EUROPEAN CRITICAL INFRASTRUCTURE PROTECTION: THE NEED FOR A REGIONAL APPROACH AND A CYBER CONSTANT CONTACT STRATEGY

Laris Gaiser

ABSTRACT: Today, Critical Infrastructures are regionally interconnected. Countries' security and stability rely more on international cooperation every day and this should be even truer within the European Union framework. Recently, the EU has provided a general definition of CI and proposed a European Programme for Critical Infrastructure Protection. It seeks to provide an all-hazard cross-sectoral approach and it is supported by regular exchanges of information between EU States in the framework of the CIP Contact Points meetings. EPCIP is fundamental for our common market security, but by analysing state-of-the-art technology, this paper will try to show that EPCIP lacks fully efficient CI protection and thus will propose an EU model of cooperation based on regional approaches and

a cyber constant contact strategy. A single coordination of several regional CI frameworks could represent an effective solution, implemented on the EU principle of subsidiarity, by avoiding excessive bureaucracy.

Introduction

In an environment where the critical infrastructures are becoming increasingly interdependent, policymakers and citizens are increasingly aware of threats presented by radical political movements and terrorist attacks. Due to their interconnected nature, which is mainly powered by cyber systems, CI's are very vulnerable and can trigger cross-border effects due to their inherently regional or global nature. Within such a scenario, the European Union is still in search of a role to play. The EU is supporting its members through the European Commission that is entrusted with the task of promoting awareness of this important topic, facilitating cooperation between member states, fostering the exchange of know-how, and coaching Member States in their efforts. In 2006, the EU launched the European Programme for Critical Infrastructure Protection (EPCIP) to improve recognizing threats as well as protection from terrorism as one of its main priorities (Commission 2006). Subsidiarity and confidentiality are among the principles that inspired EPCIP as well as, later, the EU Directive on security of network and information systems, known as the NIS Directive (European Parliament 2016). However, analysing cyberspace peculiarities of EPCIP and NIS should encourage Member States, especially in regions characterized by

higher fragmentation, to foster a new local cooperation approach within the general EU coordination scheme. This article would like to highlight that the proposed schemes, given the legal framework, do not effectively cope with the threats that countries are facing in the CI field, they remain too fragmented and do not consider the security problems posed by cyber interconnectedness.

Critical infrastructures and cyber domain in EU policies

The EPCIP framework consists of procedures for the identification and designation of European Critical Infrastructures, with a common approach to the assessment of the needs to improve the protection of such infrastructures and in measures designed to facilitate the implementation of EPCIP together with support for Member States concerning National Critical Infrastructures (NCI). The above actions are based on principles clearly defined in paragraph 2.3 of the Commission Communication about EPCIP:

- Subsidiarity
- Complementarity
- Confidentiality
- Stakeholder Cooperation
- Proportionality
- Sector-by-Sector Approach

In general, subsidiarity, one of the fundamental principles contained in European treaties, governs the exercise of the EU's competences in coordination with the principle of

proportionality. In areas in which the European Union does not have exclusive competence, the principle of subsidiarity seeks to safeguard the ability of Member States to make decisions and authorises intervention by the Union when the objectives of an action cannot be sufficiently achieved by the Member States, but can be better achieved at the Union level, 'by reason of the scale and effects of the proposed action.' The purpose of including a reference to the principle in the EU Treaties is to also ensure that powers are exercised as close to the citizen as possible, in accordance with the proximity principle referred to in Article 10(3) of the TEU (Gaiser 2018).

EPCIP defines its subsidiarity approach as the effort of the Commission in the CIP field to focus on infrastructure that is critical from a European perspective, rather than a national or regional one. Although focusing on European Critical Infrastructures, the Commission may, where requested and taking due account of existing Community competences and available resources, provide support to Member States concerning National Critical Infrastructures.

If we combine such an approach with the definition of confidentiality stating that access to CI information should be granted only on a need-to-know basis, we can argue that the existing CI European security framework does not take into account cyber domain characteristics that invent a new, more flexible and certainly more coordinated regional approach. Cyber threats are fluid and constant while the EU approach is still "sovereign based."

While going in the right, complementary, direction, the Directive on security of network and information systems did not fully solve the highlighted issue.

According to the European Commission, the NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.
- Cooperation among all Member States by setting up a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set up a CSIRT Network to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks.
- A culture of security across sectors which is vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructure. Businesses in these sectors that are identified by Member States as operators of essential services will have to take appropriate security measures and notify serious incidents to the

relevant national authority. Also, key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

Both EPCIP and the NIS Directive support the establishment of country-based authorities that should manage all cyber and CI vulnerabilities at the local level, facilitating cooperation and exchange of information among States setting up a Critical Infrastructure Warning Information Network, a CSIRT Network, and favouring the requiring cross-border synergies. Unfortunately, carefully examining the definitions contained in the mentioned documents, in coordination with the effects they had on legislation by single Member States, it is easy to note that the policies in place to remedy the increased vulnerability of infrastructures are still eminently local.

While respecting NIS, States are shaping a very heterogeneous scheme of national authorities. While Slovenia is opting for an independent institution, Italy and the Czech Republic prefer to entitle their main intelligence agencies as a coordinator of national cybersecurity strategy, still others are choosing an altogether different path to achieve the listed goals. Almost every Member State has its own NIS approach, which within EPCIP the given subsidiarity definition does not really contribute to the shaping of different, compatible, coordinated levels of authorities responsible for broader regional infrastructure networks. Critical Infrastructures

are not only national or European, they mainly connect groups of State, this means that they are regional. EU members are pursuing fragmented policies; consequently, this has led to a significant lack of cooperation between national governments and EU institutions in setting up a coordinated emergency response to potential threats. The higher degree of risk, to which our daily activities are exposed, is not mirrored by an increased response potential by EU institutions. Yet Member States are indeed interdependent critical infrastructures that are mainly cross-border infrastructures and the weakest links affect the vulnerability of all countries.

Cyberspace: a domain characterized by no sovereignty and constant contact

As noted already in the article Resilient critical infrastructure and economic intelligence in the cyber domain, the deterrence paradigm represents a stabilizing, ordering moment in understanding the CI defence issue. CI must be resistant to attacks to such an extent that it simply makes no sense for hackers to spend time and resources on taking it down. To seriously destabilize “highly qualified resources, hackers need access to state-of-the-art technology” and “in most cases, only state-players can afford such a level of coordination” (Gaiser 2017). CIs are highly qualified resources protected by state-of-the-art technologies developed through expensive research and production programmes. This means that in order to compete on this cyber level, there needs to be at least an equivalent economic and technological effort. This is the reason why a deterrence approach can be the

leading strategy in looking for answers within the cyber-warfare domain.

However, deterrence, even expressing its best denial potential right in the CI field, cannot be adopted as a comfortable solution for any kind of threat due to the very specific characteristics of cyberspace, it being the only military domain disconnected from territorial sovereignty boundaries and based, contrary to deterrence theory, on constant contact among international actors. The deterrence concept is tightly connected with the old concept of Westphalian sovereignty pretending the respect of non-intervention and territorial integrity principles. It is based on the threat of use of force with the operational aim of avoiding costly operational contacts convincing the adversary that challenging the status quo outweighs the benefits. A deterrence strategy pretends the absence of action or contact, this is the reason why it can be adopted by a critical infrastructure security strategy, especially considering that any attack in this field has to be based mainly on expensive software and hardware technologies that can cope with the most advanced defence systems adopted by CI operators. A considerable level of intelligence and coordination skills are needed to discover their vulnerabilities and the development of such weaponry requires substantial funding.

Once the threshold of deterrence, and its means of a no-action status, should be crossed, actors would find themselves in war. Cyber weapons exploit software and hardware vulnerabilities to gain access to critical targets. A cyber conflict is highly unpredictable, fast, and dynamic since it annihilates the strategic values of distance, time, and borders. In the

cyber domain, it is practically impossible to send notifications in time, the definition of sovereign territory especially loses a great part of its meaning. The cyberspace operational domain is global and unique given that there is currently no internationally agreed definition of cyberspace sovereignty and given it is a domain in which all other operational domains and national instruments of power are enabled or even dependent.

Nevertheless, every day as it becomes more technology dependent, an infrastructures' security paradigm has to accept that the greatest part of cyber destabilization occurs under the threshold of a formal act of war and that instead of absence of action it is characterized by uninterrupted action because cyberspace is a constantly contested space where State and non-State actors are continuously interconnected and consequently all operations in cyberspace always involve operational contact. The tactical, operational, and strategic bases of deterrence do not align with the characteristics and dynamics of cyberspace (Harknett, Fischerkeller 2017), where offence always has an advantage over defence. The cybernetic systems' offensive non-equilibrium favours action over passivity (Gaiser 2017). This is the reason why deterrence theory, working very well in presence of certain conditions, is only partially applicable when CI stability is at stake. States or other significant non-State actors operate in cyberspace through cyber operations, activities, and actions (OAAs) trying to dominate the domain to always be in the strongest position and OAAs usually maintain their intensity under the level of an act of war. All OAAs can be confined into three categories: sabotage,

espionage, and subversion. All three of the reported categories are closely related to the critical infrastructures' security being used together or separately to affect their efficiency but, as demonstrated by current practice, OAAs cause damages that are of a very different nature of use of force occurring regularly below such a level.

The only way to secure an unsecured space, improving defence and resilience, is by maintaining a constant presence to anticipate the exploitation of a CI system and simultaneously capture the enemy's capabilities.

A new approach to European CI cybersecurity governance: constant presence and subsidiarity

The complexity of the exposed issues above can be better understood by how they are coordinated with the challenge represented by terrorism. Cyberspace is a fluid, technically changing environment, continuously increasing in scale and sophistication that must be constantly supervised and redefined by actors' stable presence. Moreover, it is a swiftly evolving environment where actors are continuously innovating to penetrate or attack systems. In cyberspace adaptations in responses are quickly met with new breaches. This ever changing competition of learning and adapting lies at core of cyberterrorism. The need for agile learning to create capacity to adapt is an essential characteristic of cyberspace (Ariely 2014). Terrorist networks are intuitive learning organizations (Jackson 2004) which act as a complex adaptive system (Ariely 2006). This challenges the abilities of hierarchies to outlearn them and requires

government agencies and organizations to become agile and a complex adaptive system, without losing the advantages of hierarchy. According to Ariely (2006) cyber confrontation is a learning competition. In the future, the intensity of critical infrastructures' cyber destabilization can be foreseen mainly under the level of an armed aggression where OAAs can reach strategic effects. Pursuing a purely deterrence-based strategy, especially in presence of acts of terrorism, could lead to a defence vacuum. Terrorism intimately represents an asymmetric confrontation leaving a reduced space for retaliation. In the absence of a generally accepted definition under international law, terrorism can be defined as the intentional and systematic use of actions designed to provoke terror in the public as a means to certain ends. Terrorism can be the act of an individual or a group of individuals acting in their individual capacity or with the support of a State, though generally terrorist actions are rarely treated as an armed aggression. Such considerations, jointly exanimate with the above-exposed positions concerning the cyber environment, automatically imply that cyber terrorism also must be, and can be, properly anticipated and prevented before a disruptive event happens. Actors defending cyberspace enabled or dependent critical infrastructure should create matrices able to produce consequential effects, prevent exploitations, reduce enemies' capabilities, and accordingly lower potential threats. A constant presence strategy permits the shaping of a persistent mitigation policy.

Moreover, a constant presence strategy is needed because the terrain of cyber engagement is constantly changing. This is a

human created space and every new software version, platform, user interface, and process shifts that terrain. It is perpetually under construction (Harknett, Nye 2017). A European network of heterogeneous national cyber-authorities accounting to hardly comparable national bodies, coordinating private and public stakeholders on different principles, and cooperating among themselves on the EU level mainly on a voluntary basis will not likely mitigate potential attacks.

As mentioned above, while following NIS directive and EPCIP indications almost every EU Member State adopted its own policy for shaping a national experienced-based cyber-ecosystem. Even the very simple issue of defining the Critical Infrastructures Protection (CIP) Contact Points requested by EPCIP to facilitate the exchange of information and emergency management coordination financed and established by governments never reached the needed efficiency given that single local reference offices have been appointed following divergent approaches and sometimes incomparable priorities.

Even the Computer Security Incident Response Teams Network just provides a forum where Member States' National CSIRTs can cooperate, exchange information, and build trust (ENISA 2018). Thanks to the CSIRT Network, Member States' CSIRTs are able to improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents, but it is still a far cry from the tight coordination that contemporary cyberspace implies. Member states are at varying degrees of maturity with respect to the development of a comprehensive

and effective CIP policy. Second, there are islands of cooperation across the EU member states but no overall concept of operations at the EU level (CEPS 2010). A lack of coordination efficiency, together with national based CI defence approaches and no regional centres of cooperation, never shaped a CI security system that could be metaphorically defined as an IC cyber fortress within EU space.

In 2017, even as the European Council correctly detected the problem, it failed to address it in a proper holistic way. In October 2017, the European Council asked for the adoption of a common approach to EU cybersecurity following the reform package recommending a stronger EU cybersecurity agency proposed by the European Commission in September.

According to the European Council (2017), this reform would aim to upgrade the measures put in place by the cybersecurity strategy and its main pillar, the Directive on security of network and information systems - the NIS Directive. Consequently, the Commission recommended the constitution of a cybersecurity agency on the structures of the existing European Union Agency for Network and Information Security (ENISA) in order to help Member States, EU institutions, and businesses deal with cyber-attacks.

The proposal is the result of a correct analysis, but it does not solve the problem of having almost thirty national agencies or authorities dealing with cyber threats and defending national critical infrastructure and no official regional body – between national and EU levels

– coordinating regionally relevant CI security. Although European national intelligence agencies and NIS created authorities exchange their information daily, cooperating with law enforcement activities as well as to prevent threats, the subsidiarity principle as described in EPCIP and indirectly implemented through the NIS directive is unsuitable to ensure stable performances and the security of regional relevant critical infrastructures. An early warning national system concerning certain CI that works could not be "early" enough for other countries dependent on, or responsible for a length of, the same CI. Within a cyber environment, where the notions of territoriality, distance, and time lose their importance and where preventing harm involves complex mechanisms, fragmentation has to be avoided in favour of a broader synergy.

In the field of transnational CI, the old fashion national interest and need-to-know approaches characterizing cross-border and intra-agencies information exchanges should mostly be relinquished. Especially because in an environment marked by uninterrupted action where uninterrupted action is requested also for a CI security keeper, it is almost impossible to know in advance what is "need-to-know" and the safety margins designed preventively may not be sufficient to cope with the expected and, most of all, unexpected stresses arriving upon the systems (Zio 2016). Coordination centres with no real power, institutional fragmentation, bureaucratic obstacles, a heterogeneity of approaches, and insufficiency of real-time cooperation are all factors that preclude concrete cyber-defence policies. Concerning CI of European or regional importance, it cannot be forgotten that the chain is only as strong as

its weakest link and in an environment of interconnected domains, where only the constant contact strategy can erode the will or nullify the possibility of somebody from doing something, our security seeking institutions must react with synergy.

The Oxford English Dictionary defines subsidiarity as the idea that a central authority should have a subsidiary function, performing only those tasks which cannot be performed effectively at a more immediate or local level. Within the European Union, the subsidiarity principle, unfortunately, has always been understood as the duties' division between EU and national States. It has never been interpreted originally as the principle dividing responsibilities among more levels and the entitling of a certain obligation to the most suitable one, no matter if positioned in a sub-State or on an intra-State level (Gaiser, 2018).

The constitution of regional CI security bodies, regional intelligence hubs, could represent the first attempt at creating intra-State EU cooperation projects. The need for a strategy of interconnectedness that creates regional cyber ecosystems in order to support the fluent functioning of cross-border infrastructures is dictated by the contemporary economy framework as well as by its cyber interdependency. Search for security within cyberspace does not allow for institutional fragmentation or action/reaction delays. It is almost impossible to adopt a constant presence strategy otherwise, but instead, there is work without unity, with no sharing of information in real time or only on the presumed need-to-know basis and only after a carefully handled security clearance.

Regional cyber/IC ecosystems should be created to diminish the risk of cyber-attacks to critical infrastructure whose fluent operability and comprehensive security are shared among different countries. If a trunk or cyber system of a certain country fell under a cyber-attack it does not mean that that country is the main target. An enemy will likely always try to destabilize, provoking as much disruption as possible, by passing through the less risky or more weak, careless, channel, at the same time carefully planning the chain reaction propagation of its strike.

A self-reliant, fully operable, technologically updated, and intelligence active EU regional hub's network responsible for the cybersecurity of regionally relevant critical infrastructures could represent an additional step forward, a safer common market, and an improved common security policy. An EU cybersecurity governance shaped on a middle-level network between States and the EU could better prevent aggressions against our sources of power by elevating EU Member States capabilities in preventing or managing a crisis thus eliminating unavoidable frictions posed by the coordination of several national based institutions and intelligence agencies.

Conclusions

The EPCIP came about as a result of the European Council requesting, in 2004, a strategy seeking to protect critical infrastructure through its Communication on Critical Infrastructure Protection in the Fight Against Terrorism. By analysing the state-of-the-art of CI cybersecurity frameworks within the EU and being aware that terrorist organizations are fully

operable within this new domain of power, it can be concluded that the all-hazard cross-sectoral approach is not fully efficient. Coordination by EU programmes and Directives, Member States, and detected National and European Critical Infrastructures are creating their national authorities with pertinent cyber-ecosystems following almost all main indications and suggestions. They are improving collaborations thanks to better information sharing and alerting systems, the development of ways to assess interdependence, and the creation of good practices. However, the security of regionally relevant critical infrastructure is still dangerously fragmented and terrorist attacks, criminal activities, or even State sponsored destabilizations can represent, especially in cyberspace, serious threats to common CI integrity if they exploit the deficiencies presented in intelligence, defence, and management systems of single national institutions that remain primarily responsible for the protection of all facilities.

Accepting the theory that cyber domain is characterized by uninterrupted activity, occurring mainly under the threshold of the formal definition of an act of war and that a strategy of constant presence is needed to control and influence events, it is clear that any delay in understanding events, communication, or coordination can be fatal. For this reason, an improved European approach is needed. It should be based on a more appropriate interpretation of the subsidiarity principle and, consequently, on a constitution of regional CI security hubs where needed. The EU should launch a pilot project, for example, one located in a region like Central Europe marked by

numerous countries connected to a common CI, which would allow for the development of new capabilities to better guarantee stability in the common market and improve Member State security. Stability and resilience shall be achieved by shaping a new cybersecurity governance system based on regional cyber-ecosystems operating autonomously in order to effectively anticipate any potential disruption..

References

1. *Ariely, G. (2006). Learning to Digest During Fighting – Real Time Knowledge Management, International Institute for Counterterrorism. Herzlyia: IDC. Retrieved from: https://www.ict.org.il/Article/959/Learning-to-digest-during-fighting#gsc.tab=0*
2. *Ariely, G. (2014). Adaptive Response to Cyberterrorism. In T.Chen. J,Lee. S.Macdonald (ed.) Cyberterrorism: Understanding, Assessment, and Response. New York: Springer*
3. *CEPS. (2010). Protecting Critical Infrastructures in the EU. Brussels: CEPS.*
4. *Commission of the European Communities. (2006). Communication from the Commission on a European Programme for Critical Infrastructure Protectio. Brussells: Commission of the European Communities.*
5. *ENISA. (2017). CSIRT Cooperation. Retrieved from: https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building*
6. *European Council. (2017). European Council conclusions, 19-20/10/2017. Retrieved from:*

http://www.consilium.europa.eu/en/meetings/european-council/2017/10/19-20/

7. *European Parliament and Council. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Brussels: Official Journal of the European Union.*
8. *Gaiser, L. (2017). Resilient Critical Infrastructures and Economic Intelligence in the Cyber Domain. National Security and the Future, 18(1-2). 21-36*
9. *Gaiser, L. (2018). EU Institutional Fraility: An Opportunity to Rediscover the Principle of Subsidiarity. In S. Kralji ć, J. Klojčnik (ed.). From an Individual to an European Integration: Discussion on the Future of the EU. Liber Amicorum for Silvo Devetak. Maribor: University of Maribor Press.*
10. *Harknett, R. Fischerkeller, M. (2017). Deterrence is Not a Credible Strategy for Cyberspace. Orbis. Vol 61(3). 381-393. DOI: https://doi.org/10.1016/j.orbis.2017.05.003*
11. *Harknett, R. Nye, J. (2017). Correspondence: Is Deterrence Possible in Cyberspace? International Security, 42(2). 196–199. DOI:10.1162/ISEC_c_00290.*
12. *Jackson, B. (2004). Organizational Learning and Terrorist Groups. Santa Monica: Rand.*
13. *Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering and System Safety. 152. 137-150. DOI: https://doi.org/10.1016/j.ress.2016.02.009.*