EUROPEAN CRITICAL INFRASTRUCTURE

PIETER-JAN VANDOREN
THE BRUSSELS SCHOOL OF GOVERNANCE

STUDENT PAPER 2023

TEPSA
Trans European Policy Studies Association

Co-funded by
the European Union

Abstract

With the war in Ukraine, the importance of critical infrastructure becomes clear. Europe can ask itself; how is the critical infrastructure in Europe protected? In this policy brief, I will go through the legislative elements that put together the defence of the European critical infrastructure and argue that, while the EU is going on the right track, they have been consistently lagging behind.

What happens when the lights go out?

As the war keeps raging on in Ukraine, the EU has been dealt front-row tickets to the devastating effects of critical infrastructure being destroyed. Constant bombings on the energy infrastructure and temperatures dropping far below the freezing point forces Ukrainian citizens to flee the country to survive (Fleming, 2022). Attacks near the Zaporizhzhia nuclear plant damaged the electricity grid to such an extent that it had to rely on a few diesel generators in order to prevent a nuclear meltdown (Olearchyk, 2022). Finally, according to Russian media, Russian soldiers were evacuated after rumors that Ukrainians were plotting to blow up the dam, flood the city of Cherson, and kill thousands of inhabitants (Seddon, 2022).

Not only in Ukraine, but also in Europe, attacks on critical infrastructure are taking place. In France, major internet cables were cut in October 2022, leading to a slowdown in internet trafficking from and to France (Leicester, 2022).

Three weeks ago, train lines were cut in Germany, effectively halting train passage in the Northern part of Germany (Schmitz, 2022). Most famously, in the last days of September, the Nord-stream pipelines were sabotaged within the economic zones of Denmark and Sweden (Milne, 2022).

These recent events have highlighted the importance of Critical Infrastructure Protection (CIP). Without a plan for a comprehensive CIP, all infrastructure in Europe is essentially at risk of sabotage, potentially leading to massive disruptive events and threatening the basic conditions necessary for people to live, such as access to clean water, food, and energy. This highlights the need for a coherent plan to prepare, resist and recover from an attack on CI.

A European Plan for action?

Since 2006, there has been a European Programme for Critical Infrastructure Protection (EPCIP), the purpose of which was to create a legal framework to protect the European infrastructure after a series of terrorist attacks. This was followed in 2008 by the European Critical Infrastructure (ECI) Directive (Commission, 2008). It was seen as the first attempt to provide actual legislation for CIP. A review done by the European Commission in 2019 found that the directive was not able to adequately address the possible problems and was outdated (Commission, 2019). This resulted in the draft of a new directive in 2020 designed to specifically addresses the shortcomings mentioned in the 2019 review (Commission, 2020).

As the draft turned into law in the summer of 2022, it took just two months for the European Commission to realize that the developments around the world asked for, not just a simple update of the previous ECI Directive, but a radical shift.

No longer were non-state actors or distracted employees the main risk of damaging the critical infrastructures, but state-sponsored hybrid actions, with the purpose of sowing division within Europe. As a result, on the 18th of October, the head of the European Commission Ursula Von der Leyen proposed a five-point action plan, to speed up the process of protecting critical infrastructure. While this action might seem commendable, it does not solve the problem at heart.

Europe, a guiding light?

In the 2020 directive on critical infrastructure, the European Commission already acknowledged the various shortcomings of the original ECI Directive of 2008. One example was the fact that the 2008 directive only included two sectors; energy and transport. The 2020 directive, in contrast, provides eleven sectors thereby including banking, financial market infrastructure, health, drinking water, public infrastructure, food, space, digital infrastructure, and wastewater. This broadening of the scope recognizes the fact that people not only drive around with trucks and use the heating at home, but also eat, drink, and try to stay healthy.

Another improvement in comparison to the 2008 Directive was the acknowledgment of the increasingly complex risk landscape, with state-sponsored hybrid threats and natural hazards such as climate change. Additionally, new technologies such as drones and 5G cause new challenges to arise, thereby further complicating the process of securing the CI. Finally, increasing digitalization and the interconnectedness of services make operators are more and more dependent on each other (Commission, 2020). See appendix 1 for a further overview of the interdependencies of infrastructures.

A final realization of the 2020 Directive was the lack of uniformity in identification, regulation and support for the critical entities. This led to different treatments by national governments for similar types of CI in Europe. First, it led to some CI not being identified as being critical, while others were. Second, it subjected some CI to strict safety regulations, while others were not. Third, it led to no government support for some CI while others received plenty of it. It is easy to imagine the frustration for the operators, being listed as critical infrastructure and completing the additional paperwork, while your colleagues on the other side of the border do not have to deal with the hassle.

Seeing the light and walking away from it

After addressing all these shortcomings, the European Commission understood that action was needed. As a result, the 2020 directive included four possible options to choose from (see appendix 2). These options ranged from option 1: keeping the 2008 Directive and adding some voluntary measures within the existing EPCIP framework, to option 4: replacing the 2008 Directive and forming a new European Agency dedicated to the protection of critical infrastructure (Commission, 2020).

After describing the four options, the Directive chooses to take option three. This option provides the replacement of the current (2008) ECI Directive, sets out minimum requirements for the resilience of the CI of Member States, provides support for the identification of the ECI, and finally, the regulatory implementation would be supported by a dedicated knowledge hub within the Commission. The extent to which this knowledge hub will be able to fulfill all their mentioned support functions will remain to be seen, with only 7 FTEs planned (Commission, 2020).

While the Directive explains that options 1 and 2 are not far-reaching enough to deliver the desired changes it does not explain why option 4 is not chosen. The Commission advises taking option 3, because of the political feasibility, the flexibility it provides, and finally because of the complementarity to existing sectoral frameworks. While these arguments are all convincing, legislation should not be made because it is easy, but because it should address pressing issues. By choosing option 3, they made a mistake, as I will explain further.

Looking into the darkness.

Option 4 encompasses all the elements of option 3 and additionally mentions the formation of a dedicated EU agency responsible for the resilience of critical infrastructure. Looking at the events that have taken place during the past months, this EU agency would have served its purposes well in these critical times.

First, as the interconnectedness between European countries is rising, the likelihood of a cross-border crisis when infrastructures fail, increases (Fritzon, Ljungkvist, Boin, & Rhinard, 2007). Since these failures impact multiple countries, it would require a dedicated EU agency to set out the rules and intervene in crises by serving as a coordination center. The difference with the knowledge hub as described by option 3, is that the EU agency could intervene, keep a constant eye on the situation and perform proactive analysis and research to build a more resilient critical infrastructure.

Second, the increased interconnectedness does not only increase the number of cross-border failures, but can also spread to other CI, creating a cascade effect (Luiijf, Nieuwenhuijs, Klaver, Eeten, & Cruz, 2008). These cascades take place when CI that are interdependent fail.

While interdependencies between CI cannot be avoided, mapping out the level of interdependencies and possible risk flowing from it should be mandatory. Again, since CI are becoming more and more international as the backbone of the single European market (Gheorghe, Masera, De Vries, Weijnen, & Kroger, 2007), it is necessary to have a supranational organization supervising it to maintain the overview. As the current knowledge hub does not have the FTEs to perform all these tasks, it becomes once more apparent why a dedicated EU agency would be necessary.

Third, as the CI are predominantly owned by private players, it is important to involve them in the dialogue of handling the challenges associated with implementing the necessary measures to protect the CI. Since most private players are multinational companies, it is best to have a single international point of contact to have a streamlined flow of communication (Renda & Hammerli, 2010). This issue could be resolved by the formation of a single supranational agency.

How to put on the lights?

Having discussed the necessity of an EU agency specifically devoted to the protection and resilience of the CI, it could be interesting to look at the necessary implementation steps to effectively realize it.

First, and foremost, it would be necessary to convince the Member States of the practical use of the agency, since it will have to be ratified by them before it can be implemented. In the 2020 Directive, the option was already listed, meaning that it was within the realm of possibilities.

Unfortunately, no further explanation was given as to why it was not chosen. However, due to the recent attacks on critical infrastructure all over Europe, this need for convincing is gradually decreasing.

On the 18th of October, the European Commission itself issued a recommendation urging Member States to go beyond the current framework, which they agreed on two months ago. Furthermore, they mention that action is urgently needed and that the EU should step up its capacity to protect CI (Commission, 2022).

Second, since all the directives taken related to CI are based on its relevance to the internal market (Commission, 2020), we can consider it as a shared competence. As a result, it is within the legal bounds of the EU to form a new agency.

The third issue would be the budget. The European Union works with a Multiannual Financial Framework (MFF) that directly allocates money according to different priorities over a period of seven years. While the MFF has allocated about 1.100 billion euros for both the day-to-day operations and long-term objectives, it still has some financial flexibility (Becker, 2019). Already in 2018, it was argued that budgetary flexibility would be necessary to deal with 'the unstable geopolitical and domestic conditions' (Commission, 2018).

According to the EU, there is a budget for 'non-thematic special instruments, addressing generally unforeseen circumstances or new priorities' with a maximum amount that can be used for special instruments of 21 billion euros (E. Commission, 2022). Given the importance of the situation, this reserve could be put to use to support the founding of the new agency.

The illuminated path forward

Having dealt with the main impediments to the formation of the agency, we can now focus on the agency itself. Based on the issues highlighted by the European Commission, the issues as addressed by the literature, and the issues arising from the current crisis with Russia, we identified the following key functions of the new agency:

1.Identification of the CI in all Member States,
2.Coordination center during crises,
3.Knowledge center containing best practices,
4.Single point of contact for private companies and Member States,
5.Setting of resilience standards,
6.Stress testing performed by the agency,
7.Collecting data from all CI,
8.Mapping of future challenges,
9.Providing funds to Member States for the implementation of a heightened standard,
10.Continuous training of key personnel.

With these ten points in place, it would be interesting to see how this agency could react in the case of the Russian invasion of Ukraine.

First, the EU agency would be able to proactively draft a European-wide risk assessment of the war in Ukraine and the implications of it. In collaboration with this agency, the individual Member States could formulate a national security strategy specific to the previously identified CI and list them from high risk to low risk, based on the already assessed interdependencies with other CI or the cross-border impacts in case of failure.

In case of any unexpected failures, affected Member States could reach out to the agency, as a single point of contact, to ask for the expertise and more information regarding possible actions to take. Meanwhile, the Agency itself could warn neighboring Member States to explain which CI are possibly at risk due to the changing environment. Knowing the interdependencies, operators of CI at risk can look at the best practices to mitigate the consequences of the failure of related CI. Since stress tests were regularly conducted and key personnel was trained according to the standards of the agency, it would greatly facilitate the shifting of the operational capacity of the CI to deal with the shifting strategic environment.

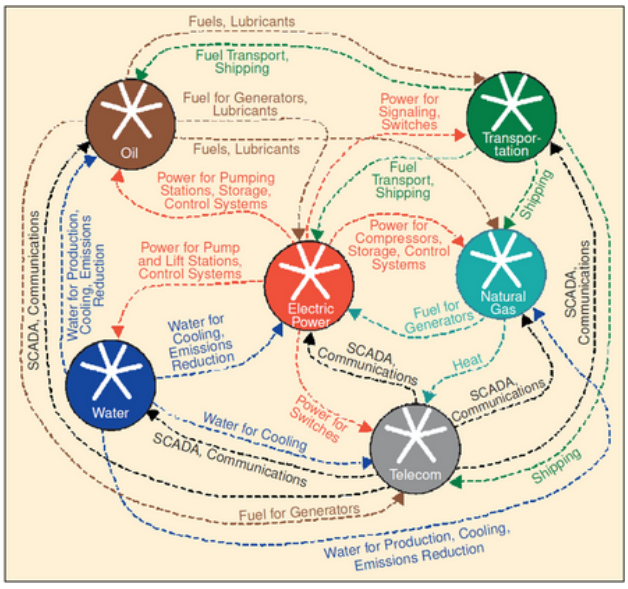
Concluding remarks

With the changing geopolitical environment, it is clear that the EU should take more action to safeguard the functioning of its CI and the stability of the European Union. The actions that have been taken by the European Union have always been on the right track but were just small steps toward the goal. Unfortunately, with Russia's actions, the time has run out to continue taking these small steps. In this policy brief, I highlighted the current path of action that the EU should take, by founding a new agency with the specific purpose of increasing the resilience of the European CI.

While not all Member States will be equally happy to have yet another competency taken over by the European Union, this policy brief has clearly shown from multiple angles that a strong European agency that not only constantly coordinates, but also improves the resilience of the CI is not a luxury, but a must.

Appendices

Appendix 1: Examples of infrastructure interdependencies (Rinaldi, Peerenboom, & Kelly, 2001).



Appendix 2: Impact assessment (Commission, 2020)

The impact assessment that supported the development of this initiative explored different policy options to address the general and specific problems described earlier. Besides the baseline situation, which would entail no change over the current situation, these options included:

– Option 1: The retention of the existing ECI Directive, accompanied by voluntary measures within the context of the existing EPCIP programme;

– Option 2: The revision of the existing ECI Directive to cover the same sectors as the existing NIS Directive and to focus more on resilience. The new ECI directive would entail changes to the existing cross-border ECI designation process, including new designation criteria, and new requirements on Member States and operators.

– Option 3: The replacement of the existing ECI Directive with a new instrument aimed at enhancing the resilience of critical entities in the sectors considered as essential by the proposed NIS 2 Directive. This option would set out minimum requirements for Member States and critical entities identified under the new framework. A procedure for the identification of critical entities offering services to or in several if not all EU Member States would be provided. The implementation of the legislation would be supported by a dedicated knowledge hub within the Commission.

– Option 4: The replacement of the existing ECI Directive with a new instrument aimed at enhancing the resilience of critical entities in the sectors considered as essential by the proposed NIS 2 Directive, as well as a more substantial role for the Commission in identifying critical entities and the creation of a dedicated EU Agency responsible for critical infrastructure resilience (which would assume the roles and responsibilities assigned to the knowledge hub proposed in previous option).

REFERENCES

- Becker, P., A new budget for the EU: negotiations on the multiannual financial framework 2021-2027, Stiftung Wissenschaft und Demokratie, 2019.
- Council of the European Union, Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008/114/EC, 2008.
- European Commission, Council recommendation on a coordinated approach by the Union to strengthen the resilience of critical infrastructure, 2022/0338(NLE), 2022.
- European Commission, Flexibility and special instruments, 2022.
- European Parliament, Directive of the European Parliament and the Council on the resilience of critical entities, 2020/0365(COD), 16 December 2020.
- European Commission, Evaluation of the Council directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008/114/EC, 2019.
- European Commission, COMMUNICATION FROM THE COMMISSIONA: New, Modern Multiannual Financial Framework for a European Union That Delivers Efficiently on Its Priorities Post-2020, COM/2018/098 final, 14 February 2018.
- Fleming, S., EU braced for more refugees as Russia targets Ukraine power grid, Financial Times, 2022.
- Fritzon, Å., Ljungkvist, K., Boin, A. and Rhinard, M., Protecting Europe's critical infrastructures: problems and prospects, Journal of Contingencies and Crisis Management, 15(1), pp 30-41, 2007.
- Gheorghe, A. V., Masera, M., De Vries, L., Weijnen, M. and Kroger, W., Critical infrastructures: the need for international risk governance. International Journal of Critical Infrastructures, 2007.
- Leicester, J., French police probe multiple cuts of major internet cables, ABC News, 2022.
- Luiijf, E., Nieuwenhuijs, A., Klaver, M., Eeten, M. v., & Cruz, E., Empirical findings on critical infrastructure dependencies in Europe, Paper presented at the International Workshop on Critical Information Infrastructures Security, 2008.
- Milne, R., Denmark, Germany and Poland warn of 'sabotage' after Nord Stream leaks, Financial Times, 2022.
- Olearchyk, R., Shelling disconnects Zaporizhzhia nuclear plant from Ukraine's grid, Financial Times, 2022.
- Renda, A., & Hammerli, B., Protecting critical infrastructure in the EU, Centre for European Policy Studies, 2010.
- Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K., Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE control systems magazine, Vol 21 No 6, pp 11-25, 2011.
- Schmitz, R., An act of sabotage shut down parts of Germany's rail system for hours this weekend, NPR, 2022.
- Seddon, M., Russia orders retreat from Kherson, Financial Times, 2022.

Coordinators: Eva Ribera and Larisa Spahic (TEPSA).

Pieter-Jan Vandoren is a Masters student in Global Security and Strategy at The Brussels School of Governance
and winner of the TEPSA Student Contest 2023: "The future of Europe in the context of Russia's war in Ukraine".