CoU Brief
Critical Infrastructure Protection

September 2019

Summary statement

- Several challenges characterise the domain of Critical Infrastructure Protection in the European Union: the definitions of what Critical Infrastructure constitutes still vary between the EU Member States. Member States often lack a common approach to identifying what the most critical components within the different sectors of Critical Infrastructure are.
- Having a common approach would be beneficial to enable cross-correlation among the EU Member States, which could finally turn in the sharing of best practices. An action point for policy-makers is, therefore, to define standard approaches. Third, there are divergences in approaches on how to protect Critical Infrastructures.
- The EU would benefit from moving away from its focus on singular asset protection towards a minimum service performance-based approach while acknowledging the interdependency of Critical Infrastructure on the national and the European level.
- Another essential topic in the context of Critical Infrastructure protection are Supply Chains, which go well beyond the EU borders.
- A policy framework which builds on the idea that Critical Infrastructures are 'silos' is outdated. In the multi-dimensional and ever-changing risk landscape, EU Member States would benefit from developing cross-sectoral policies
- A one size fits all approach is not applicable in the field of protection of Critical Infrastructure. The domain would benefit from specific protection plans for each Critical Infrastructure based on a reasoned analysis of risks and the vulnerabilities. However, there are common characteristics, including threats, privacy rules and information sharing, emergency measures, horizontal technologies and processes. Protective measures implemented in one sector may provide examples for other sectors. The field would, therefore, benefit from exploiting, despite the specific nature of protection plans, the potential for synergy between sectors.
- In an rapidly changing threat-landscape, Cybersecurity is one of the most challenging areas for Critical Infrastructure Protection. Besides the need to keep up with technological develpoments, legislation such as the Directive on Secuirty of Network and Information Systems (NIS) and the Cybersecuirty Package is curcial to ensure the necessary level of protection.
- A particular challenge for researchers in the Critical Infrastructure domain is the sensitivity of the topic and the related difficulty to disseminate research results and to share information in scientific articles about Critical Infrastructure associated topics. Due to the confidentiality of some of the research, results cannot be made publicly available which leads to an information gap.

European Commission

Introduction

This CoU brief summarises the topic Critical Infrastructure Protection and relevant EU-funded projects that participated in the 14th Meeting of the Community of Users (CoU) on Secure, Safe and Resilient Societies that took place 16 – 19 September 2019 at the BAO convention centre in Brussels. The Community of Users is a DG HOME initiative aims to improve information transfer of research outputs and their usability by different categories of stakeholders. During the meetings and thematic workshops, policy updates and information about H2020 projects are provided and interactive discussions facilitated to ensure that solutions and tools resulting from research will reach users.

Scope and relevance

According to Eurobarometer results, EU citizens consider security as an increasingly important topic. To remain a credible provider of security for its citizens, the EU is investing in the protection of physical and digital assets, which have a critical impact on the security of the EU. In this context, the European Programme for Critical infrastructure was launched in 2006 with an 'all hazards all sectors approach' and a particular focus on critical infrastructure protection. The Critical Infrastructure Protection Directive (hereafter: the Directive) adopted in 2008, therefore, constitutes a key pillar of the Programme focusing on the question how the EU can support the EU Member States in better protecting their Critical Infrastructure. An asset is classified as 'Critical Infrastructure' if at least two Member States acknowledge its critical impact on the security of the EU. The EU Member States lead the process of Critical Infrastructure identification. The European Commission has established a single point of contact in each of the EU Member States. The outcome of the 2012 review of the Directive was overall positive and found that it has boosted Critical Infrastructure awareness in Europe. However, at the time of writing, the EU Member States have only identified a few Critical Infrastructure assets.

In light of the European Commission's 2017 comprehensive assessment of the EU's Security policies, another evaluation of the Directive was conducted, which concluded that the identification of Critical Infrastructure Protection was partially effective, further increased the awareness and supported the relative coherence of Critical Infrastructure in Europe. It also found that the EU Member States further support the Directive. A challenge remains that the definitions of what Critical Infrastructure constitutes still vary from EU Member State to Member State as well as there are divergences in approaches on how to protect Critical Infrastructures.

At the same time, the evaluation included an assessment of future threats in Europe, particularly with regards to emerging technologies, for example, the prospects but also the risks of Artificial Intelligence, hybrid scenarios, cyber threats (NIS Directive) and other developments such as security of supply (food security). It concluded that new approaches must be flexible and risk-based and must include the concept of resilience as opposed to a protection-based approach. The way forward largely depends on the new European Commission and the results of on-going research projects.

Current debates and stakeholder perspectives

The 2017 evaluation of the Directive made it clear that the EU Member States would benefit from moving away from their focus on singular asset protection towards acknowledging the interdependency of Critical Infrastructure on the national and the European level. A policy framework which builds on the idea that Critical Infrastructures are 'silos' is outdated. To tackle a multi-dimensional and ever-changing risk landscape, cross-sector policies plans and institutions would be beneficial for the domain.

The added value of EU cooperation is that resilience can and has been built together especially when it comes to hybrid and cyber threats and other hostile activities where the EU Member States cannot act in isolation and would benefit from more leadership within the EU.

Critical infrastructure, civil protection and emergency management

The discussion of Critical Infrastructure protection would benefit from considering the operational layer to it. In the wake of a disaster, emergency management and Critical Infrastructure management become closer than ever. In the future, strong resilience will require a dramatic shift from physical protection only, to the performance of essential services during and after the crisis, which raises the question of what the vital requirements and bottom-line of these services should be. The Union Civil Protection mechanism (UCPM) has been activated 300 times since 2001. RescEU is adding a new EU layer to disasters by ensuring the right balance between solidarity and responsibility amongst the EU Member States. An attack on an EU Member State's Critical Infrastructure could be considered as a high impact, low probability event and calls therefore for an appropriate preparedness and response. The EU Member States would also benefit from building a framework on resilient infrastructure and considering the asset management perspective, where an emergency takes place. Another issue is related to the question of leadership during attacks on Critical Infrastructure. On the EU level, it often remains unclear which actor are in charge and responsible on the national and European level.

Emerging and new threats

Recent terror attacks in Europe made it clear that the protection of Critical Infrastructure, public spaces and essential suppliers of services (e.g. airports, ports, hospitals, railway stations, drinking water suppliers) are of crucial importance. Critical service providers and public spaces are not only vulnerable to physical attacks but are, in many cases, highly data-driven and therefore also sensitive to cyberthreats. Both physical and cyber-attacks can lead to catastrophic and cascading events which can quickly get out of control. An example of an emerging threat is the usage of drones which can be stocked with toxic chemical or radioactive substances.

H2020 projects like SecureGas, are focussing on increasing the resilience of the EU Gas Critical Infrastructure and defending the European energy infrastructure in the case of a physical or a combination attack, which can consist of a physical and cyber-attack happening at once. In practical terms, this means that existing and new gas infrastructure will have to resist to hazards and absorb their impacts more efficiently and more effectively; accommodate and recover the effects of a hazard more efficiently, timely and safely; and be designed/restored to coordinate more efficiently across the various phases of a disaster risk management cycle.

Discussion on emerging cyber and digital threats, for example, on critical financial service infrastructure, are gearing towards the integration of technologies and cyber systems into critical infrastructures. In contrast to the digital applications that aim to provide security to such sites, these infrastructures are often relatively outdated and were often not designed to allow fur such technically advanced interventions. This misfit poses challenges that projects such as Anastacia try to overcome by approaching such sites from a network perspective (i.e. installing devices to monitor the network) rather than to overhaul the full cybersecurity system of critical infrastructure.

The REACT project addressed another more fundamental challenge that persists in the domain of cybersecurity. The fact that citizens are making more and more use of digital appliances also enhances their vulnerability. The number of cyber-attacks has increased over the years; examples include the 2018 Marriot leak where customer data of over 500 million users were exposed[1] and the Wannacry ransomware that comprised computers globally in 2017.[2] Such attacks do jeopardise not only the privacy and security individuals but also those of critical infrastructure sites. To enhancing the EU's resilience against such attacks, an advanced understanding of how hackers work is essential to be one step ahead of them.

With a rapidly changing security landscape, the European Commission actively seeks to strengthen the Union's capabilities in this domain. Efforts include legislative actions such as the development of the EU Cybersecurity strategy, the Directive on Security of Network and Information Systems (the NIS Directive) that was reinforced by the Cybersecurity Package, which also includes the Cybersecurity Act. This act strengthens the EU Agency for Cybersecurity (ENISA) and has developed an EU cybersecurity certification framework. Certification of, amongst others, the 5G networks are currently being discussed.

DG CNECT emphasised the need for research and innovation to strengthen the EU's cybersecurity capacities further. The H2020 call on prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe is an illustration of such efforts.[3]

1 www.nytimes.com/2018/11/30/business/marriott-data-breach.html.
2 www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs
3 SU-INFRA01-2018-2019-2020

Main stakeholders in the Critical Infrastructure Protection landscape

The following section provides an overview of the main actor groups involved in Critical Infrastructure protection in Europe.

Operators of Critical Infrastructures are the most important actors in protection. Companies and public bodies which are engaged in the management of certain infrastructures are aware of the technical specifications, developments within the sector and most important the threat level. Their knowledge is essentialin order to provide suitable legal, operational and technological tools to protect infrastructures.

The protection of Critical Infrastructure in a dynamic environment requires constant innovation and tailor-made solutions developed by **industry and SMEs**. Therefore, they play a pivotal role in securing Critical Infrastructure in Europe.

Policy-makers on the European and on the national level also play an important role in the protection of Critical infrastructure in Europe through research funding and the development of policies which support collaboration and coordination efforts of the relevant stakeholders. Civil protection authorities would benefit from working hand in hand with the first responder community to meet the requirements of responders and foster collaboration between the actors. The Cybersecurity Act reinforces the mandate of the EU Agency for Cybersecurity to better support Member States with tackling cybersecurity threats and attacks.

One of the main challenges concerning the protection of Critical Infrastructure are the rapidly emerging threats. **Researchers** play a pivotal role in analysing the dynamic threat landscape, help to foster the understanding how Critical Infrastructure is connected to make sure critical system can recover quickly. Research can also help to examine the benefits and challenges new technologies can bring to strengthen the resilience of Critical Infrastructure for society. Research projects are the first step in the development process of innovative solutions, which can enhance security in Europe. Emerging threats are also affecting the work of first responders in the field especially concerning CBRNE-related and cyber threats, which require additional training measures and a new generation of practitioners who operate remotely and who are capable of dealing with the growing number of cyber threats. Furthermore, education and awareness-raising measures for the population are important tasks to ensure appropriate reactions and to avoid panic during an attack on Critical Infrastructure.

Relevant projects

The following section briefly introduces the projects which were presented during the event.

Critical Transport Networks

- **Security of Air Transport Infrastructure of Europe** (SATIE): SATIE adopts a holistic approach about threat prevention, detection, response and mitigation in the airports while guaranteeing the protection of critical systems, sensitive data and passengers. Critical assets are usually protected against individual physical or cyber threats, but not against complex scenarios combining both categories of threats. To handle it, SATIE develops an interoperable toolkit which improves cyber-physical correlations, forensics investigations and dynamic impact assessment at airports.
- **Scalable multidimensionAl sitUation awaReness sOlution for protectiNg European ports** (SAURON) proposes to ensure an adequate level of protection and resilience against physical, cyber and a combined threat for the EU ports and limiting, as far as possible, the detrimental effects for the society and citizens of a declared attack. The vision of SAURON is to provide a multidimensional yet installation-specific Situational Awareness (SA) platform to help port operators anticipate and withstand potential cyber, physical or combined threats to their freight and cargo business and the safety of their employees, visitors, passengers and citizens in the vicinity.

Critical Supplies

- **Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats** (STOP-IT): Water Critical Infrastructures (CIs) are essential for human society, life and health and they can be endangered by physical/cyber threats with severe societal consequences. To address this, STOP-IT assembles a team of major Water Utilities, industrial technology developers, high tech SMEs and top EU R&D providers. It organises communities of practice for water systems protection to identify current and future risk landscapes and to co-develop an all-hazards risk management framework for the physical and cyber protection of water CIs. Prevention, Detection, Response and Mitigation of relevant risks at strategic, tactical and operational levels of planning will be taken into account to generate modular solutions (technologies, tools and guidelines) and an integrated software platform

- **Defending the European Energy Infrastructures** (DEFENDER): Modern critical infrastructures are increasingly turning into distributed, complex Cyber-Physical systems that need proactive protection and fast restoration to mitigate physical or cyber incidents or attacks, and most importantly combined cyber-physical attacks, which are much more challenging and it is expected to become the most intrusive attack. This is particularly true for the Critical Energy Infrastructures (CEI). Critical Energy infrastructures (CEI) protection and security are becoming of utmost importance in our everyday life. However, cyber and system-theoretic approaches fail to provide appropriate security levels to CEIs, since they are often used in isolation and build on incomplete attack models, resulting in silos-like security management fragmented operational policies. To face these challenges, DEFENDER will (i) model CEIs as distributed Cyber-Physical Systems for managing the potential reciprocal effects of cyber and physical threats (ii) deploy a novel security governance model, which leverages on lifecycle assessment for cost-effective security management over the time (iii) bring people at centre stage by empowering them as virtual sensors for threat detection, as first-level emergency responders to attacks, or by considering workforce as potential threats.
- **Securing the European Gas Network** (SecureGas) focuses on the 140.000 kilometres of the European Gas network covering the entire value chain from Production to Transmission up to Distribution to the users, providing methodologies, tools and guidelines to secure existing and incoming installations and make them resilient to cyber-physical threats. Three business cases, addressing relevant issues for the Gas sector and beyond (e.g. oil), have been identified so that to ensure the delivery of solutions and services in line with clear needs and requirements, focused on risk-based security asset management of gas transmission and distribution networks; impacts (economic, environmental and social) and cascading effects of cyber-physical attacks on interdependent and interconnected European Gas grids; integrity and security, through the operationalization of resilience guidelines, of strategic installations across the EU Gas network. SecureGas tackles these issues by implementing, updating, and incrementally improving extended components, integrated and federated according to a High-Level Reference Architecture built upon the SecureGas Conceptual Model, a blueprint on how to design, build, operate and maintain the EU gas network to make it secure and resilient against cyber-physical threats.

Critical Services

- **Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures** (FINSEC) is a flagship project which will develop, demonstrate and bring to market an integrated, intelligent, collaborative and predictive approach to the security of critical infrastructures in the financial sector. To this end, FINSEC will introduce, implement and validate a novel reference architecture for the integrated physical and cybersecurity of critical infrastructures, which will enable handling of dynamic, advanced and asymmetric attacks, while at the same time boosting financial organisations' compliance to security standards and regulations. As a result, FINSEC will provide a blueprint for the next-generation security systems for the critical infrastructures of the financial sector.
- **Integrated cyber-physical security for health services** (SAFECARE) has the aim to provide solutions that will improve physical and cybersecurity seamlessly and cost-effectively. Thereby, it promotes new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. Over the course of 36 months, SAFECARE will design, test, validate and demonstrate 13 innovative elements optimising the protection of critical infrastructure under operational conditions.
- **RESIlience enhancement and risk control platform for communication infraSTructure Operators** (RESISTO) is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters.

Cyber and Digital Threats

- **Improving Resilience to Emergencies through Advanced Cyber Technologies** (I-REACT) To increase the resilience of European citizens and assets to natural disaster, we propose I-REACT: Improving Resilience to Emergencies through Advanced Cyber Technologies. The proposed system targets public administration authorities, private companies, as well as citizens to provide increased resilience to natural disasters through better analysis and anticipation, effective and fast emergency response, increased awareness and citizen engagement. I-REACT integrates existing services, both local and European, into a platform that supports the entire emergency management cycle. Leveraging on innovative cyber technologies and ICT systems, I-REACT will be able to enable early planning of disaster risk reduction actions, achieve effective preparedness thanks to risk assessment and early warnings, and efficiently manage emergency responses by empowering first-responders with up-to-date situational information and by engaging citizens through crowdsourcing approaches and social media analysis.
- **Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures** (Anastacia): The main objective of the ANASTACIA is to address the constant discovery of vulnerabilities in ICT components assuring that ICT systems are secure and trustworthy by design. To this end, ANASTACIA will research and develop a holistic security framework, which will address all the phases of the ICT Systems Development Lifecycle and will be able to take autonomous decisions using new networking technologies (SDN/NFV), and dynamic security enforcement and monitoring methodologies and tools.
- Cyberwatching.eu aims to implement and maintain an EU Observatory to monitor research and innovation projects in the domain of cybersecurity and privacy throughout the EU and associated countries. The initiatives are visually presented on the project's website[4], thereby providing an online catalogue of services for cybersecurity & privacy, showcasing market uptake and advancing EU sustainable competitiveness.

Possible synergies

For an overview of related projects funded prior to 2018, see section 4 (Critical Infrastructure Protection and Urban Built Environment) of DG HOME, "Community of Users on Secure, Safe and Resilient Societies – Mapping Horizon 2020 and EU-funded Capacity-Building Projects under 2016-2018 Programmes". The projects referenced within this section of the aforementioned document are universally geared towards tackling similar subjects as those discussed in this brief, and thus have the potential of exhibiting synergies with them.

Lessons learned

The Critical Infrastructure domain would benefit from acknowledging that a uniform approach on EU level is not necessarily needed because each EU Member State has a different system and knows best which measures to apply on a national level. Nevertheless, a clear framework of shared responsibilities, a common understanding and approach of Critical Infrastructure Protection in Europe would add value to the field.

A particular challenge for researchers in the Critical Infrastructure domain is the sensitivity of the topic and the related difficulty to disseminate research results and to share information in scientific articles about Critical Infrastructure associated topics. Due to its confidentiality, some of the research- results cannot be made publicly available. Incident findings made available to those who "need to know" this to take actions, not the whole research community, could contribute to more concerted action.

The Research Community would also benefit from bringing to the attention of policymakers evidence of approaches that can be commonly shared and demonstrate their effectiveness within the projects. The current lack of common approaches (which is the consequences of common metrics and indicators among the others) still represents a gap. However, the lack of common knowledge about an incident can lead to information gaps; for example, large attacks are sometimes preceded by smaller attacks which remain unknown. More research on the topic of security intelligence to overcome the current silo situation would add significant value to the domain.

4 http://cyberwatching.eu

Way forward

To further advance the protection of Critical Infrastructure in Europe, improved collaboration efforts between the research community, practitioners and policymakers are encouraged. While researchers are at the forefront of inventing innovative tools to protect the critical systems in Europe better, SMEs need incentives to develop such tools for the civil protection community and put them on the market. The role of policymakers is to shape the understanding of Critical Infrastructure as a comprehensive cross-national threat, which has to be tackled jointly.

On the European level, DG ECHO is currently working a European hub for civil protection, which has the objective to foster collaboration and knowledge exchange in the field of civil protection and crisis management. If successfully implemented, it might be a step in the right direction towards Critical Infrastructure protection in Europe. The European Commission's Joint Research Centre (JRC) is working on the verification of threat detection equipment and is testing Explosive Trace Detection (ETD) kits in the field. The JRC is also working on new standards in the field such as a Triacetonetriperoxide (TATP) spray. The explosive TATP has been used in several deadly terrorist attacks over the past two decades, which is why it is important that law enforcement is able to detect it. To train Explosives Detection Dogs (EDD), police officers, for example, spray pieces of luggage with a solution containing TATP at airports and line them up with people carrying unsprayed bags for the dogs to detect the contaminated items. The spray can also help to verify the detection capability of ETD systems and to check the swabbing technique of security staff.

DG MOVE is focussing on transport security which covers aviation, maritime and land security with the primary objective of protecting passengers, staff and goods from unlawful acts. This objective is for example achieved by legislative acts establishing common rules and standards for all of three domains such as covering port, port facility and ship security, compliance monitoring through both European Commission inspections covering airports and authorities and inspections by Member States or establishing an EU rail passenger Security platform.

The European Commission also invested considerable efforts into the advancement of the legal framework on Critical Infrastructure protection in general, and the protection of cyber systems in particular. The current framework encompasses the following key legislative documents: The European Programme for Critical infrastructure,[5] the Critical Infrastructure Protection Directive[6] and the EU Cybersecurity strategy 'An Open, Safe and Secure Cyberspace'.[7] It furthermore includes the Directive on Security of Network and Information Systems (the NIS Directive),[8] which is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. The Cybersecurity Package builds upon existing instruments and presents new initiatives to improve EU cyber resilience further, and response.[9] The European Commission also put forward the creation of an EU certification framework for ICT security products in its 2017 proposal for a regulation. Besides, the Cybersecurity Act reinforces the mandate of the EU Agency for Cybersecurity (European Union Agency for Network and Information and Security, ENISA) to better support Member States with tackling cybersecurity threats and attacks.[10]

5 https://europa.eu/rapid/press-release_MEMO-06-477_en.htm
6 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.
7 JOIN/2013/01 final. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.
8 Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
9 JOIN(2017) 450 final. Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
10 Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Key Contacts

http://www.securityresearch-cou.eu/

DG HOME
Max Brandt
Max.Brandt@ec.europa.eu

Philippe Quevauviller
Philippe.Quevauviller@ec.europa.eu