【欧州】【Common】

Common - Policies in the use of IoT, Cybersecurity: The European Commission presents proposals for improving cybersecurity and resilience of critical entities including transport infrastructure

Andrea Antolini　Former Researcher JTTRI

【概要：Summary】

Critical infrastructures (CI) of national and European importance, including transport infrastructures, electricity generation plants and others need to be better protected against an increasing number of cyber threats, cyberattacks or hybrid attacks. Since cyberthreats are almost always cross-border, a cyberattack on critical facilities in one country can affect the EU as a whole. Therefore, the EU Member States need to prepare for improving their cybersecurity and they should improve their cooperation with counterparts in other EU Member States by sharing information.

Regarding the transport system, the increasing digitalization has made it more vulnerable to cyber risks. Accordingly, in order to improve the transport sector's cybersecurity, the EU works on a number of measures to make the system more resilient to cyber risks.

The EU has now legal instruments to improve the protection of electronic communications networks and the cybersecurity of CI. Furthermore, the EU Agency for Cybersecurity (ENISA) has been working with the EU institutions on problems of the European cybersecurity and has the mandate to develop recommendations on good practice and to assist EU Member States in implementing EU legislation regarding cybersecurity.

Recently, in December 2020, the European Commission presented several proposals to improve the cybersecurity and resilience of critical infrastructures and critical entities. The Commission adopted a proposal for the revision of the European Critical Infrastructure Directive, and a revised Network and Information Systems Directive (NIS 2) as well as a new Cybersecurity Strategy.

【記事：Article】

1. The Cyber Security Act and ENISA's mandate to improve cybersecurity in the EU

Electronic communications networks and information and communications technology (ICT) and keep the key sectors of health, energy, finance and transport running. Since cyberattacks are constantly increasing and a connected economy and society is becoming more vulnerable to cyber threats and attacks, more measures have to be introduced against cyber threats and attacks. However, while cyberattacks often take place

across borders, the policy responses and measures by law enforcement authorities to improve cybersecurity are predominantly national.

In order to improve cybersecurity at European level, the Regulation (EU 2019/881) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) of 27 June 2019 establishes an EU cybersecurity certification framework for information and communication technology (ICT) products, services, and processes. The Cybersecurity Act (Regulation (EU) 2019/881) introduces, for the first time, EU wide rules for the cybersecurity certification of products, processes and services. It also requires EU Member States to determine penalties for cybersecurity certification violations, among others.

The EU Cybersecurity Act also strengthens the EU Agency for cybersecurity (ENISA). The EU Agency has been granted a permanent mandate with a list of new tasks. ENISA's main aim is to improve resilience of EU's CI against cyber threats and to develop recommendations on good practice and to assist EU Member States in implementing EU legislation on cybersecurity. ENISA also has a key role in setting up and maintaining the cybersecurity certification framework, among others. ENISA also aims to improve the resilience of the EU's information networks against cyber threats and attacks and to coordinate responses to large-scale cross-border cyber incidents.

2. The EU's new Cybersecurity Strategy

In the past years, the EU has implemented some legislative acts and initiatives to strengthen cybersecurity capacities to make Europe more cyberthreat-resilient. On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final). This strategy aims at improving the resilience against cyberattacks in transport, energy and health, telecommunications, finance, security, democratic processes, space and defence, because these are sectors, reliant on interconnected network and information systems. The Cybersecurity Strategy is expected to contribute to a cybersecure digital decade for the EU, to the achievement of a Security Union, and to the strengthening of the EU's position globally. The new Cybersecurity Strategy aims to safeguard a global and open Internet, and at the same time, it offers safeguards to ensure security and it protects European values and the fundamental rights of everyone.

The new Cybersecurity Strategy contains concrete proposals for deploying three principal areas of EU action, including, firstly, resilience, technological sovereignty and leadership; secondly, operational capacity to prevent, deter and respond; and thirdly, cooperation to advance a global and open cyberspace. The strategy aims at improving the resilience against cyber threats and ensures that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The new Cybersecurity Strategy focuses on shielding the connected devices, the electricity grid, banks, planes, public administrations and hospitals from cyber threats. Regarding resilience, technological sovereignty and leadership, the Commission proposes to reform the rules on the security of network and information systems, under a Directive on measures for high common level of cybersecurity across the EU. This revised NIS Directive or 'NIS 2 Directive' is intended to increase the level of cyber resilience of critical public and private sectors, including hospitals, energy grids, railways, but also data centres, public administrations, research labs and manufacturing of critical medical devices and medicines, as well as other critical

infrastructure and services. The Commission also proposes to launch a network of Security Operations Centres across the EU. Powered by artificial intelligence (AI), they should constitute a "cybersecurity shield" for the EU, able to detect signs of a cyberattack early enough and to enable proactive action, before damage occurs.

Regarding building operational capacity to prevent, deter and respond, the Commission is preparing, through a progressive and inclusive process with the Member States, a new Joint Cyber Unit, to strengthen cooperation between responsible EU bodies and Member State authorities. The High Representative puts forward proposals to strengthen the EU Cyber Diplomacy Toolbox to prevent, discourage, deter and respond effectively against malicious cyber activities, among others.

Regarding the cooperation to advance a global and open cyberspace, the EU will step up cooperation with international partners to strengthen the rules-based global order, promote international security and stability in cyberspace, among others. The EU will further strengthen its EU Cyber Diplomacy Toolbox and increase cyber capacity-building efforts to third countries. Cyber dialogues with third countries, regional and international organisations as well as the multi-stakeholder community will be intensified.

Regarding the cybersecurity of the 5G networks most EU Member States are already well on track of implementing the recommended mitigation measures. The coordinated work at EU level on 5G cybersecurity will continue, with the aim to complete the implementation of measures by the second quarter of 2021.

3. The revision of the European Critical Infrastructure (ECI) Directive: The Proposal for a Critical Entities Resilience (CER) Directive

In 2008, the EU introduced the "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" (ECI Directive). The ECI Directive 2008/114/EC applies to the energy and transport sectors and aims to enhance the protection of critical infrastructure in the EU. The Directive 2008/114/EC appears to be broadly consistent with relevant European sectoral legislation and policies at international level. It shows several complementarities and overlapping with other European legislation/policy documents in the energy, transport and ICT sectors.

However, because of the generality of some provisions and the different interpretations in EU Member States the Directive 2008/114/EC only partially achieved its objectives. The Directive's main weakness is its limited scope, covering only sectors of transport and energy. In view of recent technological, economic, social, policy/political and environmental developments and considering the new and evolving challenges in protecting Critical Infrastructure, the ECI Directive needed to be revised as a central pillar of the European Programme for Critical Infrastructure Protection (CIP).

The evaluation indicated that the focus needed to be shifted away from asset protection to a more system-oriented protection, which recognises interdependencies across a range of different sectors. Therefore, on 16 December 2020, the European Commission presented a proposal for a revision of the European Critical Infrastructure Directive 2008/114/EC. By presenting the "Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities" (COM(2020) 829 final), the Critical Entities Resilience (CER) Directive, the Commission intends to create a comprehensive framework to support EU Member States in ensuring that the critical entities are able to prevent, resist, absorb and recover from all disruptive

incidents. The proposal covers ten sectors, namely energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration and space. The provisions include, among others, the Member States' obligation to have in place a strategy for identifying critical entities and ensuring their resilience and to carry out a national risk assessment accordingly. Critical entities would be required to carry out risk assessments of their own, take appropriate technical and organisational measures in order to boost resilience, and report incidents to the national authorities.

Furthermore, critical entities providing services to or in at least one-third of Member States would be subject to specific oversight, including advisory missions organised by the European Commission. The Commission would offer different forms of support to Member States and critical entities, a Union-level risk overview, best practices, methodologies, cross-border training activities and exercises to test the resilience of critical entities.

The Directive on the resilience of critical entities (COM(2020) 829 final) as proposed by the Commission in December 2020 will be considered in the Council and in the European Parliament.

4. The Commission proposal for a NIS 2 Directive on measures for high cybersecurity

In 2016, the EU adopted the first legislative act in the area of cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). The NIS Directive puts in place requirements concerning national capabilities in the area of cybersecurity. It also introduced obligations concerning security measures and incident notifications across sectors, including the transport sector. The NIS Directive represents the cornerstone of the EU's efforts to step up its overall cybersecurity. A key role was attributed to ENISA in supporting the implementation of this NIS Directive. After the Directive's entry into force, the European institutions have continued their legislative efforts on the security of networks and information systems. In spite of its notable achievements, the NIS Directive had also some limitations and the situation has changed due to the digital transformation of society, which was intensified by the COVID-19 pandemic. Therefore, these new challenges and threats required a revision of the NIS Directive.

On 16 December 2020, the European Commission presented a new legislative proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020) 823 final).

The new NIS 2 Directive COM(2020) 823 final aims to address the deficiencies of the previous NIS Directive in order to adapt to the current needs and make the rules future-proof.

The proposal expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap. This means that all medium and large companies in selected sectors will be included in the scope. The NIS 2 Directive strengthens security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption. The NIS 2 Directive also contains an expanded scope to include more sectors and services, including public electronic communication networks or services, digital services such as social networking services, platforms and data centre services, wastewater and waste management, space, manufacturing of certain critical products (including pharmaceuticals, medical devices, chemicals), postal and courier services, food and public

administration. The proposal also eliminates the distinction between operators of essential and digital service providers. Entities would be classified based on their importance and divided in essential and important categories with the consequence of being subjected to different supervisory regimes. The proposal strengthens security requirements for the companies, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied. The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines. Furthermore, the proposal strengthens supply chain cybersecurity for key information and communication technologies at European level. The EU Member States in cooperation with the Commission and ENISA will carry out coordinated risk assessments of critical supply chains.

The NIS 2 Directive also includes a list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations. It establishes a European Cyber crises liaison organisation network (EU-CyCLONe) to support a coordinated management of large-scale cybersecurity incidents and crises at EU level. The proposal will be subject to negotiations between the Council of the European Union and the European Parliament. Once the proposal is agreed and adopted, Member States will have to transpose the NIS 2 Directive within 18 months. After its entry into force, the NIS 2 Directive will be periodically reviewed.

5. EU publishes cyber security toolkit for the transport sector

While the number of European businesses affected by cyberattacks is constantly increasing, many employees remain insufficiently aware of the cyber threats and risks. This is also a problem in the transport sector. Therefore, on 16 December 2020, the European Commission also published the “Transport Cybersecurity Toolkit” in order to raise awareness on cyber risks in the transport sector. The “transport cybersecurity toolkit” addresses transport organisations, regardless of their size and domain of activity. The toolkit includes a collection of recommendations and practices to enhance cybersecurity and cyber-resilience. More precisely, the toolkit contains basic information on four threats, namely malware diffusion, denial of service, unauthorised access and theft, and software manipulation. Considering those threats that may affect transport organisations, the toolkit lists good mitigating practices for all transport staff, regardless of their occupation. Furthermore, the toolkit also provides more advanced information for security and cybersecurity professionals regarding the transport modes air, maritime and land regarding cyber-awareness and cybersecurity. For each transport mode, the toolkit provides guidance on identifying, protecting, detecting and responding to cyber-threats. The toolkit is also aligned with other European Commission initiatives including the proposal for a NIS 2 Directive and the EU’s new Cybersecurity Strategy, with the aim to achieve greater resilience and cybersecurity. It will now be the European Parliament and the Council’s task to examine and adopt the proposal on the NIS 2 Directive (COM(2020) 823 final) and the Critical Entities Resilience Directive (COM(2020) 829 final).

References

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. OJ L 345, 23.12.2008, p. 75-82. (2008/114/EC). In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG, retrieved 15 January 2021

COMMISSION STAFF WORKING DOCUMENT EVALUATION of COUNCIL DIRECTIVE 2008/114 ON THE IDENTIFICATION AND

DESIGNATION OF EUROPEAN CRITICAL INFRASTRUCTURES AND THE ASSESSMENT OF THE NEED TO IMPROVE THEIR PROTECTION. Brussels, 23.7.2019 SWD(2019) 308 final. In: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-308-commission-staff-working-document_en.pdf, retrieved 15 January 2021

EUROPEAN COMMISSION: ANNEXES to the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148. {SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}. COM(2020) 823 final. ANNEXES 1 to 3. In: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union, 16.12.2020, retrieved 14 January 2021

European Commission: Commission reviews the impacts of the EU process and EU Toolbox and sets out next steps to ensure secure 5G networks in a coordinated way. In: https://ec.europa.eu/digital-single-market/en/news/commission-reviews-impacts-eu-process-and-eu-toolbox-and-sets-out-next-steps-ensure-secure-5g, 16 December 2020, retrieved 14 January 2021

European Commission: Commission Staff Working Document. Evaluation of Council Directive 2008/114 on the Identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. (SWD(2019) 308 final). In: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-308-commission-staff-working-document_en.pdf, 23.7.2019, retrieved 8 September 2020

European Commission: Critical infrastructure protection. In: https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection, retrieved 7 September 2020

European Commission: European Commission publishes 'Cybersecurity Toolkit' to raise awareness on cyber-risks and build preparedness in the transport sector. In: https://ec.europa.eu/transport/themes/security/cybersecurity_en, retrieved 15 January 2021

European Commission: Transport cybersecurity toolkit. In: https://ec.europa.eu/transport/sites/transport/files/cybersecurity-toolkit_en.pdf, retrieved 14 January 2021

European Commission: New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. In: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391, 16 December 2020, retrieved 14 January 2021

European Commission Proposal for directive on measures for high common level of cybersecurity across the Union. In: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union, 16 December 2020, retrieved 14 January 2021

European Commission: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. COM(2020) 829 final. 2020/0365 (COD). In: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf, 16.12.2020, retrieved 14 January 2021

EUROPEAN COMMISSION: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. {SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}. COM(2020) 823 final. In: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union, 16.12.2020, retrieved 14 January 2021

European Commission: Report on Member States'

progress in implementing the EU Toolbox on 5G Cybersecurity. In: https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, 24 July 2020, retrieved 14 January 2021

European Commission: State-of-play of the transposition of the NIS Directive. In: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive, 18 December 2020, retrieved 14 January 2021

European Commission: The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU. In: https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential_en, retrieved 14 January 2021

European Commission: The EU Cybersecurity Act at a glance. In: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-glance, 25 June 2019, retrieved 14 January 2021

European Commission: The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification. In: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity, 26 June 2019, retrieved 14 January 2021

European Commission/High Representative of the Union for Foreign Affairs and security policy: JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. The EU's Cybersecurity Strategy for the Digital Decade. JOIN(2020) 18 final. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018&qid=1533485886151, 16.12.2020, retrieved 15 January 2021

Regulation (EU) 2019/881 of the European Parliament and of the Council of on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, 7.6.2019, p. 15-69. In: https://eur-lex.europa.eu/eli/reg/2019/881/oj, 17 April 2019, retrieved 15 January 2021.