PRECINCT

Preparedness and **R**esilience **E**nforcement for **C**ritical **IN**frastructure cascading **C**yberphysical **T**hreats and effects with focus on district or regional protection

Enhanced Resilience of Interdependent Critical Infrastructure

Perspective of the EU H2020 PRECINCT Research Project

Dr. Ronan Frizzell, Mrs. Jenny Rainbird, Dr. Giovanni Nisato, Mrs. Loredana Mancini, Inlecom Commercial Pathways

The project has received funding from the European Union's HORIZON 2020 research and innovation program under Grant Agreement No 101021668

PRECINCT

1. The Growing Interdependency of Critical Infrastructure

Governments around the world are enacting regulations that require critical infrastructure providers to implement security measures to protect their systems. This is in response to the growing trend of cyber-physical attacks, natural hazards and hybrid threats, which leave Critical Infrastructure (CI) increasingly at risk.

An examination of a recent CER Directive from the European Parliament and Council [1] highlights the indispensable role of CI in enabling essential societal and economic functions across the Union. The growing interdependency of the Union economy is highlighted in the directive, which emphasises the need for harmonised rules to help improve resilience of CI and provide associated supporting measures.

The essence of the directive centres on ensuring CI operators are in a stronger position to prevent and mitigate the effects of adverse incidents that could interrupt the provision of essential services. A key element of this directive that this paper would like to highlight is the recognition that protective measures for individual CI do not go far enough in preventing disruption to essential operations and the topic of interdependent CI must be considered.

This topic deserves further discussion due to the nature of how essential services are being provided within the Union, which, as the directive highlights, has become increasingly co-dependent and cross-border in nature. To support this point, Article 12.2 of the directive discusses how risk assessments for critical entities must consider their dependency on essential services in other sectors and the degree to which other critical entities depend on their services. This should also include considerations of cross-border dependencies.

This white paper is intended to support the discussion on this topic and present the perspective of the EU H2020 funded PRECINCT research project (www.precinct.info). This project investigated the complexities of interrelationships between CIs and how to manage the impacts of cascading effects as a result of hazardous events, with the goal of enabling rapid recovery. The project brought together a broad range of stakeholders from across the CI ecosystem, including industrial actors and research providing organisations. In this way, the project was able to gather varying perspectives and insights from this strong, cross-industry consortium on the topic of interconnected CI and develop meaningful technological solutions to address the associated challenges. This white paper aims to ensure the learnings from this project are shared with interested stakeholders across the community and considered when developing future policy and industry standards in relation to the protection of CI.

In summary, it is the view of the project partners that interconnection of CIs should be considered an essential part of any related policy due to its importance, not only for individual CIs, but also for the collective resilience of the Union economy and citizens. In order to realise this improved resilience there is a need to develop an ecosystem where CI operators are both mandated and supported to engage collectively to mitigate risks of cascading effects associated with interdependent CI.

2. Complexity of Interconnected CIs

With the increasing interdependence of various CIs across Europe and the associated risk of disruption caused by cascading effects, it is essential to understand and manage the dynamics of this extremely complex collection of heterogeneous yet interconnected systems in order to safeguard the interests of the Union.

The complexity of interconnected CIs can be understood when one considers the potential interactions between diverse verticals (for example: emergency services, electricity, food production, telecommunications, water infrastructure, supply chains, etc.), which ultimately results in a significantly broader threat canvas compared to the case of considering a single CI operating independently. The problem is compounded by the range of possible, unanticipated combinations of threats and actions that can affect whole cities, districts or regions.

Because of the complex nature of interactions between interdependent CI and the potential for broad impact across many jurisdictions, a holistic approach is required to ensure resilience of CI within and between member states. A further challenge arises when selecting the scale at which to analyse and manage the problem. This is because the dynamics of cascading effects can vary when one considers interdependent CIs at different scales across the member states. For example, the threat of cascading effects exists with interconnected CIs across different geographical areas, such as districts, cities or regions.

The problem is also not static in nature and the appropriate reaction and/or allocation of resources in response to an incident will depend on the specifics of the incident, size of the area affected and the organisations impacted. This interplay between interconnected CI can also lead to counterintuitive, or “nonlinear”, effects, further complicating decision making aimed at mitigating the consequences of cascading effects.

From this overview of the underlying issue, it follows that there is a need to supervise and manage / coordinate these complex interdependent networks and Cyber Physical Systems of Systems (CPSoS). However, this approach is inherently challenging since the CI ecosystem is characterised by distributed ownership and management structures.

Individual CIs have clear ownership over the protection of their services and understand well how to respond to protect those services. However, it is challenging to define ownership of the interaction between CIs in terms of mechanisms, processes, data sharing requirements, etc., all of which could be implemented to enhance resilience of interdependent CIs. The challenge here is understandable because the overall situation is extremely difficult to assess by individual CIs, as in many cases these only have a local view of their own infrastructure, rather than a wider “system-view”.

To compound this issue many existing critical infrastructure protection (CIP) systems were designed and implemented independently and according to different requirements and use cases. This can create interoperability issues when implementing CIP solutions that require integration with multiple systems. This, in turn, adds complexity and cost to enabling interactions between CIP solutions. Nevertheless, interdependency must be considered in

any risk analysis, including those focused on single CI entities. This is necessary, even in cases of the most secure CI entities, where exogenous factors can affect operations, and therefore these are viable risks that must be assessed.

Direction from policy makers is very important in this context, as they can drive the behaviour of countries and their citizens. The question for policy makers to address therefore centres on how interdependent CIs could be understood and managed, such that decisions can be made on the optimal resource investment for protecting against cascading effects in such complex systems. A clear statement from policy makers and consensus from within the industry on accountability is also required in relation to addressing the issues associated with cascading effects of connected infrastructure. In addition, due to the multi-scale nature of the problem, public-private collaboration solutions that apply across different districts, cities or regions will have to be devised and driven by policy decisions.

3. Critical Infrastructure Coordination Centre (CICC)

Increasing Preparedness and Awareness

Refining the systems and processes for understanding and mitigating the effects of cascading effects of interconnected CIs is important as it can minimise the need for reactive responses to incidents and lack of information leading to resource overallocation, the cost of which will most likely be borne by the public. On-going public-private planning and communications can lead to optimisation of resource allocation by promoting information sharing and development of best practices that will ultimately benefit all Member States.

It is the view of the PRECINCT project that Centralised Critical Infrastructure Coordination Centres (CICCs) can play an important role in enabling communication between interdependent CIs. Such centres can focus on continually simulating and assessing the probable consequences of related threats, an activity that can be replicated at different levels across each Member State to address threats to interconnected CI at district, city, regional levels, as required.

During the PRECINCT project, one of the core issues considered that drives the need for such centralised roles was the challenge of coordination between various stakeholders, such as government agencies, private organizations, and regulatory bodies. Poor communication and restricted exchange of data can lead to delays or inconsistencies in the response to attacks on CI, ultimately leading to delays in recovery. In some cases, there may be overlapping governance and competence areas that further complicate the adoption of effective mitigation strategies.

The importance of this type of centralised role is recognised by the CER Directive [1], which calls for the establishment of the Critical Entities Resilience Group (CERG). This group will enable information exchange between Member States in relation to CI protection, identify and exchange proposals on best practice, and will consider cross-border and cross-sectoral interdependencies.

The CERG will facilitate exchange of information at the Member State-level, which is a broad and necessary role. Other centralised coordination centres also exist within member states covering more limited pockets of the European CI (examples include: Safe.Brussels[1], IAEMO[2], Hellenic National Platform for Disaster Risk Reduction (HNP-DRR)[3], Antwerp's Emergency Planning department[4]). However, considering the complex, multi-scale nature of the problem, it was found in the PRECINCT project that the extent to which such entities were clearly established and focused on interdependencies of CI was insufficient. This severely impacts the ability to offer widescale protection against cascading effects of interconnected European CI. It was also found that, despite the need for such CICC entities, there is a risk that such entities will not develop at a sufficient scale through natural market forces due to cost and complexity constraints, creating the need for governmental intervention at multiple scales through clear policy decisions. Directing the creation of such entities and their focus on interconnected CI through policy discussions is possibly a key role for the CERG.

The Role of the CICC

PRECINCT investigated the role of CICC entities and this paper aims to communicate learnings from the project to be considered in the development of associated policy and governance schemes.

The core role of the CICC considered during the project was to continually analyse interconnected CI at strategic levels, enabling informed, evidence-based decisions to be made about CI interconnectedness, identification of critical risks, preparation of optimised response plans, and running of training simulations.

The key recommendation coming from the project is to ensure policy decisions specifically focus on cascading effects in CI protection by enabling the creation of CICC agencies and support them in gathering information at multiple scales across member states resulting in:

- **Creation / improvement of actionable plans for cascading events**
- **Creation / improvement of emergency response training for cascading events, which can expose (and test) the critical emergency responses in realistic simulation environments**
- **Identification of case studies to be funded, which develop the justification for resource allocation to protect against cascading effects**
- **Exposing unforeseen consequences of triggering events and preparing appropriate responses**

This information is primarily targeted at strategists / planners at different levels across a Member State (e.g. regional-level, city-level, district-level) to help in understanding interdependency issues. The overall goal is to increase preparedness and awareness, and enable the implementation of training scenarios that demonstrate benefits in terms of time / cost impact on CI due to hazardous events.

To make these CICC entities effective they will require a mandate and clear legal status within Member States to ensure adequate security of data, information sharing, participation from CI owners, while enabling it to perform a monitoring and audit role. To be widely effective

1. https://safe.brussels/en
2. https://www.iaemo.ie/
3. https://www.preventionweb.net/national-platform/greece-national-platform
4. https://www.antwerpen.be/contact/dienst-noodplanning

CICCs would need to be replicated at different levels across each MS and would be required to deliver information to oversight bodies (such as the CERG discussed earlier), which would in turn facilitate inter-MS communications and other centralised functions such as: sharing of best practice, defining of minimum standards, development of decision making tools.

The expected result of the approach described here is to combine the effects of 1) enhanced coordination during adverse events, 2) improved abilities to understand, anticipate and prepare for cascading effects, and 3) sharing of lessons learned / best practice across Member States to support interdependent CIs in going beyond resiliency to an "antifragile" state. This concept, introduced by [2], is centred on the premise that predicting all causes and effects of future adverse events is not possible. It is preferable to create adaptive systems, which learn how to better respond to future threats from past experiences, and thus benefit from adverse events [3][4].

The table below summaries some of the key distinctions between CICC and CERG entities:

CICC	CERG
Multiple instances across Member States covering different groupings of CI, providing localised and detailed views of interdependent CI.	Single entity that acts as an oversight body at EU-level.
Continually analyses interconnected CI at strategic levels, enabling informed, evidence-based decisions to be made about CI interconnectedness, identification of critical risks, preparation of optimised response plans, and running of training simulations.	Enables information exchange between Member States in relation to all types of CI protection, identifies and exchanges proposals on best practice, and considers cross-border and cross-sectoral interdependencies.
Key role is to gather information at multiple scales across member states.	Receives and assesses information from various CI-focused entities across all Member States, including the various CICC entities, to provide EU-level oversight and guidance on protection of CI within the Union.
All information and findings primarily targeted at strategists / planners at different levels across a Member State (e.g. regional-level, city-level, district-level) to help in understanding interdependency issues.	Could mandate Member States to create CICC entities through policy decisions.

Building Trust with Stakeholders

The approach of implementing CICCs at multiple levels across Europe is driven by the need for a systemic solution for the protection of interdependent CI. The core issue with this holistic approach is that widescale implementation relies on adoption and engagement by individual owners of CI elements.

Within the PRECINCT project, interactions with owners of CI elements highlighted barriers to this engagement, the main issue being related to data sharing. The issue is created by the security risk of disclosing vulnerabilities to ill-intentioned agents through sharing the information necessary to understand the interdependency of CIs. For any CICC to function effectively, it will be critical to convince owners of CI that the benefits of engaging outweigh the risks of data sharing.

Trust-building among stakeholders and decision makers is crucial in any sector. This is especially so for CI management, where data sharing can go against established CI risk management processes. This presents a clear dilemma for CI owners and results in a clear barrier for adoption of centralised solutions. To encourage willingness and trust to share data among CI operators, it will be necessary for policy makers to focus primarily on clearly articulated governance models outlining central data management processes that address data sovereignty and control.

This theme of trust also extends to the selection of technical solutions that support communication between CI entities. The security management and the appropriate communication of security measures related to the technical solutions should therefore also be high on the agenda for policy makers wishing to alleviate barriers to the mitigation of cascading effects.

Based on the above discussion it can be seen that demonstrating the benefits of multi-CI interactions is crucial for building and maintaining trust with CI operators. It is recommended that these benefits be communicated at both strategic / leadership and operational levels in CI organisations to garner support and engagement in CIP strategies and technologies. Such demonstrations could utilise simulation technologies, such as Digital Twins (DTs), to reproduce past critical situations and showcase the effectiveness of management solutions that consider the effects of interconnected CI. Such an approach will need to be carried out in a focused way as no city or region is the same, and metrics for understanding the effectiveness of different CI management interventions at city / regional levels will vary on a case-by-case basis. As such, any case studies funded to develop the justification / evidence for CI owner engagement to protect against cascading effects should involve direct interactions with all stakeholders from the early stages, ensuring the specifics of future users' needs are addressed during the design process.

Diversity is also an important consideration here because of the potentially widespread impact of CI cascading effects. Diversity can be integrated at the root of policy decisions when defining required stakeholder engagements and making provisions to ensure the full community of those impacted by services from CI are fully represented. In addition, diversity can help when deciding on technologies and processes to implement to ensure they are effective in reacting to and/or preventing cascading effects across broad communities.

For example, considering cognitive diversity that arises by gathering the perspectives of a variety of people (different genders, ages, professions, etc.), it follows that diversity is critical to broadening the solution space for enhancing interdependent CI resiliency. This is because bringing diverse groups of people together enables multiple points of view to emerge, reduces perception bias and group-thinking by providing a holistic view of highly complex situations,

helping to identify vulnerabilities. Diversity can also be considered in how reactions are planned and resources allocated to prevent cascading effects, ensuring equality of responses and resources across different communities of potentially impacted stakeholders.

Unified Vocabulary and Metrics

As discussed, complexity is inherent to systems involving interconnected CI. The absence of a unified vocabulary and metrics to assess resilience in a qualitative or quantitative manner enhances the difficulty of effectively planning resource allocation and can lead to expensive, reactive approaches for mitigation of cascading effects.

It is envisaged that one of the key functions of any CICC will be to develop metrics and tools to understand how to optimally allocate resources within their area of influence to minimise adverse effects on supply of services due to the interconnection of CI entities. Such metrics provide a route for CI emergency planners to allocate their resources more effectively and efficiently. Essentially, meaningful metrics can be used to better understand how different choices of preventative measures can impact inter-CI resilience, leading to more optimal resource investment.

The choice of these metrics for evaluating CI resilience is challenging and will depend on the scenario being investigated. To ensure these metrics are meaningful, engaging with all affected stakeholders is important, and these should include regional authority personnel, operators of the CIs, and representatives from users groups. Based on this engagement, guidance could be provided by policy makers to clarify acceptable metrics or the characteristics of such metrics.

It has been discussed that sharing of data across CI is key for the implementation of solutions that tackle cascading effects. Along with the willingness and trust from CI operators to share data that was discussed earlier, this also requires **data interoperability** (a technical and organisational culture issue). The recommended approach to address this issue is to ensure the ecosystem can support the development of standardisation bodies that work to create industry-driven, standardised vocabularies (ontologies), and data exchange protocols that facilitate inter-CI collaboration and communication in the long term.

It is recognised that related activities are underway with recent efforts as part of the CEN Workshop Agreement [5]. Ensuring such standards facilitate understanding of interdependencies and interconnections between CIs will be important. In this way, the impact of failures in one CI entity could be understood by other CIs through standardised interfaces / data exchange.

Cross-Border Issues

A number of inter-country issues became apparent during the PRECINCT project, which added to the complexity and resource requirements needed from CI operators to comply with regulatory requirements. This is because regulatory requirements tend to vary across different regions and countries, creating additional challenges for commercial organisations offering services and products across borders. Essentially, this is driven by how CI is defined and regulated in different countries, and this creates issues for CI networks spanning multiple

countries. These multiple layers of legislation and varying regulation compliance requirements, both local and international, may hinder the development of generic CIP solutions, which may need instead to be developed for specific local needs and contexts. Policy decisions should consider such complexities when mandating actions from CI organisations providing cross-border services, potentially providing supports through dedicated inter-Member State agencies that can work to harmonise regulation and foster improved resilience through smoother communications channels.

Semantic modelling (i.e., controlled vocabularies, taxonomies, ontologies) can be considered here to mitigate cross-border challenges. Such modelling approaches could be maintained centrally by the EU, upon which standards can be defined and implemented. The aim of such modelling and associated standards would be to enable 1) unified identification of infrastructure that could be considered critical, and 2) enhanced communication between Member States. On this second point, translation of CI-related terms and processes to the various languages that exist in the EU is essential, but must be done in such a way that ensures the same meaning is maintained across country borders.

Cost Considerations

A significant challenge related to inter-CI resilience protection is covering the costs of enhanced protection against threats that are outside of the immediate responsibility of a particular CI operator. This calls for specific budgets allocated to measure and increase resilience of interconnected CIs. It is understood that such budgets do not yet exist, and support to unlock such funding would be necessary at the city council, regional or even national level. Existing budget lines would likely be needed initially to support developing metrics that demonstrate ROI and justify further investments by governmental agencies. The exploration / simulation activities discussed earlier to articulate the potential impact of cascading effects of interdependent CIs would be highly beneficial during budget allocation discussions and therefore a critical element in the required efforts to enhance resilience of CI.

It is noted that budget considerations would not just require the funding for analysis and justification but also require funding for implementing resilience enhancement strategies. Policy could consider the importance of these impact assessment activities in order to support financial planning at governmental levels.

CIP Market Considerations

It is expected that as the public becomes more aware of the risks facing interconnected CI, there will be increased demand for solutions that defend CI from these risks. In anticipation of this, the Critical Infrastructure Protection (CIP) market needs to be ready to meet the resulting demand. Part of overcoming this issue is to ensure policy and standardisation are in place to support the developing ecosystem.

A comprehensive analysis of the CIP market was conducted as part of the PRECINCT project, which highlighted certain issues that can be considered during policy development. Overall, the CIP sector is a highly fragmented, complex, and global market. The market dynamics

in Europe have been found to be more complex than other regions, such as the US, with municipal, regional and national dimensions to consider and higher linguistic and cultural diversity. The EU is also introducing coordination directives, such as the recent CER and NIS-2 directives in 2022 [1][6][7], which are expected to influence the market dynamics in the medium term and provide incentives for adoption of coordinated CI risk management processes [8]. The competitive yet fragmented CIP market currently lacks integrated solution to identify, prevent and manage cascading effects across interconnected CI, which poses challenges for implementation of policy decision related to this topic.

It follows that compliance with new regulations will be a significant driver for adoption of advanced CIP solutions, but also a concern from a cost and administrative-load perspective. Any new technologies needed to communicate and coordinate between CI service providers will require additional funding for dedicated training, and adaptation within CI management procedures. Ensuring awareness within the market regarding policy developments and upcoming legislation will be important for enabling CI owners to have the time to prepare for legislative changes. This awareness within the market is also important to ensure time is provided to developers of CI protection services and digital solutions to create products and service offerings such that solutions can be deployed at scale. This helps ensure costs of compliance are minimised, which is particularly important within this cost-sensitive market. The time to develop solutions is also seen as critical due to the complex global market within the CIP sector, where systems and solutions will need to be specific in order to alleviate the challenges of different classes of CI actors.

Another challenge to consider concerning sustainable roll-out of technological solutions to support compliance with new legislation is the secrecy inherent to the CI management market. This is, of course, necessary to avoid exposing vulnerabilities, as discussed earlier, however, from a market development point-of-view, it can also hamper the rate at which the CIP solution market can grow due to restrictions on sharing implementation information and / or access to certain (potentially bespoke) solutions. To address these constraint, standardisation of CIP solutions should, where possible, prioritise solutions that balance robust security with the ability to scale solutions across the sector, with the overall aim to facilitate uptake at low cost.

Supporting this low-cost requirement is the adoption of cloud-based solutions, which is increasing across all sectors, including critical infrastructure. This presents an opportunity for companies that provide cloud-based CIP solutions, which can take advantage of cloud technologies to provide greater scalability, flexibility, and cost-effectiveness.

Certain considerations, particularly around security, are necessary when considering cloud-based solutions for CI. For these solutions, it is necessary to develop specific classes of contracts that apply to this market, along with robust certification and audit mechanisms. European-level initiatives are in place to address such issues, such as GAIA-X [9], where the goal is to link cloud services to share data across a trustworthy environment.

4. Technology To Support CICCs

The purpose of this section is to share learnings from the PRECINCT project on specific technologies that have the potential to support the CI sector in better understanding the impact of interconnected CI and mitigation of related cascading effects.

From the discussion earlier it is clear the topic of interconnected CI is complex, however, there are technology-based solutions that can support enhanced resilience in these CI networks. Generally speaking, the development of emerging technologies, such as artificial intelligence (AI), digital twins, and blockchain, presents opportunities for CIP solutions that can leverage these technologies to provide more effective and efficient security solutions.

The PRECINCT project explored the potential of various tools and processes to mitigate the effects of cascading effects. These tools addressed some of the previously discussed challenges around understanding this complexity and helping users to enhance resilience and / or derive plans for rapid recovery following a disruption to services. The key requirements for this technology were **affordability, effectiveness, security, and transferability**, all of which were fundamental to allow solutions to be scaled to multiple levels across member states.

A focus of the technology explored in PRECINCT was to model the current and future behaviour of territory-based interdependent CIs in a variety of conditions and configurations, to anticipate threats, to detect anomalies, and understand dynamic interdependencies and cascading effects. This resulted in optimised command structures and coordinated responses between CIs and first responders, thereby enhancing the resilience of the territory analysed. Such a modelling approach has the potential to support previously discussed needs in the sector, such as developing the information required for buy-in from CI owners and justification of resources to protect against cascading effects of interdependent CI.

The PRECINCT Framework was key to the technologies explored in PRECINCT. This was developed to facilitate the modelling of dynamic interdependencies and cascading effects in complex networks of CI, as well as to quantify resilience (using a specific Resilience Index) and identify short-term and long-term resilience enhancement measures. To efficiently manage risks across Europe and to develop sustainable mitigation/adaptation strategies, the Framework facilitates the representation of multiple hazards, their potential spatial and temporal interrelations, their resulting risks across interdependent sectors, and how these risks may evolve over time. The output of this can be employed to prepare and adapt to multiple hazard processes, thus enhancing resiliency.

The framework is adaptable and allows CI communities of different size and make-up, operating at various scales within a Member State, to integrate the specifics of their system of CIs. This enables different systems of interconnected CIs to coordinate security and resilience management using the framework's modelling and assessment capabilities.

Central to the modelling capabilities explored in PRECINCT were **Digital Twins**, which combine data / IoT networks, AI and 3D visualisation. This technology has been proven in recent years as a promising decision support tool for various applications. Building on this, PRECINCT has

employed Digital Twins to investigate cascading effects within interconnected CI in the context of a specific region / city. The general idea is that Digital Twins link physical assets to virtual representations and facilitates a bi-directional communication link, supporting optimisation of resource allocation, control loops through sensing and actuation, and exploring "what-if?" scenarios. The tool can therefore be used in the context of training to explore how responses to adverse events can be handled using information from previous real scenarios or based on possible future attacks. For more information, see for example [10].

AI-based tools were key to the Digital Twins and are candidate technologies to identify anomalous behaviour in a network of CIs and has achieved excellent results in anomaly and intrusion detection systems. To enable such AI-based tools, semi- and unsupervised machine learning techniques can be used to detect anomalies and attack patterns within CI systems in a holistic way, characterising their normal / abnormal behaviour and investigating possible impacts on other interconnected stakeholders. In addition, machine learning algorithms can be applied to determine the optimal strategy for resilience enhancement.

A **Serious Games** approach was employed as an innovative vulnerability assessment tool for investigating cascading effects in complex multi-system living labs, where the aim was to support development of new resilience enhancement services. Serious Games are primarily used for training purposes as a form of experiential learning that employ simulation techniques as a cost-effective alternative to often high risk and costly real-life activities. Users are immersed in realistic and dynamic simulations of CI in which they can experience "attack" or disaster scenarios and observe how their responses affect the unfolding of the situations. The expectation is that the use of Serious Games will result in the identification of previously un-anticipated threat combinations involving cascading effects across multiple sectors. Another key outcome is increasing the resilience across an entire CI network by indicating the activities which allow faster recovery from an incident. Examples of the application of serious games from PRECINCT can be found in [11].

PRECINCT enabled various threat scenarios to be simulated and an understanding of the impact various mitigating effects can have on specific resilience measures. This approach is expected to be superior to traditional risk-based approaches since it can explore a very large number of potential enhancements and resulting outcomes, and is thus effective in meeting the complexity challenges highlighted earlier. Based on the simulation results expressed through the resilience scores, it is possible to estimate how strongly each CI entity is affected by given threats and to identify entities that are in danger. This information can be further used to identify protection measures, e.g., if a given CI entity turns out to be affected frequently and severely, it might be necessary to protect it better or to ready a backup in case it fails.

It is expected that tools such as these could form the basis of supporting the work of entities like the CICCs discussed earlier, along with the Critical Entities Resilience Group, outlined in the CER Directive [1], particularly in activities related to "developing best practices, guidance materials and methodologies, and cross-border training activities and exercises to test the resilience of critical entities", as described in that directive.

One of the core functionalities of the PRECINCT Ecosystem Platform was its ability to enable communication of data across CIs and distribute data for use in Digital Twins. The data

sources can be generalised IoT data from sensors and actuators, which are connected to a communications component that protects the data through blockchain-based key management techniques. This ensures total visibility across the entire system of interconnected CIs, providing a link between the physical security layer and computing infrastructure. Such approaches aim to mitigate challenges associated with siloed data sets, security by secrecy that lead to poor communication and coordination between interdependent CI entities. The key benefit from such secure communication channels is an ability for CI operators to be more objective in their decision making due to improved communication across key CI. This can lead to increased situational awareness, which facilitates improved resilience against cascading effects.

To enable this approach, the **PRECINCT Ecosystem Platform** integrated multiple scalable and often open-source components. These included, for example, AI-based and Big Data Analytics (BDA) infrastructural services, Semantic Connectivity and Dynamic Integration infrastructure, along with a situational awareness user interface / data analytics visualizer. This was coupled to the computational, networking and storage resources needed to deploy and interconnect the various tools.

Despite the benefits of these various technologies in enabling improved protection of interconnected CI, there were certain challenges highlighted through the PRECINCT project:

1. There is a potential for a lack of trust in new technological solutions, especially ones that involve predictive decision support capabilities. This acceptance issue is particularly evident when asking CI operators to accept decisions of non-human systems in critical situations.

2. Trust is also an issue between CI entities, both in terms of data sharing and in being confident that reactions to cascading effects made by one entity will be in the best interests of others.

3. The culture of the CI market has been found to be resistant to change, often demonstrating long and complex procurement cycles.

4. Regulatory compliance can also be a challenge, especially when considering cross-border interactions and data sharing. Technologies often do not inherently recognise borders and so inter-state data sharing issues will have to be managed during the solution design phase, enhancing the complexity of solutions.

5. Long development cycles for new technologies in the CI market are also a challenge. These are often driven by long periods where proof of concept solutions must run in parallel with older solutions, requiring additional resources from CI entities, which might not exist.

Further details of technology developed during the PRECINCT project can be found at: https://www.precinct.info/en/publications/articles-press-releases/.

5. Conclusions

With the growing interdependency of the Union economy the European Parliament and Council has emphasised the need for harmonised rules to help improve resilience of CI and provide associated supporting measures. This is driven by the indispensable role of CI in enabling essential societal and economic functions across the Union.

This white paper is intended to support the discussion happening at the EU-level on this topic [12] and present the perspective of the EU H2020 funded PRECINCT research project, which investigated the complexities of interrelationships between CIs. The white paper aims to ensure the learnings from this project are shared with interested stakeholders across the community and considered when developing future policy and industry standards in relation to the protection of CI.

In summary, it is the view of the project that interconnection of CIs should be considered an essential part of any related policy and development of industry standards due to its importance, not only for individual CIs, but also for the collective resilience of the Union economy and citizens. In order to realise this improved resilience there is a need to develop an ecosystem where CI operators are both mandated and supported to engage collectively to mitigate risks of cascading effects associated with interdependent CI.

The summary of key topics below is intended to assist the wider CI community (policy, standard, industry and research organisations) in effectively enhancing the reliance of interconnected CI:

Theme	Description
A Holistic Approach	Cascading effects among interdependent CI have the potential for broad impact across many jurisdictions, requiring a holistic approach to ensure resilience of CI within and between member states.
Managing Complexity	The dynamics of cascading effects vary depending on the specifics of the incident, size of the area affected and the organisations impacted. This leads to complexity in understanding system dynamics and determining optimal resource investment to protect CI. Regulations are needed to ensure CI owners share the required information to manage this complexity centrally but in such a way as not to be overburdened with monetary or administrative burdens.
Accountability	A clear statement from policy makers and consensus from within the industry on accountability is also required in relation to addressing issues related to cascading effects of connected infrastructure. Accountability and governance structures in this space are essential and need to be created where they do not exist.
Multi-scale in Nature	Due to the multi-scale nature of the problem, public-private collaboration solutions that apply across different districts, cities or regions will have to be devised and driven by policy decisions.

Centralised Coordination	Policy decisions should specifically focus on cascading effects in CI protection by enabling the creation of centralised coordination agencies with jurisdiction over groups of interdependent CI. Policy should support these entities to effectively gather the required information at multiple scales across their areas of influence.
Trust	To encourage willingness and trust to share data among CI operators, it will be necessary for policy makers to focus primarily on clearly articulated governance models outlining central data management processes that address data sovereignty and control.
Security	Security management and the appropriate communication of security measures related to the technical solutions should therefore also be high on the agenda for policy makers wishing the alleviate barriers to the mitigation of cascading effects.
Diversity	This topic can be integrated at the root of policy decisions when defining required stakeholder engagements and making provisions to ensure the full community of those impacted by services from CI are fully represented.
Cross-Border Issues	Regulatory requirements tend to vary across different countries and this creates compliance challenges / burdens for CI networks spanning adjacent countries. Such CI would benefit from harmonised regulation that fosters improved resilience through smoother cross-border communications channels. Semantic modelling (i.e., controlled vocabularies, taxonomies, ontologies) can be considered here to mitigate cross-border challenges. This can enable 1) unified identification of infrastructure that could be considered critical, 2) translation to the various languages of the EU, and 3) enhanced communication between Member States.
Cost	Covering the costs of enhanced protection against threats that are outside of the immediate responsibility of a particular CI operator is a significant challenge. This calls for specific budgets allocated to measure and increase resilience of interconnected CIs. Policy development can play a key role in highlighting the impact of interconnected CIs in order to support budget justification and financial planning at governmental levels. Resulting budgets need to be specific to the circumstances of the networks of CI examined and will depend on the area of influence and the nature of threats considered.
Market Growth	Compliance with new regulations will be a significant driver for adoption of advanced CIP solutions that addresses market needs related to interconnected CI. Ensuring awareness within the market regarding policy developments and upcoming legislation will be important for providing CIP solution / service providers the time to effectively prepare for legislative changes. In support of these efforts, standardisation of CIP solutions should, where possible, prioritise solutions that balance robust security with the ability to scale solutions across the sector, with the overall aim to facilitate uptake at low cost, which is a key consideration in the CIP market.

It is interesting to consider how the recommendations discussed here align with the recent CER Directive in terms of timeline and roadmap. The goal of this Directive is to ensure that CI are sufficiently resilient to the increasingly complex threat landscape that exists today (e.g. natural disasters, terrorism, sabotage, etc.) and is expected to develop with time [13]. The CER Directive has already come into force as of January 2023 and Member States have until October 2024 to ensure the requirements of the directive are implemented in national law. This is a relatively brief timeline, yet creates an opportunity to revise how CI protection is implemented, particularly in the area of interdependent CI. The recommendations and actions outlined in this white paper can therefore be considered during the development of CI protection strategies at European and national levels, which must now take place to meet the adoption deadline of January 2026.

The European Commission will assess each Member State's compliance with the CER Directive, which is mandated to happen by July 2027. Considering the discussion within this white paper, it seems appropriate that any such assessment should specifically address the extent to which provisions are made within each Member State's national laws to account for threats due to the increasingly interdependent nature of CI.

Finally, this paper presented an overview of specific technologies explored during that PRECINCT project. These have the potential to support the CI sector in better understanding the impact of interconnected CI and mitigation of related cascading effects.

The key requirements for this technology were affordability, effectiveness, security, and transferability, all of which were fundamental to allow solutions to be scaled to multiple levels across member states. A focus of the technology explored was to model the current and future behaviour of territory-based interdependent CIs in a variety of conditions and configurations, to anticipate threats, to detect anomalies, and understand dynamic interdependencies and cascading effects.

The technologies examined by PRECINCT aimed to provided insight on optimised responses to hazardous events, thereby enhancing the resilience of the territory analysed. The approaches examined have the potential to support previously discussed sectorial needs, such as developing evidence-based arguments required for buy-in from CI owners and justification of resources to protect against cascading effects of interdependent CI. This approach supports efforts to promote long-term benefits for the Union, including economic stability, public safety, and environmental sustainability.

Further information on the specifics of the PRECINCT project can be found at https: //www.precinct.info.

References

[1] DIRECTIVE (EU) 2022/2557 Of The European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC. Online. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[2] Taleb, N. N. (2013). Antifragile. Penguin Books.

[3] Bangui, H., Buhnova, B. and Rossi, B, 2022, Shifting towards Antifragile Critical Infrastructure Systems. In Proceedings of the 7th International Conference on Internet of Things, Big Data and Security (IoTBDS 2022), pages 78-87

[4] Munoz,, A., Billsberry,, J. & Ambrosini,, V. (2022) Resilience, robustness, and antifragility: Towards an appreciation of distinct organizational responses to adversity. International Journal of Management Reviews. 24: 181–187.

[5] CEN Workshop Agreement (CWA 18023:2023) August 2023. Online. Available: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/RI/cwa18024.pdf

[6] European Commission, 2022, "CER and NIS-2 Directives enter into force to strengthen EU's Resilience". Online: Available: https://ec.europa.eu/newsroom/cipr/items/764849/en. (Accessed 08th September 2023).

[7] NIS-2 directive Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Online. Available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[8] Critical Infrastructure Protection Market Size, Share, Revenue Forecast & Opportunities | Markets and Markets (2023). Available at: https://www.marketsandmarkets.com/Market-Reports/critical-infrastructure-protection-cip-market-988.html (Accessed: 30 May 2023).

[9] Gaia-X, About Gaia-X. Online. Available: https://gaia-x.eu/what-is-gaia-x/about-gaia-x/

[10] Nguyen, L., Segovia, M., Mallouli, W., Oca, E.M.d., Cavalli, A.R. (2022). Digital Twin for IoT Environments: A Testing and Simulation Tool. In: Vallecillo, A., Visser, J., Pérez-Castillo, R. (eds) Quality of Information and Communications Technology. QUATIC 2022. Communications in Computer and Information Science, vol 1621. Springer, Cham.

[11] Meisam Gordan, ili Ko, Páraic Carroll, Daniel McCrum, Mona Soroudi, Sandra König, Stefan Schauer, Lorcan Connolly, A Serious Game Conceptual Approach to Protect Critical Infrastructure Resilience in Smart Cities, 14th International Conference on Applications of Statistics and Probability in Civil Engineering (ICASP14), Dublin, Ireland, 2023.

[12] European Commission: 2022, "Critical Infrastructure: Commission accelerates work to build up European resilience". Online. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238.

[13] Cyber Risk GmbH. "The Critical Entities Resilience Directive (CER)". Online. Available: https://www.critical-entities-resilience-directive.com/ (Accessed 08th September 2023).

PRECINCT

PRECINCT COORDINATOR

INLECOM COMMERCIAL PATHWAYS

PRECINCT Project Coordinator
Dr Takis Katsoulakos – Managing director

PRECINCT Project Manager
Jenny Rainbird - Head of EU Projects Delivery

Inlecom Commercial Pathways
Room 12, Gateway Business Suites,
The Reeks Gateway, Killarney, Co Kerry, V93 PPA0

PRECINCT_PM@inlecomsystems.com

Please, follow us on LinkedIn or Twitter and keep up to date
with our news items and downloadable content at **www.precinct.info**