plans to build a Cybersecurity Competence Centre to aggregate investment in cybersecurity research, technology, and industrial development in order to improve the security of the internet and other vital network and information systems. The new entity, which will be based in Bucharest, Romania, will channel cybersecurity funds from Horizon Europe and the Digital Europe Program, among other things. This "European Cybersecurity Industrial, Technology, and Research Competence Centre" will collaborate with a network of national coordinating centers established by member states. On April 20, 2021, the Council approved the regulation establishing the Centre and network. The European Parliament will then vote on the final version[42].
29/04/2021	Combating child abuse online – informal deal with European Parliament on temporary rules	Negotiators from the European Council and the European Parliament have reached a provisional agreement on a temporary measure that will allow providers of electronic communications services such as web-based email and messaging services to detect, remove, and report child sexual abuse online, as well as anti-grooming, until permanent legislation announced by the European Commission is in place. The accord calls for a derogation from the ePrivacy directive's provisions 5(1) and 6(1), and it must be approved by the Council[43].
17/05/2021	Cyberattacks: Council prolongs framework for sanctions for another year	The Council has voted to extend the framework for restrictive measures against cyberattacks that pose a threat to the EU or its member states for another year, until May 18, 2022. This framework enables the EU to impose targeted restrictive measures on individuals or businesses involved in cyberattacks that have a major impact and pose a threat to the EU or its member states from the outside. Restrictive measures can also be applied in response to cyberattacks against foreign countries or international organizations if they are deemed necessary to fulfill the Common Foreign and Security Policy's objectives (CFSP)[44][45].
19/10/2021	Council adopts conclusions on exploring the potential of a joint cyber unit	The Council adopted conclusions calling on the EU and member states to improve the EU's cybersecurity crisis management system, notably by looking into the possibility of forming a combined cyber unit. The Council emphasizes the importance of consolidating existing networks and creating a map of potential information sharing gaps and needs inside and beyond cyber communities in its recommendations. Following that, an agreement on the major aims and priorities of a proposed combined cyber unit should be reached[46].
3/12/2021	Council agrees its position on new cybersecurity directive	EU ministers accepted a "general approach" on measures for a high shared level of cybersecurity across the EU during the December

		Telecommunications Council, as part of the so-called "NIS2" directive. The legislation's goal is to increase the public and commercial sectors' resilience and crisis response capabilities, as well as the EU's overall. Its goal is to eliminate disparities between member states' cybersecurity standards and implementation of cybersecurity measures[47][48].
8-9/03/2022	EU ministers united in strengthening cyber resilience in the EU	EU ministers responsible for telecommunications and digital affairs met on 8 and 9 March 2022 at an informal meeting organized by the French presidency of the Council. Ministers called for bolstering and accelerating the pace of European cooperation in the area of cybersecurity, following an increase in cyber threat levels, worsened by the situation in Ukraine and the risk of cyber incidents within the EU. They also called for more information on risks threatening European communications networks and infrastructure, and for recommendations on how to strengthen their resilience. The 27 ministers adopted a political declaration intended to boost the EU’s cybersecurity capabilities[48].

Concerning the energy sector:

As industry continues to digitise (often referred to as "Industry 4.0"), a large-scale incident in one industrial area may have ramifications in other industries. Cybersecurity and the difficulties it poses are rapidly growing, which is why the European Commission has taken a number of steps to address them. The construction of a comprehensive legislative framework that builds on existing legislation is one of the most important of these.

In April 2019, the Commission adopted sector-specific recommendations to promote awareness and readiness in the energy industry. This advice, which comes in the form of a Recommendation and a staff working paper, assists in the implementation of horizontal cybersecurity rules.

Furthermore, the Clean Energy for All Europeans package, which was agreed in 2019, would aid in the transformation of Europe's energy systems while maintaining a high degree of security, not least in terms of reinforcing cybersecurity in the energy sector.

According to the Special Eurobarometer, conducted in 2019, 86 percent of EU citizens agree that increased cybersecurity cooperation in the energy sector across EU countries is needed to provide access to secure electricity.

The ambitious EU Security Union Strategy, unveiled in July 2020, intends to maintain European security in both the physical and digital worlds, across all sectors of society. Recognizing the need for sector-specific measures, particularly in the energy sector, the strategy describes a future project to improve the resilience of vital energy infrastructure against physical, cyber, and hybrid threats. This will ensure that energy companies compete on an equal footing across borders.

Despite the fact that there is a comprehensive overall regulatory framework for cybersecurity, the energy sector has some unique characteristics that necessitate special attention[49]:

- Real-time requirements: Some energy systems must react so quickly that typical security procedures, such as command authentication or digital signature verification, are simply not feasible due to the time required to implement them.
- Cascading effects: Across Europe the energy trading infrastructure as in electricity grid and gas pipelines are deeply interconnected, so an outage happening in one country could be transmitted triggering blackouts or shortages of supply in other areas and countries. (ENISA) has emphasised the significance of mapping the reciprocal dependencies of crucial sectors. This is critical for determining the extent of an incident's potential spread and ensuring well-coordinated responses.
- Combined legacy systems with new technologies: Many aspects of the energy system were conceived and constructed long before cybersecurity was a factor. This heritage must now interact with cutting-edge automation and control equipment, such as smart metres and connected appliances, as well as gadgets from the 'Internet of Things,' without being vulnerable to cyber-threats.

The Risk Preparedness Regulation requires EU countries to include cybersecurity measures in their national risk assessment plans, while the Energy Regulation requires the Commission to design a network code for cross-border electricity flow cybersecurity. The Smart Grids Task Force Expert Group 2 published recommendations on the regulation's implementation in 2019. Furthermore, the Agency for the Cooperation of Energy Regulators (ACER) has been asked to contribute to the development and acceptance of the code set for 2022.

The Commission also established a drafting committee of relevant parties in February 2020 to carry out preliminary work on the network code. The project culminated in a technical report that included suggestions to the Commission as well as issues that needed to be addressed. in particular:

- Cross-border cyber risk assessment and management
- ISO/IEC 27001 certification or proof of equivalence
- common functional and non-functional security controls and requirements
- an assurance scheme and information sharing

The collaboration in cybersecurity aspects requires a shared trust across stakeholders and EU countries taking into consideration potential cascading and cross-border repercussions. To that purpose, the Commission is working to increase awareness and stimulate broad talks in the energy sector. It has organised three major events on energy cybersecurity in Brussels in October 2018 and July 2019. The European Energy–Information Sharing Analysis Centre (EE-ISAC), which helps utilities strengthen the cybersecurity and resilience of their grid by facilitating trust-based data and information sharing, also collaborates with the Commission.

6. Discussion and Conclusions

The European Commission is laying out a plan to create a new Joint Cyber Unit to combat the escalating number of significant cyber events affecting public services, enterprises, and citizens throughout the EU. As cyberattacks rise in quantity, scale, and consequences, advanced and coordinated responses in the field of cybersecurity have become increasingly required, posing a serious threat to our security. All relevant EU actors must be ready to respond collectively and disclose pertinent information based on a 'need to share' rather than a 'need to know' premise.

Governments, utilities, and other stakeholders in the power value chain must be proactive in their search for solutions that can adapt to changing cyberthreats. It will be vital to maintain a long-term commitment to cooperation and partnership.

Smart application functionalities are not clearly framed in official norms that usually define and impose quantifying criteria in terms of technical specifications. This is why working and elaborating on the standardization enclosure, especially for the most affiliated pieces of the smart grid, becomes an urgent need.

Coordination between Member States is vital in order for Member States to be compliant with the NIS Directive. This requires not only cooperation nationally between the single point of contact of each Member State and the CSIRTs but also among Member States' governments and enforcement agencies.

The cooperation is expected on many levels: firstly, between the CSIRTs, which will create a CSIRTs network to effectively exchange information and support one another, but also between national competent authorities that need to assess the compliance of operations of essential services.

Lastly, the legal instrument utilised by the European Union legislators - a Directive, means that even though it is a legally binding act, it requires each Member State to implement the set of objectives and further specifications in its national legislation. Unavoidably, this represents a further level of difficulty in the harmonisation of a high common level of security of network and information systems across the European Union.

There is a need for a more coordinated approach to crisis response so that Member States promptly share relevant critical information with each other and also alignment and consistency of messages to the public takes place resulting in containment of the damaging impacts of cyber-attacks.

In conclusion, there is no simple response to such questions: the NIS Directive is viewed as a baseline for critical infrastructure cyber security, with a focus on measures such as the establishment of CSIRTs inside Member States and coordination through a CSIRT network. Any additional law or legislation should clearly build on and complement the frameworks created by the NIS Directive and GDPR to the greatest extent practicable.

7. References

[1] "Cybersecurity: how the EU tackles cyber threats - Consilium." https://www.consilium.europa.eu/en/policies/cybersecurity/?utm_source=linkedin.com&utm_medium=social&utm_campaign=2021-03-22-cybersec&utm_content=vignette (accessed Mar. 25, 2021).

[2] A. Dagoumas, "Assessing the Impact of Cybersecurity Attacks on Power Systems," *Energies*, vol. 12, no. 4, p. 725, 2019, doi: 10.3390/en12040725.

[3] V. Smart and G. Cybersecurity, "Guidelines for smart grid cybersecurity," vol. 1, 2014, doi: 10.6028/NIST.IR.7628r1.

[4] P. Arsene, "Smart Energy Grids," no. September, pp. 1–10, 2011.

[5] "Better energy efficiency policy with digital tools – Analysis - IEA." https://www.iea.org/articles/better-energy-efficiency-policy-with-digital-tools (accessed Mar. 31, 2022).

[6] “The History of Making the Grid Smart - Engineering and Technology History Wiki.” https://ethw.org/The_History_of_Making_the_Grid_Smart (accessed Jun. 18, 2020).

[7] N. Uribe-Pérez, L. Hernández, D. de la Vega, and I. Angulo, “State of the Art and Trends Review of Smart Metering in Electricity Grids,” *Appl. Sci.*, vol. 6, no. 3, pp. 1–24, 2016, doi: 10.3390/app6030068.

[8] “Home — ESMIG.” https://www.esmig.eu/ (accessed Mar. 30, 2022).

[9] D. Tellbach and Y. F. Li, “Cyber-attacks on smart meters in household nanogrid: Modeling, simulation and analysis,” *Energies*, vol. 11, no. 2, 2018, doi: 10.3390/en11020316.

[10] Y. S. Patil and S. V Sankpal, “Multi-Player Attack Detection Model for Smart Meter Security in Smart Grid Systems,” *Int. J. Appl. Eng.*, vol. 14, no. 7, pp. 1488–1492, 2019.

[11] D. B. Avancini, J. J. P. C. Rodrigues, S. G. B. Martins, R. A. L. Rabêlo, J. Al-Muhtadi, and P. Solic, “Energy meters evolution in smart grids: A review,” *J. Clean. Prod.*, vol. 217, pp. 702–715, 2019, doi: 10.1016/j.jclepro.2019.01.229.

[12] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014, doi: 10.1109/TSG.2014.2298195.

[13] R. Leszczyna, “Standards on cyber security assessment of smart grid,” *Int. J. Crit. Infrastruct. Prot.*, vol. 22, no. September, pp. 70–89, 2018, doi: 10.1016/j.ijcip.2018.05.006.

[14] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, “STRIDE-based threat modeling for cyber-physical systems,” in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2017 - Proceedings*, 2017, vol. 2018-Janua, pp. 1–6. doi: 10.1109/ISGTEurope.2017.8260283.

[15] F. Nejabatkhah, Y. W. Li, H. Liang, and R. R. Ahrabi, “Cyber-Security of Smart Microgrids : A Survey,” 2021.

[16] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011, doi: 10.1109/TSG.2011.2163807.

[17] P. Li, Y. Liu, H. Xin, and X. Jiang, “A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant under Cyber-Attacks,” *IEEE Trans. Ind. Informatics*, vol. 14, no. 10, pp. 4343–4352, 2018, doi: 10.1109/TII.2017.2788868.

[18] “The NIS Directive | Cyberwatching.” https://www.cyberwatching.eu/policy-landscape/cybersecurity/nis-directive-and-its-challenges (accessed Jul. 13, 2021).

[19] “Netztransparenz > EEG > EEG-Umlagen-Übersicht.” https://www.netztransparenz.de/EEG/EEG-Umlagen-Uebersicht (accessed Mar. 20, 2022).

[20] European Commission, “Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union,” Brussels, Oct. 2017.

[21] “EU Cybersecurity Act | Cyberwatching.” https://www.cyberwatching.eu/policy-landscape/cybersecurity/eu-cybersecurity-act (accessed Jul. 14, 2021).

[22] “The Cybersecurity Strategy | Shaping Europe’s digital future.”

https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy (accessed Mar. 25, 2021).

[23] C. of the E. P. Release, “Fight against criminal activities in cyberspace : Council agrees on practical measures and next steps - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2016/06/09/criminal-activities-cyberspace/ (accessed Mar. 31, 2022).

[24] C. of the EU, “Transport, Telecommunications and Energy Council, 24/10/2017 - Consilium.” https://www.consilium.europa.eu/en/meetings/tte/2017/10/24/ (accessed Mar. 31, 2022).

[25] G. S. P. Release, “Cybersecurity: EU institutions strengthen cooperation to counter cyber-attacks - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2017/12/20/cybersecurity-eu-institutions-strengthen-cooperation-to-counter-cyber-attacks/ (accessed Mar. 31, 2022).

[26] C. of the E. P. Release, “Response to malicious cyber activities: Council adopts conclusions - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/ (accessed Mar. 31, 2022).

[27] C. of the E. P. Release, “EU to create a common cybersecurity certification framework and beef up its agency – Council agrees its position - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/ (accessed Mar. 31, 2022).

[28] E. Council, “European Council, 18/10/2018 - Consilium.” https://www.consilium.europa.eu/en/meetings/european-council/2018/10/18/ (accessed Mar. 31, 2022).

[29] Council of the EU Press release, “Cyber defence: Council updates policy framework - Consilium.” Accessed: Mar. 31, 2022. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/

[30] C. of the E. P. Release, “EU to become more cyber-proof as Council backs deal on common certification and beefed-up agency - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/ (accessed Mar. 31, 2022).

[31] C. of the E. P. Release, “EU to pool and network its cybersecurity expertise – Council agrees its position on cybersecurity centres - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/ (accessed Mar. 31, 2022).

[32] Council of the EU Press release, “Cyber-attacks: Council is now able to impose sanctions - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/ (accessed Mar. 31, 2022).

[33] “Significance and security risks of 5G technology – Council adopts conclusions - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/ (accessed Mar. 31, 2022).

[34] Council of the EU, “Video conference of telecommunications ministers - Consilium.” https://www.consilium.europa.eu/en/meetings/tte/2020/06/05/ (accessed Mar. 31, 2022).

[35] C. of the E. P. Release, “Shaping Europe’s digital future - Council adopts conclusions - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2020/06/09/shaping-europe-s-digital-future-council-adopts-conclusions/ (accessed Mar. 31, 2022).

[36] “EU imposes the first ever sanctions against cyber-attacks - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ (accessed Mar. 31, 2022).

[37] C. of the E. P. Release, “Cybersecurity of connected devices – Council adopts conclusions - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/ (accessed Mar. 31, 2022).

[38] C. of the E. P. Release, “How the seat of the Cybersecurity Industrial, Technology and Research Competence Centre will be selected - Consilium.” https://www.consilium.europa.eu/en/infographics/seat-selection-cybersecurity-centre/ (accessed Mar. 31, 2022).

[39] C. of the EU, “New Cybersecurity Competence Centre and network: informal agreement with the European Parliament - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/ (accessed Mar. 31, 2022).

[40] Council of the EU Press release, “Council calls for strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/ (accessed Mar. 31, 2022).

[41] C. of the E. P. Release, “Cybersecurity: Council adopts conclusions on the EU’s cybersecurity strategy - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/ (accessed Mar. 31, 2022).

[42] C. of the EU, “Bucharest-based Cybersecurity Competence Centre gets green light from Council - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/ (accessed Mar. 31, 2022).

[43] C. of the E. P. Release, “Combating child abuse online – informal deal with European Parliament on temporary rules - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2021/04/29/combating-child-abuse-online-informal-deal-with-european-parliament-on-temporary-rules/ (accessed Mar. 31, 2022).

[44] C. of the E. P. Release, “Cyber-attacks: Council prolongs framework for sanctions for another year - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/ (accessed Mar. 31, 2022).

[45] Council of the EU Press release, “Sanctions: how and when the EU adopts restrictive measures - Consilium.” https://www.consilium.europa.eu/en/policies/sanctions/

(accessed Mar. 31, 2022).

[46] C. of the E. P. Release, “Cybersecurity: Council adopts conclusions on exploring the potential of a joint cyber unit - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2021/10/19/cybersecurity-council-adopts-conclusions-on-exploring-the-potential-of-a-joint-cyber-unit/ (accessed Mar. 31, 2022).

[47] C. of the E. P. Release, “Strengthening EU-wide cybersecurity and resilience – Council agrees its position - Consilium.” https://www.consilium.europa.eu/en/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/ (accessed Mar. 31, 2022).

[48] C. of the EU, “Transport, Telecommunications and Energy Council (Telecommunications) - Consilium.” https://www.consilium.europa.eu/en/meetings/tte/2021/12/03/ (accessed Mar. 31, 2022).

[49] “Critical infrastructure and cybersecurity.” https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en (accessed Apr. 12, 2022).

[50] F. Hasse, A. Von Perfall, T. Hillebrand, E. Smole, and M. Lay, L., & Charlet, “Blockchain – an opportunity for energy producers and consumers.,” 2016. [Online]. Available: www.pwc.com/utilities