【欧州】【Common】

Common - Policies in the use of IoT: Cyber Security - EU supports projects for improving the protection of critical infrastructure against cyber threats

Andrea Antolini　Former Researcher JTTRI

【概要：Summary】

Critical infrastructures (CI), such as transportation systems, electricity generation plants and others infrastructure of national and European importance need to be better protected against a constantly increasing number of cyber threats, cyber attacks or hybrid attacks. Since the CIs are increasingly vulnerable against cyber attacks, the EU has introduced the Directive on Security of Network and Information Systems (NIS Directive) and the EU Cybersecurity Act among others. The EU Agency for Cybersecurity (ENISA) develops advice and recommendations on good practice on information security and it assists EU Member States in implementing relevant EU legislation. The main aim is to improve the resilience of the EU's CIs including transport systems and information networks against cyber threats and attacks. In the past years, the European Commission has supported research and innovation actions in the area of cybersecurity that contribute to better protecting key infrastructure and the people living in European smart cities.

The European Commission has been working on the revision of the Critical Infrastructure Protection Directive under the Commission's 2020 new work programme. Meanwhile, the European Commission announced that it would fund several innovative projects in the field of protecting critical infrastructure against cyber and physical threats and making cities smarter and safer through the EU's research and innovation programme Horizon 2020.

【記事：Article】

1. Cyber security related EU instruments and the EU Agency for Cybersecurity (ENISA)

Improving resilience of critical infrastructures has become a priority also in the EU. Critical infrastructures, such as electricity generation plants, transportation systems, manufacturing facilities are controlled and monitored by Industrial Control Systems (ICS).

The ICS products often use commercial off-the-shelf software, which reduces costs but at the same time, it increases the exposure to computer network-based cyber attacks. Emerging threats, as well as unconventional attacks to critical infrastructures show the limits of traditional risk assessment and risk mitigation efforts. Therefore, there is a need to secure critical infrastructure in the EU against deliberate disruptions and cyber-attacks. The EU has now legal instruments to protect electronic communications networks, including the Directive

on Security of Network and Information Systems (NIS Directive) and the EU Cybersecurity Act among others. The NIS Directive has introduced new mechanisms for cooperation at EU level, measures to increase national capabilities, obligations for operators of essential services and digital service providers to adopt risk management practices and report significant incidents to the national authorities. The Cybersecurity Act introduces, for the first time, EU wide rules for the cybersecurity certification of products, processes and services. In addition, the Cybersecurity Act defines a new permanent mandate for the EU Agency for Cybersecurity (ENISA), and allocates more financial resources to the Agency in order to enable it to fulfil its goals. Since 2019, the Agency ENISA has been drawing up cyber security certification schemes. It also develops advice and recommendations on good practice in information security and it assists EU Member States in implementing relevant EU legislation. The main aim is to improve the resilience of Europe's information infrastructure and networks against cyber threats and attacks. ENISA's current tasks regarding cyber security include the support of policy development and implementation as well as capacity building. These tasks have also been strengthened and refocused. New tasks have been added and most prominently regarding cybersecurity certification. The new mandate incorporates additional important tasks such as the role of the secretariat of the Computer Security Incident Response Teams (CSIRTs) Network that brings together national CSIRTs of EU Member States.

In support of EU efforts to protect critical infrastructures, the JRC coordinates the European Reference Network for Critical Infrastructure Protection (ERNCIP) and provides technical support for the review of the Directive on European Critical Infrastructures of 2008 (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). The JRC also carries out different research activities such as the development of methods and tools for international cyber security exercises, the assessment of the vulnerability of networked infrastructures in case of extreme space weather events, and the evaluation of the resistance of buildings and transport systems against explosions.

The ERNCIP (European Reference Network for Critical Infrastructure Protection, ERNCIP) is a framework under which various measures together aim to improve the protection of critical infrastructure in the EU. Its Project Platform supports the development of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities. It is a framework within which experimental facilities and laboratories can share knowledge and expertise in order to better align test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards.

Regarding the vulnerabilities of the transport sector's cyber security, the EU works on a number of measures to make the system more resilient to cyber risks. The EU has taken important steps including the adoption of the EU Cybersecurity Strategy in 2013. Since the adoption of the 2013 EU Cybersecurity Strategy the ENISA's mandate and role has been reviewed and re-defined, according to the significantly changed overall policy context. 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. In this context, a key role was attributed to ENISA in supporting the implementation of this NIS Directive. ENISA acts as a centre of expertise dedicated to enhancing network and information security in the EU.

In September 2017, the European Commission presented a proposal on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM (2017) 477 final). On 27 June 2019, this new European Cybersecurity Act, Regulation (EU) 2019/881, on ENISA and on information and communications technology cybersecurity certification became effective. With the introduction of the Cybersecurity Act, the Commission intends to strengthen the mandate of the ENISA and establishes a EU-wide cybersecurity certification framework in which ENISA will play a key role. It upgrades ENISA into a permanent EU agency for cybersecurity and strengthens ENISA's ability to help EU Member States to address cybersecurity threats. The two new key areas where the Agency will play an important role are cybersecurity crisis management and cybersecurity certification and standardization of ICT products and services.

2. The revision of the European Critical Infrastructure (ECI) Directive

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 (European Critical Infrastructure (ECI) Directive) aims to enhance the protection of critical infrastructure in the EU.

In July 2018, the European Commission presented a staff-working document on the evaluation of the Council Directive 2008/114. The evaluation considered the implementation of the Directive from its entry into force in January 2009 to the start of the evaluation in August 2018 and its application in each EU Member State (SWD (2019) 308 final).

Under the European Commission new work programme's fifth priority - "Promoting our European Way of Life", published in January 2019, the Commission announced to issue a legislative proposal for additional measures on Critical Infrastructure Protection. According to the work programme, the proposal should be adopted in the fourth quarter of 2020 and include an impact assessment.

In the evaluation, it was concluded that the Directive is currently only of partial relevance in light of a very different security landscape compared to the time when the Directive entered into force in 2009. The Directive's main weakness is its limited scope, covering only sectors of transport and energy. Therefore, in its conclusions of December 2019, the Council invited the Commission to consult with Member States on a possible proposal for a revision of the Directive (2008/114/EC) for the identification and designation of European critical infrastructures (ECIs) including potential additional measures to enhance the protection and resilience of critical infrastructure in the EU. The overall objective of the external evaluation was to identify and designate European critical infrastructures and the assessment of the need to improve their protection. In view of recent technological, economic, social, policy/political and environmental developments and considering the new and evolving challenges in protecting Critical Infrastructure, the Directive has to be revised. 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 overlaps with other pieces of European sectoral legislation/policy documents in the energy, transport and ICT sectors and has partially achieved improvements in the level of

protection for ECIs (European critical infrastructure) in the energy and transport sectors. However, because the generality of some of the Directive's provisions, the EU Member States had interpreted the provisions differently and therefore the Directive 2008/114/EC has only partially achieved the objective of establishing a common approach to the assessment of the need to improve the protection of ECI. The evaluation was ultimately inconclusive regarding the question if the Directive contributed to the overall objective of an improved level of protection of the critical infrastructure with EU relevance. While the extent of the costs associated with implementation of the Directive appeared to be limited, a lack of available quantifiable data from the Member States and ECI owners/operators makes it difficult to carry out a sound assessment of the Directive's regulatory burden on stakeholders.

The Directive generated EU added value, like in case of a common framework for the protection of ECI. On the other hand, certain specific provisions, like the Operator Security Plan, the Security Liaison Officer function and reporting requirements, proved to have limited added value for many Member States.

The evaluation made clear that the Directive as a central pillar of the European Programme for Critical Infrastructure Protection (CIP) initially played an important role in bringing attention to bear on CIP. However, the interdependencies between CIs in different sectors are considerable and extend beyond Europe's boundaries. This needs to be considered when addressing the security of European CI in the years to come. The evaluation indicated that while some elements of the Directive remain useful, others are of limited value and could be revised in order to better achieve the Directive's stated overall objective of an improved level of protection of CIs in the energy and transport sectors. This could mean shifting the focus away from asset protection to one that is more systemic and which recognises interdependencies across a range of different sectors. Many Member States have also incorporated resilience thinking into their national CIP frameworks. This means ensuring that CIs are both well protected and capable of quickly recovering from disruptions in those instances where protective measures are inadequate.

The consultations suggested that there is continued support on the part of Member States for EU involvement in CIP policy. However, a number of Member States argued during the consultations that CIP is primarily a national responsibility and suggested that the EU's engagement both now and in future should respect the principle of subsidiarity and demonstrate clear EU added value.

Based on the findings of the evaluation, there is clearly room for further reflection at EU level as to how best further improve the protection of CI in Europe, including the 93 ECIs that have been designated thus far. As of August 2018, the Member States had designated 93 ECIs, the identities of which are not public information. Out of these, 88 were in the energy sector, with the remaining five CIs being in the transport sector. However, as the evaluation suggests and the NIS Directive demonstrates, there are additional sectors that the Member States consider worthy of additional protective action at European level. Based on the evaluation's findings, there is clearly room for further reflection at EU level as to how best further improve the protection of CI in Europe and to develop strategies for identifying and addressing those vulnerabilities that result from the interdependencies that exist between them.

Further work would be needed in order to assess the potential advantages of aligning CIP and NIS policy to better reflect how issues related to critical infrastructure protection and resilience are connected. In its conclusions from December

2019, the Council estimated that protecting national and European critical infrastructures is a key priority, and invited the Commission to consult with Member States on a possible proposal for a revision of the Directive (2008/114/EC), including potential additional measures to enhance the protection and resilience of critical infrastructure in the EU. The Council emphasised that while the responsibility for critical infrastructure protection is primarily a matter of national competence, the high degree of cross-border and cross-sectoral interdependencies require coordinated or harmonised efforts at the EU level, including in view of the uninterrupted functioning of the internal market. Following the July 2019 evaluation on the implementation of the Directive (2008/114/EC).

In its 2020 Commission Work Programme of 29.1.2020 COM(2020) 37 final, the Commission pointed out that it would put forward a new EU Security Union Strategy in order to set out the areas where the Union can bring added value to support Member States in ensuring security - from combatting terrorism and organised crime, to preventing and detecting hybrid threats, to cybersecurity and increasing the resilience of critical infrastructure in the EU. The Commission will also strengthen the Europol mandate in order to reinforce operational police cooperation. Based on the Commission's 2020 work programme it is also planned to present a Proposal for additional measures on Critical Infrastructure Protection in the fourth quarter of 2020.

3. The European Commission supports projects for the protection of critical infrastructure against cyber threats

On 15 June 2020, the European Commission announced to fund several projects in the field of protecting critical infrastructure against cyber and physical threats with more than EUR 38 million. The projects would be funded through the EU's research and innovation programme Horizon 2020.

According to the Commissioner for Internal Market Thierry Breton, while facing cybersecurity threats, the EU needs to take concrete measures to protect critical infrastructures, information systems and to enhance cyber resilience, among others. Accordingly, the European Commission supports three projects, namely SAFETY4RAILS, 7SHIELD and ENSURESEC, which intend to improve prevention, detection, response and mitigation of cyber and physical threats in the transport sector for metro and railway networks, ground space infrastructure and satellites, as well as e-commerce and delivery services. In addition, two other projects, IMPETUS and S4ALLCITIES, receive funds to enhancing the resilience of cities' infrastructures and services and protecting citizens in case of security incidents in public spaces.

The projects are expected to start until October 2020 and they will run for two years. The Research Executive Agency will manage the five selected projects and has finalised the preparation and signature of grant agreements with the beneficiaries. The EU's financial contribution is provided in the form of grants that can be up to 100% of the project's total budget.

The SAFETY4RAILS Project is a databased analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS. Railways and Metros are safe, efficient, reliable and environmentally friendly mass carriers, and they are even more important means of transportation given the need to address climate change. However, since they are such critical infrastructures, it turns metro and railway operators as well as related intermodal transport operators into attractive targets for cyber and/or physical attacks. In order to protect this critical infrastructure, the SAFETY4RAILS project delivers methods and systems to increase the safety and

recovery of track-based inter-city railway and intra-city metro transportation. It addresses both cyber-only attacks, physical-only attacks and combined cyber-physical attacks. SAFETY4RAILS concentrates on rush hour rail transport scenarios where many passengers are using metros and railways to commute to work or attend mass events. When an incident occurs during heavy usage, metro and railway operators have to consider many aspects to ensure passenger safety and security. The aim of SAFETY4RAILS is to improve the handling of such events through a holistic approach by analysing the cyber-physical resilience of metro and railway systems and by delivering mitigation strategies for an efficient response. Grant agreement is signed and the project will start on 1 October 2020 and end on 30 September 2020. The SAFETY4RAILS budget is EUR 9,641,911.94 with a EU contribution of EUR 7,697,691.39. It is coordinated by the Fraunhofer Gesellschaft zur Foerderung der Angewandten Forschung e.V., Germany.

The 7SHIELD Project addresses Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats. It is a new market with the massive amounts of satellite data that the ground segments of space systems serve to the market and governmental bodies. A physical/cyber-attack to their installations or communication networks, respectively, would cause a negative impact on public safety and security of EU citizens and public authorities. A physical attack on a space ground segment would make the distribution of satellite data problematic and, on the other hand, a cyber-attack in its data storage, access and exchange would not only affect the reliability of space data, but also their “FAIR” standards, including accessibility and interoperability. The 7SHIELD will be an integrated, yet flexible and adaptable framework enabling the deployment of innovative services for cyber-physical protection of ground segments, such as e-fences, passive radars and laser technologies, and multimedia AI technologies, that enhance their protection capabilities. The project will be evaluated and demonstrated in five installations of ground segments of space systems. The 7SHIELD project’s grant agreement is ID: 883284 and the project started on 1 September 2020 and will end on 31 August 2022. The project’s overall budget is EUR 8,682,437.50, with a EU contribution of EUR 6,969,568.75. It is coordinated by Fair Dynamics Consulting s.r.l., Italy.

The third project is the ENSURESEC project for an End-to-End Security of the Digital Single Market’s E-commerce and Delivery Service Ecosystem. ENSURESEC intends to safeguard the Digital Single Market’s e-commerce operations against cyber and physical threats. ENSURESEC addresses the entire modern e-commerce, from standard physical products purchased online and delivered via post, to entirely virtual products or services delivered online. It addresses threats ranging from maliciously modifying web e-commerce applications or rendering them unavailable to legitimate customers, to delivery issues or fraud committed by insiders or customers. It focuses on the common software and physical sensor interfaces that sit along the e-commerce, payment and delivery ecosystem. ENSURESEC’s grant agreement ID is 883242 and it is an already on-going project, which started on 1 June 2020 and will end on 31 May 2022. Its overall budget is EUR 9,230,681.25 with a EU contribution of EUR 7.701,519.75. The ENSURESEC is coordinated by INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS, Portugal.

The S4ALLCITIES project, short for “Smart Spaces Safety and Security for All Cities” integrates advanced technological and organizational solutions in a market oriented unified Cyber - Physical Security Management framework. It aims at raising the resilience of cities’ infrastructures, services, ICT systems, IoT and

fosters intelligence and information sharing among city's security stakeholders. S4AllCities comprises of three pilot cases, with the engagement of a total of 5 cities in 4 countries (Spain, Romania, Czech Republic and Greece). S4ALLCities smart components will demonstrate their technological advances in tackling terrorist attacks with high risk for mass casualties, within the complex environment of open crowded spaces. The multidisciplinary consortium of 9 EU Member States will exploit the project's innovative technological systems in the global market providing a cost efficient and market ready integrated solution. S4ALLCities exploitation phase will promote good practices and guidance material across EU cities so as to enhance capacity building of involved stakeholders, reduce the vulnerabilities of public spaces, mitigate the consequences of adversary attacks, raise public awareness and strike a balance between improving security and preserving the open nature of public spaces as well as citizens' sense of freedom.

S4AllCities with the grant agreement ID 883522 started on 1 September 2020 and will end on 31 August 2022. The project's overall budget is EUR 9,738,317.34 with a EU contribution of EUR 7,992,479.88. The project is coordinated by EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS, Greece.

Finally, the already finalised project IMPETUS, short for Information Management Portal to Enable the inTegration of Unmanned Systems, had the objective to research on the application of the "micro-services" paradigm as a flexible and cost efficient solution for lifecycle support of the expected high variety of drones and missions. Moreover, IMPETUS explored how to design a Smart UTM Concept taking into consideration the "Function as a Service" paradigm to develop a cloud-based server-less environment, characterized by its scalability to respond to multiple users with diverse business models, and its flexibility to facilitate the integration with manned traffic management systems.

IMPETUS consortium consisted of key stakeholders that provided complementary views on the current and envisioned UTM and ATM information management processes. The IMPETGUS project's Grant agreement ID 763807 started on 1 October 2017 and ended on 30 September 2019. Its overall budget was EUR 899,160 with a 100% EU contribution. It was coordinated by CENTRO DE REFERENCIA INVESTIGACION DESARROLLO E INNOVACION ATM, A.I.E., Spain.

All projects were selected for funding under a competitive call for proposals and the support is part of the EU's commitment to build a strong cybersecurity culture and enhanced capabilities to resist and respond effectively to potential cyber threats and attacks.

4. Conclusion

While in the past, the Council of the European Member States emphasised that it is the individual Member States' responsibility to protect critical infrastructure, the high degree of cross-border and cross-sectoral interdependencies require coordinated or harmonised efforts at the EU level. In its 2020 Work Programme, the Commission put forward the plan for a new EU Security Union Strategy in order to set out the areas where the EU can support Member States in ensuring security, including combatting terrorism and organised crime, to preventing and detecting hybrid threats, to cybersecurity and increasing the resilience of the EU's critical infrastructure.

Meanwhile, the European Commission supports projects like SAFETY4RAILS, 7SHIELD and ENSURESEC in order to improve the prevention, detection, response and mitigation of cyber and physical threats in the transport sector for metro and railway networks, ground space infrastructure and satellites, as well as e-commerce and delivery services. In addition other projects receive funds to enhancing the resilience of cities'

infrastructures and services. The EU's financial contribution is provided to these projects in the form of grants that can reach up to 100% of the project's total budget.

However, in future, more investments in innovative cybersecurity technologies at EU and national level will be necessary in order to improve the EU's critical infrastructure's resilience to cyber attacks and to increase security levels of CI.

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 (Text with EEA relevance). In: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563433473943&uri=CELEX:32008L0114, retrieved 9 September 2020

Council of the European Union: Complementary efforts to enhance resilience and counter hybrid threats- Council Conclusions, 10 December 2019. In: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf, 10 December 2019, retrieved 2 September 2020

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 2 September 2020

European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions. Commission Work Programme 2020. A Union that strives for more. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:37:FIN, COM/2020/37 final, 29.1.2020, retrieved 7 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: 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. 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 8 September 2020

European Commission: EU grants €38 million for protection of critical infrastructure against cyber threats. In: https://ec.europa.eu/digital-single-market/en/news/eu-grants-eu38-million-protection-critical-infrastructure-against-cyber-threats, 15 June 2020, retrieved 8 September 2020

European Commission: EU grants €38 million for protection of critical infrastructure against cyber threats. In: https://ec.europa.eu/commission/presscorner/detail/en/mex_20_1063, 15 June 2020, retrieved 7 September 2020

Proposal for additional measures on Critical Infrastructure Protection / after 2020-09. In: https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-critical-infrastructure-protection

The 7SHIELD project. In: https://cordis.europa.eu/project/id/883284, retrieved 7 September 2020

The ENSURESEC project. In: https://cordis.europa.eu/project/id/883242, retrieved 8 September 2020

The IMPETUS project. In: https://cordis.europa.eu/project/id/763807, retrieved 7 September 2020

The S4AllCities project. In:
https://cordis.europa.eu/project/id/883522, retrieved
7 September 2020
The SAFETY4RAILS Project. In:
https://cordis.europa.eu/project/id/883532,
retrieved, 7 September 2020