Securitisation in critical infrastructure identification: from cyber to elections and pandemics

July 2021

Glasgow University Student Number: 2451335R

Dublin City University Student Number: 19108443

Charles University Student Number: 19515135

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 22664

Supervisor: Dr. Vít Střítecký, M.Phil., Ph.D

Date of Submission: 23.07.2021

CHARLES UNIVERSITY

Abstract

Expressive description of the importance of critical infrastructure (CI) has been a common trend in the security literature, especially in the immediate aftermath of 9/11, when for the first time civilian infrastructure was purposefully targeted and the cascading effect so evident at such a scale. The first step in building efficient protection is the correct identification of critical assets: the European Union (EU) set a respective common approach in its 2008 Council Directive. However, it recognises only energy and transport infrastructures as critical and does not correspond with the 2016 Network Infrastructure Security (NIS) Directive.

As compared to how much attention CI protection receives, CI sector identification is, arguably, a knowledge gap. Natural disasters, blackouts, human error, and especially resulting cascading effects are the focus of sectoral regulations, but are severely under-represented on the strategic level. The issue is that while pragmatic risk assessment may work for individual industries, on the state level the identification and designation are ultimately a political decision, which is something the existing frameworks do not account for. A study of securitisation in these domains could reveal the role of various sectoral and political interests, as well as social perceptions in the formulation of CI identification strategies.

The purpose of this research is to determine how the EU Member States utilise securitisation in CI identification. A better understanding of what makes states identify their particular infrastructures as critical could lead to a harmonised CI identification framework which would, in turn, increase resilience of the entire society.

Contents

Introduction

Expressive description of the importance of critical infrastructure (CI) has been a common trend in the security literature, state legislation, and institutional reports for the last two decades: from the enabler of "fundamental democratic rights" to "the backbone of the country's economy, security, and health" and "the lynchpin to functioning … (of) political systems" (FP Insider 2020; Protective Security Act 1996). Such attention is not unwarranted: for instance, in a single attack against SingHealth, the largest healthcare group in Singapore, 1.5 million patient accounts were affected, whereas in Europe the medical IoT market is expected to reach $40 billion in 2022 (Markopoulou & Papakonstantinou 2021). The very nature of CI makes it a good target: it is spaciously spread, sophisticated, and involves a lot of people and money that can be lost in a single blow.

Although the term itself appeared as early as 1990s, the surge of attention happened in the immediate aftermath of 9/11, when for the first time civilian infrastructure was purposefully targeted and the cascading effect so evident at such a scale (Lewis et al. 2012). In the following years, specific focus on CI protection (CIP) kept changing in response to the emerging threats and ideas: from terrorism to cyber risks, interconnectivity, and resilience, which are still high on the decision makers' agenda (European Commission 2005; 2008; EU 2016; United States 2001).

The first step in building efficient protection is the correct identification of critical assets (European Commission 2008; EU 2016). The European Union (EU) set a respective common approach in its 2008 Council Directive "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" (European Commission 2008). According to the regulation, the EU recognises only energy and transport infrastructures as critical, while the 2016 Network Infrastructure

Security (NIS) Directive sets compulsory measures for a much longer list of national sectors.

To add to the regulatory confusion, as compared to how much attention CI protection receives from the governments, media, and inter-state organisations, CI sector identification is, arguably, a knowledge gap. Natural disasters, blackouts, human error, and especially resulting cascading effects are the focus of sectoral regulations, making the expert approaches predominantly risk-based (Bendiek and Schulze 2019; Cederberg 2018; ECEP 2019; European Commission 2020a; Horizon 2020; Knight 2019). However, these topics are severely under-represented on the strategic level. The issue is that while pragmatic risk assessment may work for individual industries, on the state level the identification and designation are ultimately a political decision, which is something the existing frameworks do not account for. Therefore, there is no structured, publicly available way of verifying how much of the risk is empirically substantiated and how much is politically constructed. A study of securitisation in these domains could reveal the role of various sectoral and political interests, as well as social perceptions in the formulation of CI identification strategies.

Making CI 'a matter of national security and defence' seems to be a common trend in the 'Western' security community: NATO, a purely defence-oriented organisation that historically focused 'traditional' matters (e.g. international terrorism, political instability, and the spread of nuclear weapons) (NATO 2021), set quite a precedent in 2010 by including critical energy infrastructure, trade, and water scarcity to the context of its new Strategic Concept (NATO 2010). This indicates a significant change of discourse after the 2000s' interventions on foreign soil and since the defence budget capacity decreased in the 2008 economic crisis, thus requiring a strict set of priorities.

The purpose of this research is to determine how the EU Member States utilise securitisation in CI identification. By engaging with the current political

discourse, relevant regulations, and empirical evidence, it seeks to identify milestones that led to political criticality assignment. France, Sweden, Czech Republic, and Croatia were chosen for the case study to represent different strategic environments. Following the history of the EU CI legislation and the most recent developments, the study tracks the changes using the topics of terrorism, cyber security, and elections, since technological accidents and natural disasters seem to be confined to the sectoral regulations but not the overarching frameworks.

Ultimately, the study aims to use the observations to provide tentative policy recommendations and projections for the EU to strengthen its CIP framework. The challenge of reaching consensus where interest meets reality undermines the effort of finding the long-advertised 'common approach' (European Commission 2020a). A better understanding of what makes states identify their particular infrastructures as critical could lead to a harmonised CI identification framework which would, in turn, increase resilience of the entire society.

The paper proceeds as follows: first, the Literature Review provides a background on both the securitisation theory and the place of CI in the global security structure. Next, for each case and the EU as a whole, the history of CI regulation is related to the national context to explain the most basic tendencies. In the Analysis part, the lists of critical sectors are compared, the regulations are tracked against the statistical trends, and the language patterns from the CI regulations are processed. Results present the analysis of securitisation applied by Member States and the EU to their CIP discourse and the Implications section follows with potential improvements. Finally, Conclusions and Further Discussion touch upon the highlight of "essential services" during the ongoing pandemic and suggest further research directions.

Literature review

Critical infrastructure has been a persistent topic in the security discourse, both academic and practical, for more than two decades. CI refers to those sectors of the human activity (whether political, social, or economic) that the societies need to properly function, which normally includes energy, transportation, communication systems, food and water provision and sanitation (Mendizabal et al. 2021; Quijano et al. 2018; Turner & Johnson 2017; Zabyelina & Kustova 2015). Although the notion of infrastructure is not new, its *criticality* only entered the discourse after the Cold War, when with the erosion of bipolar militarized threats the risks became perceived as too diverse and overwhelming – from natural disasters to terrorist attacks and massive malfunctions of infrastructure. Therefore, the need to optimally allocate limited resources dictated that the states chose which assets they could leave to the sectoral authorities and which required "the protection by the state" (Langenohl 2020). As a founding milestone, the 1996 Executive Order 13010 pledged to the protection of the infrastructures that are "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States" (Presidential Documents 1996).

This development can be traced to what Langenohl (2020) calls "a modernist imaginary of infrastructure which aligns imaginations of full functionality and operability with that of a sovereign guarantee of security". Infrastructures are placed within state strategies to establish and maintain control over a secure, demarcated space and outlaw those who act against the state's objectives (Turner & Johnson 2017). Therefore, the political value of CI is understood through how states seek to integrate the territorial structures by making them dependent on the services and resources only the state can provide. Without such equitable provision (roads, communication), the space becomes "de facto ungovernable" (Langenohl 2020), and the power asymmetry creates preconditions for conflict.

The modern conflict dynamics substantiate this theoretical basis. Gone are the times of the Clauswitzean battlefield; most victims in violent conflicts worldwide are civilians (Security Council Report 2019), and indirect impact from the destruction of infrastructure forms a considerable portion of that number. The 1991 civil war in Somalia and 2016-2018 conflict in Yemen resulted in damaged water systems which, in turn, led to cholera outbreaks affecting, respectively, 55,000 and more than a million with about 2200 dead (Gleick 2019). Even if not a deliberate attack, the Flint Water Crisis in April 2014 resulted in household water supply contaminated with lead, which caused significant health risks and led the authorities to impose the state of emergency (Abernethy et al. 2016).

Even though international humanitarian law prohibits indiscriminate attacks on civilian infrastructure (Gleick 2019), it relates to inter-state wars, while for conflicts just below the qualifying threshold (which have been prevalent) IHL is mostly a guidance. In the meantime, targeting CI means targeting large groups of civilians by definition since the infrastructure is mostly dual-use and does not allow for discrimination of targets. Unfortunately, the existing legal constraints are not strong enough to impose severe, deterring liability for targeting civilian infrastructure, and 'emerging' hybrid threats only expand the regulatory gray area.

Under such conditions, it is no wonder that the states feel a considerable popular pressure to ensure the civilian protection. This may seem to apply only to the structures susceptive to such pressure, i.e. with assertive democratic control; Langenohl (2020) adds that criticality of infrastructure characterises "western nation-states' modes of operation and imagination". However, such North- and even state-centric view is limiting. First, a relevant example is China's One Belt One Road project, which is a massive infrastructural initiative (Chatzky & McBride 2020) arguably aimed at the projection of China's political interests westward. Secondly, violent non-state actors, such as ISIS, Boko Haram, and Colombia's ELN and FARC, have been known to exercise a degree of

governance through the provision of essential services (Mendizabal et al. 2021; Varin & Abubakar 2017).

Therefore, it is better to regard CI through an overarching lens of governance. CI is used by actors to forward interests and secure outcomes through relations ('soft' infrastructures) in a specific space ('hard' infrastructures) thus turning it in a territory and asserting a territorial mandate (Turner & Johnson 2017). The function of such mandate is, thus, dual: immediate service provision and ensuring the necessity of an actor in the first place. Supra-national formations can construct their own infrastructural mandates, as well, among which the European Union (EU) is a vivid example. Integration has been an essential part of the European policy; with the principle of equitable resource distribution not as pressing as in many other regions of the world, closing infrastructure gaps (Langenohl 2020) has been manifested through projects like Trans-European Transport Network and Trans-European Network for Energy (European Commission 2019).

Nevertheless, even taking the criticality of inter-state EU infrastructure at a face value, it still ultimately serves to enable individual interests of Member States. A testament to that is a very uneven regulatory field in CIP and especially the identification and designation of critical sectors. The only existing specialised regulation for CI identification is the European Commission Directive 2008/114/EC which establishes criteria for assets qualified as *European* CI (ECI) (European Commission 2008). The scope of the Directive is limited: the criteria only apply to the energy and transport sectors and normally for assets already deemed critical on a national level (European Commission 2020a; 2020b). A comprehensive assessment of the Directive emphasised the generality of the provisions but still left the national identification unregulated (European Commission 2020a). To compare, an entire agency (ENISA) was dedicated to devise identification guidelines for critical *information* infrastructure, which is rather indicative of the sectoral prioritisation (ANSSI 2020; EU 2016; Ford 2015).

Surely, over the last two decades the focus of CIP has evolved in response to the emerging threats. First, the 1990s' focus on social and community development made a radical turn in the aftermath of 9/11 when the civilian protection was conceptualised and institutionalised through CIP (e.g. the establishment of the Department of Homeland Security in the United States). Since then, CI has been viewed almost exclusively within sectoral security frameworks, the first of which was counter-terrorism (Aradau 2010; European Commission 2005; 2008). Over the years, the focus shifted to the automation of industrial systems and so-called Industry 4.0, which led to cybersecurity that, in turn, raised the challenges of interconnectivity and cross-cutting criticality criteria (Andrea & Bernhard 2010; European Commission 2008; Niesen et al. 2016; Tantawy et al. 2020). Next came the highly unpredictable cascading effects bringing attention to resilience in CIP (EU 2016; Joint Staff Suffolk 2014; Public Safety Canada 2020). With minor modifications, these concepts are still dominating in current regulations and public discourse (Helmbrecht 2017; Mattioli & Levy-Bencheton 2014; Mtibaa et al. 2014).

Predominantly, individual solutions have outpaced the overarching approach: there are EU-level regulations for gas supply, satellite navigation, Eurocontrol, and Galileo protection (European Commission 2020b; Security Research 2020). Following the U.S. example, several states designated election systems as national CI (Cederberg 2018; CISA 2020a; ECEP 2019; ENISA 2019; Fischer 2018; Politico 2018). Recently, climate change and pandemics were added to the list (CISA 2020b; European Commission 2020b; Fekete 2011). These changes were deemed critical enough to commit time and funding to, yet they did not trigger a general policy update; what threshold was used in each case is a knowledge gap.

CI identification, as something evidently risk-informed, should be a pragmatic question. Priority criteria could be calculated based on the consequences of damage (multi-unit loss of life, resources, utility, economic value, demoralisation), the difficulty of protection due to how they are spaciously

spread, interconnectivity, and potential cascading effects as seen vividly with 9/11 (Lewis et al. 2012). The resources and instruments are abundant: sectors develop their own databases like the Energy Infrastructure Attack Database by Giroux et al. (2013) for Colombia, while the data on cyber attacks and vulnerabilities are universally so plentiful that the problem is organisation rather than aggregation or access. The existing tools include Agent-Based Infrastructure Modelling and Simulation analyses interdependencies in Canada, CI Interdependencies Integrator for components restoration in Monte Carlo, Fast Analysis Infrastructure Tool for economic impact assessment for different sectors, Knowledge Display and Aggregation System for cascading effects, CARVER criteria based ranking for single assets, Maritime Security Risk Analysis Model, and Model Based Risk Analysis for a network analysis (Lewis et al. 2012). The academia suggests using network theory (Lewis et al. 2012, Quijano et al. 2018), dynamic risk assessment to cover real-time variation during operation (Adedigba et al. 2018; Parhizkar et al. 2020), borrowing data-driven and model-based risk analysis from transport regulations, E-commerce, offshore drilling, biopharmaceutical and other manufacturing, and early warning in natural and anthropogenic disasters like flood risks and water pollution accidents (Aagedal et al. 2002; Abernethy et al. 2016; Blaauwbroek et al. 2018; Hou et al. 2014; Izuakor & White 2016; Molina 2018; Moteff & Parfomak 2004; Mtibaa et al. 2014; Niesen et al. 2016; Novotny et al. 2015; Rubio-Hervas et al. 2018; dos Santos & Tavares 2015; Tantawy et al. 2020; Westerberg et al. 2013; Xu et al. 2019). Others distinguish a less probability-dependent concept – criticality (Fekete 2011; Mauro et al. 2010; Theoharidou et al. 2009). Even alternative theories rejecting strictly material, inanimate regard of infrastructure rely on objective indicators to some extent (Aradau 2010; Coward 2009).

Nevertheless, what looks like a good choice out of numerous straightforward approaches is not, in fact, such: the mechanisms of asset identification and ranking have still not been standardised, neither in the EU nor in the US or

elsewhere for where the information is available (Lewis et al. 2012). 'Too much' or 'too little' risk could be attributed to a truly increased number or cost of the attacks, massive resources dedicated to the protection and deterrence, or a customary understanding that destruction of such magnitude is unacceptable (Mauro et al. 2010; Tannenwald 2018). What is more, neither human error, nor technical disruptions are as publicly covered as deliberate attacks, even if the consequences could be the same (Adedigba et al. 2018; Parhizkar et al 2020). In practice, for the EU it means that each Member State decides for itself which assets will be designated, both nationally and as ECI, and how they will be protected based on its resources and capabilities making the starting point, therefore, extremely uneven.

Although the choice of critical sectors mentioned above is understandable in terms of development and humanitarian needs, some states identify sectors that are much less self-explanatory in a sense of pragmatic security: values, monuments, elections etc. This leads to two questions: how the function of a designated critical sector is reflected onto the societal processes and how much of the sector criticality is empirically substantiated and how much is politically constructed. As for the first, identification of a sector as critical also means that the perception of its function has changed: if before the value of assets was internal to the sector, now they are seen as providers of "mundane and routine" (Langenohl 2020) processes which are only truly noticed if missing (Turner & Johnson 2017) and for which the contrast between the polar states of function and non-function will come as a shock to society.

In turn, a failure of CI might be perceived as a failure of the enabling actor (e.g. a state) thus undermining the actor's legitimacy, for which CI can be outside of the immediate control and not always responsive to the state's pressure as it is (Blaauwbroek et al. 2018; Turner & Johnson 2017). Consequently, a sector can be "declared under constant and existential threat" (Langenohl 2020) to justify assertive policies towards the owners. This leads

to a classical articulation of the Copenhagen School's theory: by calling material assets 'essential for the very existence of the society' a speech act is performed upgrading those assets to the utmost matter of security under an ultimate threat, which constitutes an act of securitisation (Buzan et al. 1998; Waever 1996). Indeed, in the absence of any framework for the critical sector identification, assigning priority by dramatising a sector as having said priority might account for at least part of the identification and designation practice: if infrastructure is a threatened object to a point when it is called *critical*, it requires extraordinary protection, a sovereign provider of which is the state.

The securitisation theory is best applicable to the current analysis for several reasons. First, securitisation is not supposed to be explained via any 'objective' risk since the political move itself plays a formative role. Second, Buzan, Wæver, and de Wilde (1998) add a certain 'sectoral logic' to the theory with security as an "integrating force" for the referent objects, which allows for the analysis of CI as a whole as well as 'a structure of structures'. Finally, the cross-sector effects of securitisation demonstrated by the Copenhagen School (Langenohl 2020) relate closely to the issue of interconnectedness found frequently in the CIP discourse.

Langenohl (2020) goes as far as to claim that "the construct of critical infrastructure thus denotes a specific perception of vulnerability which is derived from understandings of the ways contemporary, highly differentiated, and deeply technicised societies are organised". If securitisation of CI stems from the nature of the society itself, applied to the EU the research will have to address that it is, ultimately, not a state. Rather, the EU is a supra-national actor to which certain issues of security are outsourced by Member States. The assignment of criticality as a securitising move requires an audience to accept a particular message, and the nature of 'audience' for the EU is different from the ones of individual Member States.

Consequently, several things will be considered in the research. First comes the question of identity: the polity has a prerogative to assign criticality, and the Euro-polity (Waever 1996) is highly fragmented. Where, then, lies the line between national perceptions and 'the European identity' as interests for the sake of which the sectors are identified as critical? Both value and acceptable risk are highly contextual notions, especially when it comes to "threats without enemies" like natural disasters (Langenohl 2020), so the already varying policies need to stay cohesive and apply just as well to the non-deterrable threats. Next, what does the EU see as its sovereignty? How much capacity does the EU have to exert control over the audience as opposed to the need to utilise securitisation and manipulate risk perception? Finally, the notion of the European security would have to be dissected into the security of Member States and the EU as an entity external to them, thus distinguishing the security of the same political space, yet on the national, regional, and international level.

Methodology

The broad research question is finding a political threshold that the EU states and the EU as a whole use to assign criticality to a sector. Member States are chosen according to the EU Macro-Regional Strategies to represent different strategic environments with similar political objectives within the EU (Council of Europe 2014). Therefore, Croatia represents the Adriatic and Ionian region, France – the Alpine, Sweden – the Baltic Sea, and Czech Republic – the Danube regions. Surely, the research cannot be fully extrapolated onto the entire EU; however, geographical and geopolitical representation recognised by the EU itself, as well as the different timing and circumstances of joining the EU allow to speak of a fairly representative sample.

By design, the research is of broadly comparative nature. CI identification allows to facilitate protection through specialised coordinating agencies, prioritise resource allocation, and through politicising and securitising language

might also serve as a deterrent. Therefore, the research leverages a combination of historical and discourse analysis to identify securitisation patterns and place them into the historical, political, and regulatory context.

Preliminary analysis of the regulatory literature has shown that the CIP legislation developed in waves in response to the terrorist and cyber threats, and then the 'emerging' hybrid threats like the election interference. It is understandable that states review, enhance, and accelerate their CIP efforts in the wake of such threats, since CI, by nature, constitutes a valid attack target. First, deliberate attacks against CI serve to undermine the state as a holder of the infrastructural mandate and convey a political message through indiscriminate, maximised civilian damage. Cybersecurity itself has a prominent discursive role, but it was after the Stuxnet attack in 2010 that brought attention to the potential physical damage from something "virtual", even if it was not the first case (Romanova 2020). The number of cyberattacks against SCADA systems has indeed increased in the last decade (Ford 2015), while the language describing cyberspace became more and more intricately linked to the matters of strategic priority ('cyber warfare', 'cyber defence and offence', even 'cyber sovereignty' and 'cyber diplomacy') (Dunn Cavelty 2013). Cyberattacks and disinformation campaigns are the kind of hybrid threats that remain below the threshold of outright (attributable) aggression and so complicate the response. Foreign interference in the elections became a topic somewhat separate from its 'cyber' origin after the 2016 interference in the US presidential election, even though, just like with cyberattacks, the case was hardly new or one-sided (Dorell 2018). The election criticality was then explained as the US priority for "the confidence in the value of people's votes" that relied on the confidence in the enabling infrastructure (CISA 2021a), which is reminiscent of the way an attack against the 'physical' drinking water provision assets could lead to a "loss of public confidence in water supply systems" (Copeland 2008). To summarise, attacks against CI are of concern to the states since not only are they environmentally damaging, but also disrupt

supply chains, state and private revenues, and can damage the image of the governing authority, which makes CIP a top political priority.

The first step is, therefore, to use the Global Terrorism Dataset (GTD) and the Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) dataset and basic descriptive statistics to check for a correlation between the timeline of adopting thematic regulations and the empirical attack trends (START 2019; 2020). The strength of such correlation could at least partially reflect the extent to which pragmatic risk is used as an indicator for CI identification and designation. The rest of the analysis relies on the national and EU-level regulations on CI identification and designation for the analysis of the securitising language. The use of specific speech expressions and patterns is identified and the frequency of their occurrence counted. A study by Langenohl (2020) on the securitisation of financial institutions used where and how frequently the sector is referred to as critical, in which and how many frameworks and handbooks on security mentioned, what agencies are responsible for it, when it has become an object "of risk analysis methodologies with respect to critical infrastructure worldwide", and the "collaboration between political and financial institutions in the fight against perceived threats, or question the foundations on which the state is attributed core financial functions" as evidence of the sector securitisation. The present study utilises a similar approach as applied to CI and contextualises the discourse by using the milestone events for each case.

Only the regulations where CIP is addressed (even if briefly) are utilised so that the study does not diverge into the securitisation of terrorism and cybersecurity. With the same requirements, reports and assessments supported by the (inter-)governmental agencies (e.g. GCSP) are included, while for the elections – to compensate for the comparatively less legislation as a data source – coverage by experts and government representatives during the EU-supported events (like the GLOBSEC Bratislava Forum). For the threat representation, the identified securitising language is only utilised when stated explicitly, even if

the linguistic forms can vary. When the same expression is repeated in the same document, the usage count is added only if it is applied to a different object to expand the study from securitisation analysis in a particular document and cover the regulatory filed as a whole.

Limitations

For the topic of the research, participative research as a method for expert elicitation (e.g. by Kapellmann & Washburn 2019, Niesen et al. 2016, or European Commission 2020a) could be more beneficial. Experts could be asked why they saw a sector as critical and then, if threats were specified, ask if they were familiar with the statistics on these threats. Combined with the discourse analysis, such questionnaire could provide a direct reflection of the securitizing language on the expert and decision-making community, while a focus group discussion could display the group dynamics leading to CI identification. However, under the circumstances, especially since the operators of CI find themselves under exceeding workload due to the pandemic, it was decided against in-person data collection method.

Next, both GTD and SMICI are only available until 2019, while the regulations reach 2021 and the current year has seen some of the major attacks against CI worldwide. This drawback, as well as any potential caveats (underreporting, unobservable data) in data are not decisive since the trends only serve indicatively for the discourse analysis and are not under strong precision requirements. Human error is severely underrepresented in the state regulation, while different mental states of the designating persons and potentially different understanding of the same concepts increases the uncertainty; nevertheless, these topics are beyond the scope of this research and the analysis of securitisation can still be projected onto them to an extent.

Finally, it is difficult to isolate a role of one regulation where several instruments coexist. Therefore, the analysis included broader legislation covering the topic, regardless of its sectoral attribution.

Case background:

The EU

In June 2004, the European Council called for the preparation of a strategy to protect CI against terrorism. The following Commission Communication on Critical Infrastructure Protection in the Fight against Terrorism was the first suggestion regarding how to enhance European efforts in prevention, preparation for, and response to terrorist attacks involving CI. It also included a list of sectors that may be covered under the European Programme for Critical Infrastructure Protection (EPCIP): power plants and networks, information and communication technologies, finance, health, food, water, transport, production, and government (e.g. information networks, property, and even key national monuments and sites).

In 2005, the European Commission organised two seminars to gather the existing national approaches to CIP and adopted the resulting Green Paper on the CIP Programme, which placed itself in the context post-Madrid and London bombings. Although the initial primary focus was on terrorism, the threat assessment was later extended. It aimed to "work on reaching agreement on a common list of definitions and CI sectors" to protect "the European economy as a whole". The indicative list of sectors was somewhat different from the one suggested in 2004 but still comprehensive: energy, ICT, water, food, health, financial, public and legal order and safety, civil administration, transport, chemical and nuclear industry, space and research. The Paper was quite ambitious with questions for future regulatory development: how a common framework could best facilitate compliance for the transborder companies through at least partial control over the national designation, how risk ranging could be harmonised and calibrated, suggested three options for the levels of national designation and two – for the multilateral ECI criteria. Finally, the paper suggested a single agency overseeing CIP in the EU as opposed to establishing national contact points (European Commission 2005).

Evidently, CIP has arisen from the counter-terrorism policies. The European Convention on the Suppression of Terrorism dates back to 1977, TREVI information sharing system existed since 1970s, and the European experience with terrorism included, among others, groups in France, Spain (ETA, GRAPO), Corsica, Italy (Red Brigades), and the United Kingdom (Anglmayer 2021; Bures 2006; Den Boer 2003). Still, only the events of early 2000s led to hands-on protection measures beyond the cross-border judicial procedures. After the 2004 Communication, the EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013 would provide funding for CIP related measures (European Commission 2005; European Commission 2006). Arguably, Madrid bombings in 2004 served as a wake-up call instead of 9/11: the latter was followed with the tried criminalisation path with the 2002 European Arrest Warrant, the normative 2001 "European policy to combat terrorism", and the 2002 Decision the European Council on Combat against Terrorism (Bures 2006; Wilkinson 2005), while only in the 2005 EU Strategy to Combat Terrorism, after the tragedies on the European soil, did the policies align for the critical asset protection (Bossong 2014; Delpech 2002; Haemmerli & Renda 2010; Wilkinson 2005).

The 2006 Communication on a European Programme for Critical Infrastructure Protection established a Critical Infrastructure Warning Information Network and a CIP expert group, promised a directive for ECI identification and designation and "support for Member States concerning National Critical Infrastructures (NCI) which may optionally be used by a particular Member State", already making the national designation regulation non-binding and explicitly prioritising the energy and transportation sectors (European Commission 2006). The April 2007 Council conclusions on the EPCIP pointed out "the ultimate responsibility of Member States to manage arrangements for the protection of critical infrastructures within their national borders" (European Commission 2008). Thus, year-by-year, the minimum version of the 2005 Paper

was adopted: national CIP under the framework was optional, the criteria for ECI were chosen to be bilateral (which still resulted in individual agreements rather than a common approach), and no single agency was established or designated. What is more, the milestone Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection only listed energy and transportation (European Commission 2008).

Instead of the suggested focus on the terrorist threat, the Directive opted for the all-hazards approach, and since then counter-terrorism and CIP went separate ways. The EU reversed to the judicial practices of early 2000s (Den Boer 2003; UNODC 2021). Combatting terrorism remained one of the three priorities in the 2015 Security Strategy and the 2017 Strategic Assessment listed terrorism as one of the existential threats. In the recent years, the focus shifted considerably to de-radicalisation and countering terrorist content online (European Commission 2018b; European Parliament 2021).

As for the 2008 Directive, the planned 2012 review had limited added value. It found that the general CIP awareness had increased, but the application was limited and less than 20 European critical infrastructures were designated (European Commission 2017). This should have been expected since the national dimension remained unregulated and ECI designation was almost voluntary: there was no mechanism to verify which national criteria applied to the baseline lists and if two Member States designated everything that the EU might deem critical. The review found it necessary to change from sectoral expansion to systems and risk-based approach (European Commission 2020a). The 2013 CIP framework reflected the findings, but the progress was arguably marginal. Emphasis on the interdependence did not change the fact that no common methodology was adopted, and the law itself neither rectified the 2008 Directive nor was consistent with it (European Commission 2020a). Nevertheless, some added value was in piloting the 'new approach' to the four major pan-European infrastructures: Eurocontrol (the European aviation

organisation); Galileo (the European global satellite navigation system); the European electricity transmission grid; and the European gas transmission network (European Commission 2017).

A year before the review, the Commission announcement COM(2011)163 Regarding the Critical Information Infrastructure Protection suggested adding the "ICT sector-specific elements to be considered for the review of Directive 2008/114/EC", which was not accounted for (European Commission 2017). Nevertheless, cybersecurity and CIIP in the EU go a long way back. The 2001 Convention on Cybercrime and the 2003 Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems were related to terrorism like most regulations of the time (Anglmayer 2021). The European Union Agency for Cybersecurity (ENISA), still the closest thing the EU has to a CIP (CIIP) agency, was established in 2004, the same year as the CIP Communication was adopted and much earlier than such frequently cited milestones as the attack on Estonia (2007) or Stuxnet (2010). Over the course of its operation ENISA acquired the capacity to identify critical sectors, coordinate CIIP in Member States, and provide technical and legislative guidance (ENISA 2014; 2015). It requires the EU Member States to adopt cyber security strategies (Helmbrecht 2017), runs the European Cybersecurity Challenge (ENISA), organises the Cybersecurity Month awareness campaign, and oversees CERT-EU (Communication 2016).

The 2005 Green Paper suggested a priority for the ICT as well as the first definitions of CII and CIIP, but the 2008 Directive only acknowledged its future potential designation (European Commission 2005; 2008). Attacks against Estonia were reflected in the 2009 CIIP Action Plan, even though it did not specify any sectors and was rather broad in scope (European Commission 2009; European Commission 2011; Markopoulou & Papakonstantinou 2021). The Action Plan was not included in the 2012 review either. As a result, the 2013 Cybersecurity strategy was also rather generic with no clear focus or innovation. The 2016 NIS Directive, however, was a true turning point in the EU CIP

regulation. It aimed to protect the ICT elements of the critical assets in seven sectors: energy, transport, banking (credit institutions), financial market infrastructures, health, water, digital infrastructure (EU 2016). It was service- (rather than asset-) based and provided very clear steps, guidelines, and criteria for the identification of CII and its protection.

In the following years, cybersecurity and CIIP did not only retain their priority position but became a focus of the CIP in the EU. The 2017 Communication on the Fight Against Cybercrime mentioned industrial control systems in CI and might have been a reaction to the 2017 WannaCry ransomware attacks (Paris Call 2018). In 2018, the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres were suggested (European Commission 2018). The 2019 Cybersecurity Act further reinforced the mandate of ENISA (EU 2019). Most recently, the 2020 Cybersecurity Strategy covered CIP, the role of IoT devices, and formed a part of the Commission's Recovery Plan for Europe and of the Security Union Strategy 2020-2025 (European Commission 2021a). Finally, a reviewed NIS2 Directive has already been proposed for later this year (European Commission 2021a).

A specific direction the cybersecurity took in the recent years is the election security. While not formally designated as critical, this sector received huge attention in the form of additional regulations, funding, and EU-wide exercises. The cases of interference with the electoral systems in Estonia, Georgia, and Ukraine were first discussed as a cybersecurity topic, while other examples included disinformation campaigns in France and Germany (Dorell 2017), meddling with the Brexit and the Catalan independence referenda (Dorell 2018; Kirkpatrick 2017). However, it was the infamous interference with the 2016 US presidential election that brought separate attention to the matter (van der Staak & Wolf 2019). Later the same year, the Joint Framework on Countering Hybrid Threats was developed (Maurice 2021) and the Report on "potential and

challenges of e-voting in the European Union" was issued (European Commission 2021b).

More concerns arose for the upcoming 2019 elections to the European Parliament. They were comprised of 28 independent elections with 300 million potential voters in all Member States (Politico 2018). The elections were considered vulnerable from the start, with the composition of the European Parliament at stake and the diverging voting practices, resources, and complicated voting mobility legislation making it a perfect target for cyber and disinformation campaigns (European Commission 2021b). Multiple steps were taken: ENISA released "Recommendations on EU-wide election cybersecurity" (ENISA 2019), the NIS Cooperation Group drafted the Compendium on Cybersecurity of Election Technology as part of the package 'Securing free and fair European elections', and other documents included the Action Plan on Disinformation and the Recommendation on Election Cooperation Networks, Online Transparency, Protection against Cybersecurity Incidents and Fighting Disinformation Campaigns in the Context of Elections to the European Parliament (Dunn Cavelty 2013; van der Staak & Wolf 2019). Prior to the elections, Member States participated in a simulation exercise to train for an attack against the election infrastructure (European Parliament 2019). The European data protection bodies were heavily involved (Privacy International 2019), while Facebook, Google, Twitter, and Mozilla agreed to self-regulate through signing the Code of Practice on Disinformation (European Commission 2018a).

The elections went without any major disruptions, but the work is not over. In 2020, the European Commission presented its Action Plan for European Democracy and the European Centre of Excellence for Hybrid Threat Assessment was established (Maurice 2021). The enhancement of the Code of Practice is underway (Privacy International 2019), and the EU participated in the development of the Transatlantic Commission on Election Integrity and endorsed (so far) President Macron's call to establish an agency to protect the

European democracy (Brattberg 2019). The EU is most likely using a window of opportunity to implement more assertive regulation with stricter, more universal obligations; however, if this will be enough to designate the elections infrastructure as CI remains to be seen.

As of now, 94 ECIs have been designated with a clear Central and Eastern European geographical focus (European Commission 2020d). Both the 2017 Comprehensive Assessment of EU Security Policy and the 2019 Evaluation of the 2008 Directive emphasised the latter's limited impact, omission of the emerging threats (e.g. drones, insider infiltration, hybrid threats), rigid structure, and the generality of provisions (European Commission 2020a; 2020b). It was also found imperative to harmonise the regulation with the NIS (and NIS2) Directive.

The problem is that the EU is not regulating how the different MSs approach the national designation at all: some states use a service-based approach, others go sector-by-sector, the criticality criteria differ, and an attempt to rectify these exact drawbacks in 2005 was met with scepticism. Such reluctance is understandable: not only does the designation mean an obligation to issue Operator Security Plans and Security Liaison Officers, but also gives the European Community the right to intervene (within reason) should a Member State not be capable of the protection itself (European Commission 2008). Therefore, designation of just two sectors that applies only to the critical assets with trans-border value was the said Community playing safe. More so, mere transposition of the regulations that do exist does not equal to their harmonised implementation within the existing frameworks.

Alpine Region: France

The first mention of CI can be found in the list of critical sectors of 1998 called "Security of Activities of Vital Importance" (ANSSI 2020). However, the current regulation is the Prime Minister's Order of 2nd June 2006 "Establishing

on the List of the Sectors of Critical Infrastructure and Designating Coordinating Ministers of these Sectors" (Instruction 2014). As of now, twelve sectors are considered critical: civilian activities, legal activities, military activities, food, communication, technology and broadcasting, energy, space and research, finance, water management, industry, health, transport (SGDN 2017).

In 2014, "Operators of Critical Importance" (Opérateur d'importance vitale, OIV) were designated in the French Code as "whose damage, unavailability or destruction due to malicious action, sabotage or terrorism would directly or indirectly seriously compromise the military or economic capabilities, the security or the survival ability of the nation or seriously threaten the lives of its population" (SGDN 2017). Under these provisions, the operators of information systems within the critical sectors are considered OIVs, as well, and follow the security obligations under the same code. France uses the concept of 'vitality' instead of criticality (CIPedia 2021), but still uses the term 'critical infrastructure' in the transposition of the 2008 Directive.

The General Secretariat for Defence and National Security (SGDSN) is responsible for the national CIP (SGDN 2017). The National Cybersecurity Agency (ANSSI) is responsible for the information security within the SGDSN, where it protects strategically important institutions, conducts exercises, and oversees the national CERT established in 2009. The Information Systems Security Strategic Committee is another regulating authority; however, in terms of CIP, the only sectoral representative is the SGDSN, with all the other members being from the defence and intelligence institutions. France is the only of the cases to have an institution for the CIP regionalisation – the Zonal Commission for Defence and Security (CZDS) (Instruction 2014).

Prior to 9/11, France's counter-terrorism system was already in place (Delpech 2002). Historically, France has faced attacks from the widest spectrum of extremists groups: the far-right Organisation de l'Armée Secrète (OAS) in the

1950-1960s, the radical-left Action Directe in the 1980s, Basque and Corsican ultra-nationalist separatists, and between 1994 and 1996 the Algerian-based Armed Islamic Group (GIA), who carried out a series of bombings against transportation infrastructure (Archick et al. 2006; Counter Extremism Project 2015; Shapiro & Suzan 2003). As a response, a plan VIGIPIRATE was established in 1978, under which in case of a threat the government can deploy additional police forces to protect embassies, train and subway stations, airports, bridges, tunnels, and energy infrastructure, especially nuclear power plants since they provide 50% of France's electricity (Archick et al. 2006).

Following 9/11, the trend of attacks continued, al-Qaeda publicly threatened France, but unjustified "the tranquillity of the population" was observed (Delpech 2002; GTD). An internal security law was passed on the 15th November, 2001, to legalise additional authority for searches, checks, and surveillance (CODEXTER 2016b). France was also one of the only two states in the EU (with the UK) to increase their defence budget (Delpech 2002). Under the VIGIPIRATE plan, more than 4,000 police personnel were deployed to the metro system alone (Archick et al. 2006). In 2002, attacks on a bus with French expatriates in Karachi and a Limburg supertanker in Aden were carried out (Counter Extremism Project 2015). These and an overall increasing trend were followed by the creation of the Council for Internal Security (Le Conseil de sécurité intérieure, or CSI) and a force of 1,000-5,000 military personnel to respond to a large-scale terrorist attack or a "natural or technological catastrophe," such as damage to a nuclear power plant (Archick et al. 2006).

In the 2013, the White Paper on Defence and National Security established a CIP framework for the first time, while the 2014 Instruction General Interministérielle Relative a la Sécurité des Activités d'Importance Vitale 6600 is recognised as the main CIP strategic document. It is centred around the terrorist threat, especially for the CI, and provides a clear algorithm and criteria for designation of assets within the sectors (Instruction 2014). The Instruction recognised that the 2006 EPCIP did not limit itself to terrorism so a more

comprehensive threat assessment is necessary for the compliance (which was never attempted).

However, it was not until the attacks on the French soil that a strong reaction from the government followed. The turning point came with an attack on Charlie Hebdo and a series of coordinated shootings and suicide bombings throughout Paris in November 2015 (130 dead, 493 wounded). Then-President Hollande said it was "an act of war" and declared a national state of emergency (Counter Extremism Project 2015; Maillet-Contoz 2018). When the other states were preparing to adopt the NIS Directive, France was dealing with the worst terrorist cases in its history. Although the Bush administration's reaction to 9/11 was heavily criticised in France, it responded to the attacks with "drastic restrictions of civil liberties" and enforcing the majority of the civil emergency acts (including CIP) (Lucke 2016). For instance, Operation Sentinelle, which is a domestic military deployment of some 7,000 military personnel, was set to protect "sensitive sites and large events" (Maillet-Contoz 2018; U.S. Department of State 2019b).

Cybersecurity in France also has a long history, with the first national CERT-FR established in 2000 and the Central Information Systems Security Directorate in 2001 to provide support to the operators of vital services (UNIDIR 2021b). The origins of CIIP can be traced to the Loi no 2004-575 pour la Confiance dans l'Economie Numerique (2004). However, it was after the cyberattacks on Estonia in 2007 that France considerably heightened its defences (Vitel & Bliddal 2015). The 2008 French White Paper on Defence and National Security served as a starting point for both cybersecurity and CIIP. It first proclaimed cyberspace as a matter of national security and then mandated the protection of national infrastructures against cyberattacks. In 2009, ANSSI and the Zonal Cybersecurity Observatory (OzSSI) were established under its provisions (Brangetto 2015).

In the 2011, the first National Cyber Strategy "Information Systems Defence and Security: France's Strategy" was issued. It reinforced the role of ANSSI and obliged the OIVs to report cybersecurity incidents, comply with the listed technical and organisational measures, and undergo cybersecurity audits by the agency (ENISA 2016). In 2012, the government created a Cyber Citizen Reserve (ANSSI 2021). Next, the 2013 French White Paper for Defence and National Security amended the Code of Defence with provisions of interest to CI (ENISA 2016). In a sense, it was a turning point: the State extended its responsibility for cybersecurity provision from its own systems to the OIVs. In the same year, Article 22 of the 2013 Military Programming Law was devoted to CIIP (UNIDIR 2021b), while ANSSI finally articulated a CIIP framework, which only applied to the systems considered critical within the already critical sectors (ANSSI 2020; Brangetto 2015).

Even cybersecurity in France is intrinsically connected to the threat of terrorism: the January 2015 terrorist attacks in France were accompanied by an unprecedented wave of cyberattacks on private and public domains, including the TV5 Monde television news channel (Vitel & Bliddal 2015). The 2015 National Digital Security Strategy put the fundamental interests, resilience against the terrorist threat, and "defence and security of State information systems and critical infrastructures" on the same level. Objective #1 was to ensure "the security of its critical infrastructures in case of a major cyberattack" (French National Digital Security Strategy 2015). It was also clear that the authors anticipated the adoption of the NIS Directive yet decided not to wait for its provisions: "At the right moment, France will specify the operators who are essential to its economy according to the orientations of the Directive and will participate in the European initiatives intended to reinforce their digital security" (French National Digital Security Strategy 2015). In 2016, seven sector-specific orders were issued for the information systems security plan applicable to the OIVs in the finance, media industry, ICT, health care products, water management, and food supply sectors outside of any framework (Jonesday

2016). This was quite consistent with the pace of cybersecurity legislation adoption that France had set since 2008. The NIS Directive itself was transposed by the Law no 2018-133 in May 2018.

The recent years saw the number of cyberattacks scale up: in 2018 alone there were more than 2,000 threat reports, with targets more and more frequently in CI sectors such as national defense, health, and research. According to the Director General of ANSSI Guillaume Poupard, the agency identifies espionage as a top risk: "organized groups are preparing … by infiltrating the infrastructures of the most critical systems" (ANSSI 2020; Woollacott 2019). This was met with a surge in cybersecurity legislation: France's International Digital Strategy 2017, the 2018 Strategic Review of Cyber Defence (how to manage cyber crises), the 2019 Cyber Norm Initiative, the first doctrine for offensive cyber operations in 2019, and the 2019-2025 Military Programming Law (UNIDIR 2021b).

France is active in the international cooperation on cybersecurity (less so in CIIP): ANSSI has been invited to Poland in 2016 to share its experience of cybersecurity and give its feedback on the French approach to CIP (ANSSI 2016). The Paris Call for Trust and Security in Cyberspace was presented at the Paris Peace Forum in 2018. The state is also a prominent advocate in the United Nations as well as within NATO where it pushed forward the adoption of a Cyber Defence Pledge during the Warsaw Summit in June 2016 – the famous pledge recognising cyber space as the next field of operations (France Diplomacy 2019).

A test for the cyber and information security came with the 2017 elections, to an extent that often experts (Past 2019) and media outlets claim that France has designated the election infrastructure as critical, which formally it has not. Similar to other states, the government vehemently condemned the 2016 US election interference but even more so the 2017 Democratic National Committee hack. The reason was that France itself had an upcoming presidential

election in 2017, which was then considered at “high risk of being hacked” and “campaign staff have zero training in how to stop it” (Hirst 2017; Vinocur 2017). The concerns did not go in vain: the breach of emails of the Macron campaign in 2017 became a major scandal (Cerulus 2020).

Many in the establishment claimed that “unlike the US and the UK, France managed to maintain its democratic integrity” and reacted “in the most effective way” (Bulckaert 2018). However, the attack happened at the mandated pre-election time of media silence, so the spread of disinformation was limited (Cerulus 2020; CSS 2017). Next, the electronic voting system was abandoned altogether as a measure of protection, which is a questionable success in the service provision (CSS 2017; Grunemwald 2018). Guillaume Poupard and the Ambassador for Digital Affairs Henri Verdier put the election interference on the same level as the irresponsible AI development, fake news, and hacks into *critical infrastructure* (Poon & Basu 2019). Yet, only information in the e-voting systems and statistical websites is considered critical, not the election infrastructure itself (Radware 2017).

A reaction followed as a call for further social media regulation. In July 2017, the programme “Defending Digital Democracy” was established to involve social media companies in securing the “democratic mechanisms” (Grunemwald 2018). France was one of the five states to establish the Global Internet Forum to Counter Terrorism and hosted the Christchurch Call to Action Summit in Paris (U.S. Department of State 2019).

Looking forward, counter-terrorism policy remains the government’s top priority in 2019, as stated in the new French National Intelligence Strategy (2019-2024) (U.S. Department of State 2019b). The ongoing pandemic left an imprint: on the one hand, moving restrictions meant less in-person radicalization activity, no large gatherings – fewer viable targets, and international travel restrictions – fewer foreign fighters. On the other hand, the combination of psychologically vulnerable, alienated people (especially teenagers) stuck at

home and increased online activity allowed to heighten radicalization through digital means (Dettmer 2021). Such a situation allows to expect a new wave of recruits.

France dedicated 500 million euros to enhancing cybersecurity of companies and public authorities and announced a new cybersecurity centre to be opened in Paris in late 2021 (Cyberwiser 2021a). After the 2021 regional elections went without any massive disruptions but with a very low turnout, so the 2022 presidential election is to be monitored.

To summarise, due to a consistently high risk of terrorism, CIP, cybersecurity, civilian emergency management, and other security related affairs revolve around the counter-terrorism framework. Such focus partially explains considerable involvement of the military forces, legislation, and assertive contingency plans with more restrictive measures than in the majority of the EU Member States. On the other hand, France has a tendency to "legislate" against terrorism (Maillet-Contoz 2018) rather than issue guidelines for practical CIP measures. In 2005, the then-new French Anti-Terror Bill focused on surveillance, and so did the new counterterrorism bill for surveillance of extremist websites in 2021 presented after the stabbing of a police employee in Rambouillet (D'Souza 2021; Steiner 2005). Such approach allows to justify harsher measures (which is important for the following securitisation analysis), but also creates a somewhat rigid centralised system without an efficient mechanism to adopt the best practices bottom-up.

The Baltic Region: Sweden

The first mention of CI can be found in the Protective Security Act (1996:627) that "contains provisions on the protection against espionage, sabotage, terrorism and other crimes that may threaten security of the realm, and protection in other cases of information covered by confidentiality which concerns security of the realm" and places CI identification as a prerequisite for

various risk and vulnerability analyses and prioritisation mechanisms (e.g. Styrel – the Ordinance for the prioritisation planning of vital societal electricity users) (CODEXTER 2014). As of now, eleven sectors are considered critical: energy, ICT, financial services, social insurances, public health services, food, trade and industry, protection, security, and safety, municipal services, and public administration (CIPedia 2021).

The Swedish Civil Contingencies Agency (MSB) is the central authority responsible for the CIP. In 2011, the agency started a national risk assessment, which identified 27 particularly serious (national) events and eleven scenarios. The MSB has the right to issue regulations for government authorities in information security, but not for private companies within specific sectors. Also, the MSB does not have the authority to investigate cases of non-compliance nor issue binding instructions to public administrations or market operators (unlike e.g. the Telecom Authority) (ENISA 2016). Overall, assignment of any sector under the authority of MSB in practice means treating it as critical while the agency will coordinate the operations and funding, share information, and organise exercises within the National Forum for the Direction and Coordination of Exercises (MSB 2014). It cooperates with the Security Serivce (Sakerhetspolisen 2021) and is part of the Counter-Terrorism Cooperation Council.

The Protective Security Act of 1996 set a beginning of the national CIP (an updated SOU 2015:25). The main topic was civilian resilience against terrorism, with CII briefly mentioned after the transportation of nuclear waste and hazardous substances. In the immediate aftermath of 9/11, a Swedish Royal Commission was set up to investigate the impact of the incident on Sweden (Norell 2005). The national police established a counter-terrorism service responsible for the civilian protection and the 2002 European Union's Framework Decision on Combating Terrorism was transposed into the Act on Criminal Responsibility for Terrorist Offences (Polisen 2021). The number of terrorist attacks in Sweden remained low; the most notorious case at the time

was a plot to assassinate Lars Vilks for controversial Islam-themed caricatures (Counter Extremism Project 2020). The Installations Protection Act (2010:305) (which was implicitly about the protection of critical assets) and the Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crime were adopted in 2010 (CODEXTER 2014). The 2011 MSB's Report on a Unified National Strategy for the Protection of Vital Societal Functions provided a clear, detailed guide with step-by-step objectives, implementation dates, and responsible actors for CI identification, recommended ISO 31000 Risk Management Standard and ISO 22301 Business Continuity Management Standard (CODEXTER 2014).

Although Sweden considered itself a state without much terrorism, between 2014 and 2018 there was an observable surge in the attacks number and scope. First, according to the testimonies of several perpetrators, the attackers sought to punish Sweden for intervening as part of the anti-ISIS coalition. Although Sweden first sent troops to Afghanistan in 2002 as part of the multinational counter-terrorism force, when it sent the military to Iraq in 2015, a surge in online activity led to the increased recruitment of foreign fighters from Sweden and from 200 known Islamic extremists in 2007 the number reportedly surged to "thousands" in 2017 (Counter Extremism Project 2020). Statistically, at least a half of the recruited fighters return to Sweden (Counter Extremism Project 2020). The first time a Swedish court convicted foreign fighter for the crime of terrorism was in late 2015. Next, far-right domestic groups like the Nordic Resistance Movement (NRM) grew by at least one-third between 2015 and 2016 and were responsible for violent clashes in Stockholm, Borlange, and Falun, and several series of bomb attacks against refugee centres in 2017 (Counter Extremism Project 2020). Nevertheless, the most shocking attack happened on the 7th of April, 2017, when a perpetrator ran a truck into a crowd of people in Stockholm which resulted in 5 fatalities and 15 injured (Counter Extremism Project 2020).

The 2014 Counter-terrorism strategy highlights risk and vulnerability analysis for the most important operations and societal functions adding that "the terrorist threat must be more clearly incorporated in this work than is currently the case" (Government Communication 2014). Since the biggest concern remains about the returning extremists, the tightening of counter-terrorism legislation in 2016-2017 concerned criminalisation of "travel for the purposes of undergoing military training or committing acts of terrorism abroad," strengthened financial monitoring, and expanded surveillance capacity, but nothing closely related to CIP. Even in February 2017 during a specialised UN Security Council Open Debate "Protection of Critical Infrastructure Against Terrorist Attacks", Sweden presented a speech about accountability for terrorism and financing terrorism, which was closer to the counter-terrorism legislation than CIP itself (Counter Extremism Project 2020).

As for the cybersecurity, in the Protective Security Act information security was identified as one of the three fundamental protective security areas (CODEXTER 2014). However, as of 2008, Sweden did not have a definition of CII, even though the ICT had long been designated a critical sector. The first National Cybersecurity Strategy was published in 2010 (Cyberwiser 2021b). In the 2011 review of the Protective Security Act information security was included into the security context. The question of public image and accurate information dissemination can be traced back to the terrorist threat: "A terrorist attack does not only cause direct damage but can also lead to great anxiety in society … reach out to the general public and the media with well-considered, correct and consistent information" (Government Communication 2014).

The Swedish Security Service analyses and investigates the serious electronic attacks against CI. The National Defence Radio Establishment (FRA) and the Military Intelligence and Security Service (MUST) also participate in the provision of information security of the state. In particular, the FRA has developed a technical detection and warning system for essential services and critical infrastructure. The main authority, as for any other critical sector, is the

MSB. In 2011 it tested a pilot version of the Swedish IT support system for information warnings (MSB 2011), which was part of the EPCIP's Infrastructure Warning Information Network (CIWIN).

Since 2016 (potentially, since the adoption of the NIS Directive), the CIIP started to evolve faster. The new National Cyber Security Strategy of 2016 finally referred to digital systems as "[a] critical infrastructure" and discussed cybersecurity of critical sectors (National Cyber Security Strategy 2016). The Strategy also assigned MSB a coordinating role in cybersecurity, which was a reasonable step within the "one agency" approach in CIP. Finally, an implementation guide on cyber security for essential and digital services (SOU 2017:36) was devised in 2017 and came into force in August 2018 transposing the NIS Directive. Just like the Directive, the transposing act applied to 8 (out of 11 in Sweden) sectors: energy, transportation, banking operations, financial infrastructure, health sector, drinking water, and digital infrastructure, leaving out the national designation of social insurances, food, protection, security, and safety, municipal services, and public administration (Export.gov 2019). The reviewed Protective Security Act of 2018 imposed stricter rules for the operator of critical IT infrastructures (O'Dwyer 2019).

Sweden has participated in several international exercises like Cyber Europe 2010, the US Cyberstorm III, and the Telo 19 attack simulation exercise (Telecompaper 2019b). At the national level, the MSB has arranged NISÖ – an information security exercise for the public-private cooperation in case of an attack. Among other projects is Cybernode – a platform established in late 2020 for joint agendas and investments in cybersecurity (Cyberwiser 2021b).

Back in 2011, in the report on the newly adopted CI strategy, among the critical areas MSB listed "the functioning of society, democracy, legal security and civil liberties and human rights" (MSB 2011). Then, the 2016 Cybersecurity Strategy stated that "attacks can also be directed against our fundamental values and the democratic functions of society, e.g. through disinformation and influence

campaigns" and that there were "information risks undermining confidence in our public institutions and challenges the security of society" (National Cyber Security Strategy 2016). The International Institute for Democracy and Electoral Assistance (IDEA 2019) was set up in Stockholm the same year.

After the Russian interference in the 2016 US presidential election, Sweden found itself preparing to their own election in September 2018. The principle of protection was articulated in the whole-of-society election defence approach when the election infrastructure was designated critical (Cederberg 2018). Without any legislative CIP update the MSB was appointed as a leading agency for election coordination. Sweden itself claimed that it was done to mobilise the government, the media, and the wider society, as well as to coordinate a counterinfluence project (Cederberg 2018). To put the threat into context, the Swedish election administration is highly decentralised and paper-based, but "more technology is seen as unavoidable in future elections" (van der Staak & Wolf 2019).

Looking forward, in July 2018 the government commissioned an action plan for 2019-2022 (Goud 2021), while the Comprehensive cyber security action plan 2019–2022 was issued in March 2019. It includes the steps such as organising an annual information security conference, promoting the use of protected satellite services for CI (including the importance of the Galileo system for water treatment, food, electricity, communications, security services, and transportation, as well as the future "wireless applications in smart cities such as self-driving vehicles") (Goud 2021). Although the plan was issued after the designation of election systems as critical, they were not mentioned there even once.

Other plans include the development of national and military cyber ranges, the Total Defence Exercise 2020 (TFÖ 2020) in cooperation with the MSB, and the National Information Security Exercise 2021 (NISÖ). In 2019, the Swedish government announced that a new national cybersecurity centre would be

established in 2020 (Telecompaper 2019a). It was not yet achieved as of the beginning of 2020, but the government announced a further investment of SEK 440 million (circa €43 million) by 2025 (Goud 2021; Telecompaper 2020).

To summarise, Sweden started quite early with the concept of critical assets and managed to create a comprehensive protection system with a single agency at the helm (the MSB). The overall focus seems to be on soft-power approaches such as cooperation, education, prevention of radicalisation, open societies, and liberties, but added with several very clear and detailed risk assessment and business continuity guides. The ad hoc transposition of the EU legislation, however, seems to confuse the national level since instead of incorporating it into the existing system, Sweden adds it on top without much harmonisation.

Danube region: Czech Republic

In Czech Republic, the beginning of CIP can be traced to the Act 240/2000, or so called 2000 Crisis Act: although it initially covered general civilian emergency preparedness, its 2010 amendment explicitly required the protection of selected critical assets, the provision of a CI Subject Crisis Preparedness Plan, and a Security Liaison employee (Crisis Management Act 2000). Since the initial 2000 provisions were similar to those later established by the 2008 EC Directive, the Czech Republic used the Crisis Act and the Government Regulation No 432/2010 on the Criteria for Determination of Elements of Critical Infrastructure to transpose the 2008 Directive and implement ECI protection in its legislative framework (Lukas & Hromada 2011; Rehak et al. 2016).

As of now, nine sectors are considered critical: energy, water systems, food industry and agriculture, health services, transport, communication and information systems, financial market and currency, emergency services, and public administration (CIPedia 2021; Novotny et al. 2015). The Crisis Act also constitutes the beginning of the cybersecurity legislation, with CII given an explicit definition in its amended version.

The regulating authority is the General Directorate of the Fire Rescue Service of the Czech Republic with its Population protection and Crisis management division. In the 2000 Crisis Act, civilian protection covered "crisis situations, which are not related to provision of defence of the Czech Republic against an external attack … and during their solution and protection of critical infrastructure" (Crisis Management Act 2000). Since then, CIP is intrinsically embedded into the civilian crisis management, which in itself is understood as either preparation for crisis – which is self-explanatory – or CIP (HZSCR 2021; Rehak et al. 2016). This observation is important for the following analysis: unlike in the other three cases, anything the Czech government calls 'crisis management' automatically includes CIP.

Additionally, the Foreign Security Policy Coordination Committee (FSPCC) includes Deputy Ministers of Finance, Health, Agriculture, and Industry and Trade among others, while the Defence Planning Committee (DPC) includes Deputy Ministers of Agriculture, Finance, Industry and Trade, Transportation, Labour and Social Affairs, Health, and the Chair of the Czech Telecommunications Authority (CODEXTER 2012). Although CIP mainly refers to (domestic) civilian crisis management, most critical sectors are represented in the bodies responsible for the foreign and defence policy of the state, while the General Directorate of the Fire-Fighter Rescue Service remains the prime contact and the representative of the Czech Republic's CIP in NATO and the EU (CODEXTER 2007).

Historically, the former Czechoslovakia possessed a system to prepare the civilian economy for a potential war (Vaskova 2015). Prior to 9/11, there were no terrorist attacks or other major purposefully disruptive incidents; however, in 1997 and 1998 the Czech Republic suffered from several destructive floods (Vaskova 2015). These two considerations might explain the focus of CIP: in the post-Cold War world, there was no need in extensive military preparation of the civilian population, so the emergency laws of 2000, and the Crisis Act in particular, created an Integrated Rescue System which was based on different

principles and a different structure. The worst disasters of the time being of natural kind, the Czech legislation emphasised resilience and civilian emergency which included CI, unlike in many EU states where this was first considered after 9/11.

All the above considered, the turning point for CIP was still 9/11 (Vaskova 2015). In case of the Czech Republic, it meant the articulation of threats to CI, which were not specified in the Crisis Act. The National Action Plan to Combat Terrorism was presented in April 2002 (CODEXTER 2012). Next came the Security Strategy of 2003, but only later the same year did the Committee for Civil and Emergency Planning present a "Project Analysis of the principal functions of the state, including the protection of critical infrastructure in the event of emergencies" which, for the first time since 9/11, explicitly connected the 'new' threats and the protection of critical assets (Vaskova 2015).

Most of the following legislation had CIP in their provisions. The National Action Plan to Combat Terrorism 2005-2007 had a separate section devoted to CIP and a heavy focus on transportation (Ensuring Security of Civil Aviation, Crisis Management in Transport), although no ICT among the "new technologies related to some aspects of the fight against terrorism" (CODEXTER 2007). In the National Action Plan to Combat Terrorism 2007-2009 there was already a short paragraph on cybernetic threats and a call for a comprehensive strategy; however, critical information systems and the public administration information systems were extensively covered in the CIP section instead (National Counter-Terrorism Plan 2007).

The next wave of updates came after the new NATO Strategic Concept in 2010. The amended Crisis Act came into effect in 2011, but still did not specify any strategic threats (Crisis Management Act 2000). To the contrary, the 2011 Security Strategy stated the political and economic pressure and aggression (short of an actual physical attack) as a primary threat long before the notorious cases of massive disinformation campaigns and election interference. At the

same time, it connected all the security topics: “terrorist groups … are capable of directly threatening … critical infrastructure” and “growing dependence on information and communications technologies increases the vulnerability of the state and its citizens to cyberattacks … (that) may have criminal or terrorist motivations” (Security Strategy 2011).

The focus narrowed down to the energy infrastructure and “supplies of strategic raw materials” with the threats ranging from criminal activity to politically motivated manipulation of financial and resource flows (Security Strategy 2011). In the section on cooperation, “the Czech Republic monitors foreign investment in branches of critical infrastructure and in strategic companies in order to avert the threat that such investment will be misused to promote the economic and politic interests of a foreign power at the expense of the Czech Republic” (Security Strategy 2011). Evidently, in those years the Czech Republic found itself under the threat of resource dependence turned into a political leverage, which was perceived as a higher risk than any other.

This focus in indirectly sustained in the 2013 Counter-Terrorism Strategy. Although there was a notorious case of the Prague terror plot in 2006, in 2008 the Czech Ambassador to Pakistan was killed in Islamabad, and the Strategy references “a milestone in the shift towards a possible terrorist attack being carried out in the new EU countries”, namely the 2012 incident in Burgas, Bulgaria, the strategy claims that the Czech Republic does not suffer from the terrorist threat and takes and active stance in solidarity with other states (Strategy 2013). That said, the same strategy makes the Czech Republic the only state under study to include the EU Stockholm programme on the protection of citizens against terrorism into its 2013 strategy (Strategy 2013). It, yet again, focuses on transportation and no longer covers cyber threats not to duplicate the same-period Cyber Security Strategy 2011–2015.

The most recent events have put an end to such optimistic stance. An act of what was called “state terrorism” was reported by Prime Minister Andrej Babis and

Minister of Foreign Affairs Jan Hamacek about the 2014 case 58 tons of ammunition explosions in Vrbetice, which resulted in 2 fatalities, hundreds endangered in the immediate vicinity, and the material damage in "tens of millions of euros" (Kleckova 2021). According to the announcement, the evidence indicated orchestration by GRU (the Russian military intelligence service) agents to disrupt a shipment either to Ukraine or Syria (Kleckova 2021). This act constituted a breach of the sovereign NATO and EU member's territory, something the Czech Republic stated in the previous strategies as 'highly unlikely'. What followed was an exchange in expelling diplomats in May 2021 which was added by Slovakia, Romania, and the Baltic states. This came a year after the Konev and the Ricin affairs – a series of cyberattacks and an assertive disinformation operation aiming to make the Czech public believe there was a Russian intelligence officer bringing Ricin to the state (Kleckova 2021). Although it was just a hoax, the goal was still aggressive intimidation of the Czech public. Any further reaction to the matter is yet to be observed.

Going back to CIIP, the regulating agency is the National Security Authority (NSA); its division, the National Cyber Security Centre, handles CII within the governmental CSIRT (GovCERT) (ENISA 2016). Unlike most Member States, the Czech Republic provides publicly available thresholds for CII designation: "if it causes death to more than 250 people, or the economy of the state is damaged of more than 0,5% GDP, or it has serious impact on providing necessary services to more than 125,000 people … [or] containing personal information about 300,000" (ENISA 2014). However, under the CII definition, these only apply to the already established sectors.

A milestone is considered a cyber offensive campaign in March 2013 directed against the media, banks, and mobile operators (Kadlecova et al. 2017). The 2014 Cyber Security Act and the 2015 Cyber Security Strategy were at least in part shaped by these attacks. The identified problems included absent contact points in big companies and limited information sharing – the issues highlighted later in the 2016 NIS Directive; therefore, the attacks put the Czech Republic

ahead of the EU in this regard. The 2014 Cybersecurity Act focused on vital systems and their priority protection, the Regulation on Cyber Security Incidents and Reactive Measures gave protection guidelines, and the Regulation on the Determination of Important Information Systems and Their Determination Criteria (IIS Regulation) overcomes the gap between the importance of CII and other types of systems (Kadlecova et al. 2017). Afterwards, the Cybersecurity Act was amended to comply with the NIS Directive, and "the Act newly presents Operator of Essential Service (OES) and Digital Service Provider (DSP)" (Kadlecova et al. 2017). These amendments led to a certain degree of confusion: OES, according to the definition, is very close to CI, their systems comply with similar provisions as CII, and yet they are only treated within cybersecurity frameworks and are not connected to the crisis management legislation, just like IIS is not formally CII either. The whole process resembled patching more than revising.

In addition to the general provisions, the Cybersecurity Act defined a state of cyber emergency similarly to any other civil emergency as "a state, during which information security in information systems or security and integrity of services or electronic communication networks is seriously endangered and the interests of the Czech Republic may thus be violated or endangered". The imposition of this state performs an awareness function, but mostly allows the government to intervene into ISP's operations (Cyber Security Act 2014). In 2017, the National Cyber Security Centre was replaced by the National Cyber and Information Security Agency (NUKIB) which became a primary cybersecurity authority, also responsible for Galileo (UNIDIR 2021a).

The question of cybersecurity was risen again in 2019 when after the 2019 EU parliamentary elections the Czech Republic still had an upcoming election within a month. The previous experience was not optimistic: in 2017, websites of the Czech Statistical Office volby.cz and volbyhned.cz were under a DDoS attack "in an effort to disrupt the reporting of the results" of the parliamentary election (Auchard 2017). The attack did not affect the election process but was

not the first attack against the "political infrastructure" in 2017 (Tannam 2017). The same year, emails of senior Czech diplomats were hacked which was considered very similar to the attack against the DNC in the US (Tait 2017). The Czech Ministry of foreign Affairs was hacked in 2019. No wonder that the upcoming elections were called "critical" (van der Staak 2017).

The problem was seen as cyber as much as disinformation related (Corredoira et al. 2021). Political risks have been high on the state security agenda for a decade: the 2011 and the 2015 Security Strategies both had a paragraph on threats in the form of "hard-line attitudes … against the fundamental values of our society", "casting doubt on the concept of the democratic rule of law and denying fundamental human rights and freedoms", and "the power-seeking aspirations of some states that increasingly refuse to respect the international order and basic principles of international law" (Security Strategy 2011; 2015). And yet, prior to the elections, unlike e.g. Sweden, the Czech Republic did not distinguish the elections infrastructure into any separate category, let alone designate it critical. On the other hand, the Centre Against Terrorism and Hybrid Threats for counterpropaganda and counterterrorism was established within the Ministry of the Interior of the Czech Republic to provide research and information sharing on disinformation, fake news, foreign propaganda, migration, extremism, disinformation campaigns (MVCR 2021).

To summarise, in the Czech Republic CIP has never been merely an element of the security sphere. Rather, being a part of the all-encompassing civilian crisis management allowed it to become a backbone of the national security. However, while pioneering in theory, it has been slow to react in a binding manner to the emerging threats.

Adriatic/Ionian region: Croatia

Croatia constitutes an interesting case since it was the last state (to date) to join the EU and, more importantly, it joined in 2013 – long after the milestone frameworks were adopted. Before joining the EU, Croatia did not have any

explicit regulations on CIP; instead, the 1999 Ordinance on Criteria for the Designation and Protection of Objects of Special Importance for the Defense of the Country in accordance with the Defense Act identified "military and other objects of particular importance to the defense of the country" (Mihaljevic 2018).

Therefore, the primary milestone for Croatia is the year 2013. As of now, eleven sectors are considered critical (in the ranging sequence, unlike in the rest of the cases): energy, information and telecommunication technology, transportation, health, water management, food, finance, production, storage, and transportation of dangerous goods, public sector, national monuments and values, and science and education (Vlada Republike Hrvatske 2013; Zakon 2013). To devise its CIP framework, Croatia had both its own sectoral experience and the one of the EU states. In practice, first of all CI designation entails monitoring by "the responsible state authorities" (although it is unspecified which ones) and the fines ranging between HRK 500,000 and HRK 1,000,000 (€67,000 to €130,000) for violating the regulatory provisions (Zakon 2013).

Historically, Croatia has been a post-conflict country located in an unstable region, which explains its initial military focus in CIP. After the Homeland War, the only considerable event of physical destruction was a car-bomb attack in front of the police station in Rijeka in 2005, which was a classical act of terrorism (Peresin 2013). Even if the term itself was formally adopted twelve years later, Croatia still recognises 9/11 as the point when CI became an essential part of national security for "each country" (Mihaljevic 2018). The 2002 National Security Strategy served as a general strategic framework for combating security risks and listed terrorism as one of the threats (CODEXTER 2016a). However, neither incident was enough to change the Croatian approach to the perception terrorism: the state did not, in its assessments, consider terrorism as a considerable threat to national security and did not formulate a policy to counter it. Instead, the Criminal code continued to be the only

document to clearly define terrorism. During the Croatian presidency at the Counter-Terrorism Committee of the UN Security Council in 2008 – 2009, it introduced the National Strategy for the Prevention and Suppression of Terrorism and an action plan to implement it, which, however, never happened. If anything, far-right and far-left groups "are likely to pose a greater risk of death and injury, despite being poorly organised" (Crisis24 2021).

The very first National Strategy for the Prevention and Countering of Terrorism in 2008 included a threat of "attacking critical national infrastructure" to maximise the scale of an attack, with the listed examples of transport, energy, communications, industrial, financial and administrative. The 2010 Protection and Rescue Plan mentioned CI, too, without giving it a definition as part of the resilience against natural disasters, same as the 2010 Private Protection Act (Mitrevska et al. 2019). The need to work on a single strategy was emphasised in the National Strategy and Action plan for the Non-Proliferation of Weapons of Mass Destruction (2013), Risk Assessment of the Croatian Natural and Technical and Technological Disasters and Major Accidents (2009), a study on connectivity criteria for the energy sector as "critical infrastructure" (Simic et al. 2009), and a few other documents; the government was aware of the issue, but the approach was relatively decentralized and not very urgent.

Right before joining the EU in 2013, Croatia was undergoing the baseline research which presented peculiar observations, especially on the specific routine issues. For instance, the unwillingness to share information regarding the threats to CI attributed to "some intolerance and stereotypes in a particular group of senior police officers and private security employees" is often implied, but rarely articulated this way in state-level documentation (Mihaljevic 2018). The Critical Infrastructure Act was issued in 2013 defining the process for identifying critical assets within the sectors established in the Decision on Designation, where they are ranked by criticality criteria (Vlada Republike Hrvatske 2013; Zakon 2013). Unlike the first CI legislation in the other cases, the Act did not explicitly focus on terrorism, since it was not the reason of

adoption. Instead, it focused on the creation of the Critical Infrastructure Security and Resilience System (CISR) (Mikac & Cesarec 2016). Within it, the National Protection and Rescue Directorate was established as the national, EU, and international point of contact (Mihaljevic 2018; Mikac & Cesarec 2016). Lower-level regulations were adopted in the Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure (Mikac & Cesarec 2016).

Even though the Act was adopted to comply perfectly with the EU regulations, relative inertia in establishing a functional CIP network, the lack of research, and "no publicly available insights into the current problem of systematic CIP" kept the actual progress limited (Mihaljevic 2018). As of 2016, CI was still not identified and Croatia was yet to implement even the dual CI/ECI approach (RECIPE 2015).

In 2015, the same year as a Croatian citizen Tomislav Salopek was abducted and killed by ISIS (U.S. Department of State 2019a), the National Strategy for Prevention and Countering Terrorism was adopted. This time, CI was strongly represented, largely as the result of the intensive advocacy by the National Protection and Rescue Directorate. The Strategy recognised terrorism and potential attacks on national CI as serious threats to "national security, the health and lives of people, property and the environment, security and economic stability and continuous functioning of government" and included cybersecurity into the list of measures required to protect CI (Mitrevska et al. 2019).

In fact, cybersecurity is something that Croatia started regulating quite early on, especially considering the lack of the EU legislation to enforce it. The National Information Security Program of 2005 contained nothing similar to CI or CIIP provisions, but the first marginal changes can be traced to the Security and Intelligence System Act 2006 (BSA 2014). Then, a comprehensive Information Security Act was issued in 2007 which addressed only the access to classified information in the public sphere (The Croatian Parliament 2007). Importantly,

though, it mandated to have Information Security Advisers available for the systems processing and storing such information and established the Information Systems Security Bureau (ZSIS) (www.zsis.hr) as the national information security authority (Vukina 2020). The following Strategy for the Development of Electronic Business in the Republic of Croatia for the period 2007-2010, the Operational Plan for Implementation of the e-Croatia 2007 Program, and the Regulation on Information Security Measures 2008 introduced further security measures that will be later present in, for example, the NIS Directive (risk assessment, operator security plan etc), even though they still did not apply to any other systems but the ones processing classified information. The National CERT (www.cert.hr) was established in 2009 and connected to ZSIS (BSA 2014).

In 2013, the Critical Infrastructure Act did not take cybersecurity of critical assets into account (Mitrevska et al. 2019). A major change was the 2015 Cybersecurity Strategy that Croatia adopted ahead of the upcoming NIS Directive, which recognised that "the security of the cyber space is critical to the security of the critical infrastructure as a whole" (Official Gazette 2015). A great deal was dedicated to critical communication and information infrastructure, as well as the management of cyber crises. Its first objective was to determine the criteria for CII identification, added by cooperation in risk management for ECI (Official Gazette 2015). Overall, the Strategy and the Action Plan to implement it provided more guidance on CIP than any other national strategy and/or assessment at that point (Cesarec 2020).

The 2017 National Security Strategy opened with the national context and "contemporary threats such as terrorism, illegal migrations, ideological and religious extremism, abuse of the cyberspace and different forms of asymmetric and hybrid threats to our stability and security" (SOA 2017). Unlike the previous strategies, this one was focused on terrorism, if maybe rather migration-related. It also recognised effective CIP as a pre-requisite for national cybersecurity and placed it (CIP) as the top strategic goal (SOA 2017). The

Strategy claimed that as part of the EU Croatia is unlikely to experience war, therefore it prioritised civil emergency preparedness to the natural disasters along with tourism (!) as an important industry (SOA 2017). The same year, the Homeland Security System Act listed CIP as one of the six key provisions, while the Annual Work Plan of Coordination for the Homeland Security System of the Republic of Croatia in 2018 and 2019 re-iterated "the need to identify and designate critical national infrastructures" (Mitrevska et al. 2019).

The 2018 Cyber Security Law for Key Network Operators and Digital Service Providers nearly word-by-word transposed the NIS Directive and included an annex with the "criteria for determining the incidents with significant impact on essential service provision" (Cyber Security Law 2018). Lastly, the same year, a proposal for a new Critical Infrastructure Act suggested the establishment of National Infrastructure Protection Centre with additional focus on CII, as well as the energy and transport sectors, which would be consistent with the EPCIP (Mitrevska et al. 2019).

As for the election infrastructure, the regulation is provided by the Republic of Croatia European Parliamentary Elections Act, which has no provisions on cybersecurity or disinformation campaigns as the threats (Sabor 2021). The overall trend is as follows: to date, Croatia has not suffered any visible interference with its elections and generally considers itself a "low tech" state, especially in the electoral processes. Historically, the issues were identified in the minority representation, the media participation, and inequalities for the candidates (IRI 2000). In 2020, the trends changed to the electoral code, constituency boundaries, and the equal participation of women, but still no risk of disruption (OSCE 2020). Before the 2020 presidential elections, the majority of warnings were about demonstrations and rallies, asking the citizens to "refrain from discussing political subjects in public or on social media", and the security of voters during the pandemic (GardaWorld 2019; IFES 2020).

Nevertheless, cybersecurity of elections is indeed proclaimed important for Croatia, since such attacks have been observed in many EU Member States. During the 4th Croatian Internet Governance Forum in 2018, out of 15 messages from the Resistance of Democracy panel 5 concerned cybersecurity and disinformation, including in the electoral processes (IGF 2018). During the 2019 EU parliamentary elections, the State Electoral Commission was also reported to work with the Information Systems Security Bureau against cyber threats (IFES 2020).

Croatia actively participates in international cooperation platforms: RACVIAC – Centre for Security Cooperation which is a representative body for the defence and security sectors in south-eastern Europe based in Croatia; the Balkan Security Agenda Cyber Defence and Cybersecurity Initiative, Balkans Regional Cyber Defence workshops co-hosted with Slovenia, and the Visegrad 4. It also takes part in exercises such as Cyber SOPEx and Cyber Europe 2018 where it faced the scenario of intense cyber-security incident at the airport as part of the CI (Balsec; Blueprint Energy Solutions 2019).

To summarise, a version of the CI concept existed in the Croatian national legislation long before it joined the EU. The transposition started from carte blanche, which is why it seemed textbook clear and cohesive. In practice, although the prior defence-centred approach was well-developed and established, the transition was not harmonised. The defence protection system was not replaced, which led to the assets designated as ‘critical’ and ‘of importance to defence’ at the same time, confusing the coordinating authorities and requiring both representing security specialists to be on-sight (Mitrevska et al. 2019). The draft of the new Long-Term Development Plan of the CAF 2015 – 2024 started with the defence strategy, but included nothing on the CI, for which such long-term plan has not yet been developed (U.S. Department of State 2019a). Additionally, NPRD has a responsibility over CIP, but not the threat assessment which is exacerbated by the poor cooperation with security sector agencies (Mitrevska et al. 2019). In the recent years, CIP has been more

and more included in the strategic documentation of the state. However, despite the perfect opportunity to avoid confusion and duplication, the lack of the political will has inhibited progress based off a great – in theory – framework.

Analysis

Bossong (2014) argued that the 2005 Green Paper was too ambitious in including eleven critical sectors since the divergent understanding of what constitutes an 'essential service' would be difficult to match among Member States. However, a look at the national CI designation by sector reveals that it was not as much the case as to agree on only two sectors in the end:

Table 1

France	Sweden	The Czech Republic	Croatia	The EU	The EU (NIS Directive)
Energy	**Energy**	**Energy**	**Energy**	**Energy**	**Energy**
Transport	**Transport**	**Transport**	**Trans-port**	**Trans-port**	**Transport**
Communica-tion, technology, broadcasting	**ICT**	**ICT**	**ICT**		**Digital infrastruc-ture**
Finance	**Financial services**	**Financial market and currency**	**Finance**		**Financial market infrastruc-tures**
Health	**Public health**	**Health services**	**Health**		**Health**
Food	**Food**	**Food and agriculture**	**Food**		

Industry	Trade and industry				
Civilian activities	Social insurances				
Military activities	Protection, security, and safety	Emergency services			
Water management	**Municipal services**	**Water treatment systems**	**Water manage-ment**		**Drinking water supply and distribution**
Legal activities	**Public administra-tion**	**Public administra-tion**	**Public sector**		
Space and research			Science and education		
			Produc-tion, storage, and transport-tation of dange-rous goods		Banking
			National monu-ments and values		

All the states (except for Croatia since it was not an EU Member State in 2008) had already established their lists of critical sectors by the time the ECI Directive rolled out, and they happened to coincide in ICT, health, food, water management, military and security services, and public administration designation as opposed to only energy and transportation. The NIS Directive partially rectified the gap and it is understandable that Member States would not perceive any external regulation over their state administration and military feasible. However, the Directive adoption did not go without caveats either. The following table shows the sectoral picture of the NIS Directive transposition:

Table 2

France	Sweden	Czechia	Croatia	The EU (NIS Directive)
Energy	**Energy**	**Energy**	**Energy**	**Energy**
Transportation	**Transportation**	**Transport**	**Transport**	**Transport**
Digital infrastructure	**Digital infrastructure**	**Digital infrastructure**	**Digital infrastructure**	**Digital infrastructure**
Financial market infrastructure	**Financial infrastructure**	**Financial market infrastructure**	**Financial market infrastructure**	**Financial market infrastructures**
Health	**Health sector**	**Health sector**	**Health sector**	**Health sector**
Drinking water supply and distribution	**Drinking water**	**Drinking water management**	**Drinking water supply and distribution**	**Drinking water supply and distribution**
Banking	**Banking operations**	**Banking**	**Banking**	**Banking**
Logistics systems		Chemical production	Business services for state authorities	

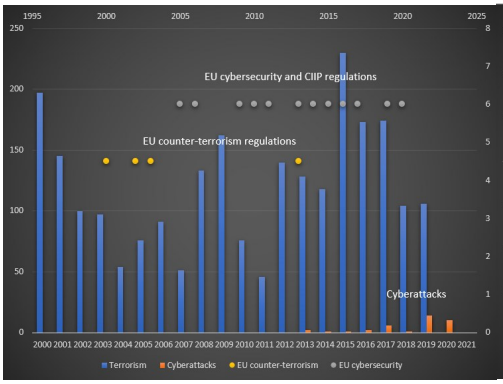
Financial services				
Insurance				
Social services				
Employment and professional formation				
Education				
Restauration				

As evident, each Member State included all the recommended sectors in their transposing legislation; however, neither formally added banking as a separate sector in amended acts or all their own national sectors into the transposition (which might mean they only wanted to transpose it strictly formally), while each state but Sweden took it as a creative opportunity to add sectors on top (neither of which correspond with their initial designation). Consequently, in all four cases, Member States have two independent lists of critical sectors – one in a CIP and one under the cybersecurity/CIIP framework.

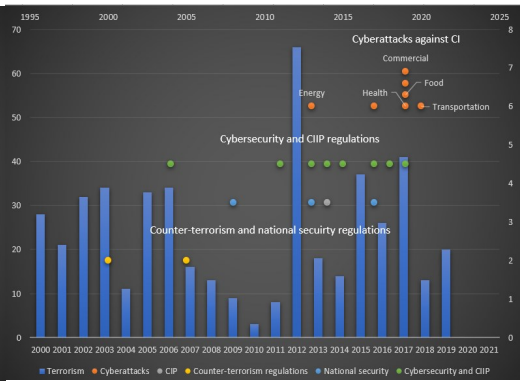
As an illustration of what CI designation means in the EU, a Member of the European Parliament Aldo Patriciello asked the European Commission if the EU was going to create a list of critical dams and provide assistance to the operators of hydroelectric power plants after the 2016 and 2017 earthquakes in central Italy, the answer of the Commission being that the dams did not fall under the jurisdiction of the 2008 Directive and such provisions were not provided by the specialised Floods Directive 2007/60/EC either (Anglmayer 2021). The basis of the securitisation of CI, therefore, is the promise by the respective authority to protect the valuable resources and services even though they are defined by the transborder flows that surpass a particular polity (Langenohl 2020; Turner & Johnson 2017). Since the average level of social

welfare in the EU is high and a major disruption of something as taken-for-granted as drinking water supply would come as even more of a shock, the EU as a securitising actor can apply extraordinary measures (Waever 1996) including partially infringing a state's sovereignty by taking over the matters of security. At this point, it is important understand whose interests the EU fights for (its own as a supra-national formation, the EU citizens, Member States, their citizens separately) and what constitutes an audience for its securitising speech.

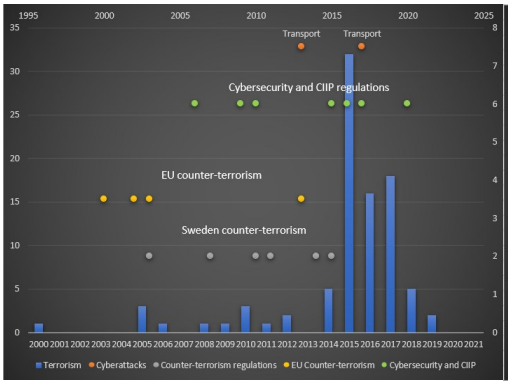
To provide an empirical basis for the further analysis, the timeline of adopting relevant CIP regulations is checked against the attacks statistics from GTD and SMICI. This will allow to verify on the initial step whether and risk dynamics are a major factor in the CI securitisation. The timelines of regulations are presented in Annex A, full-size graphs – in Annex B.



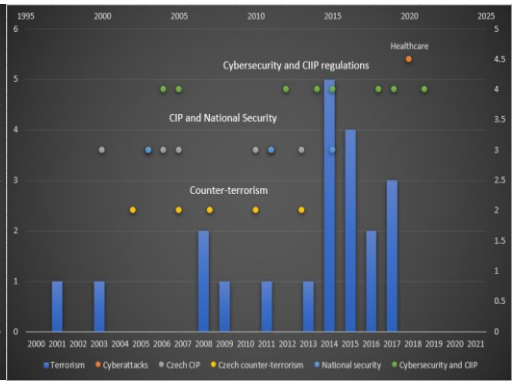
a)



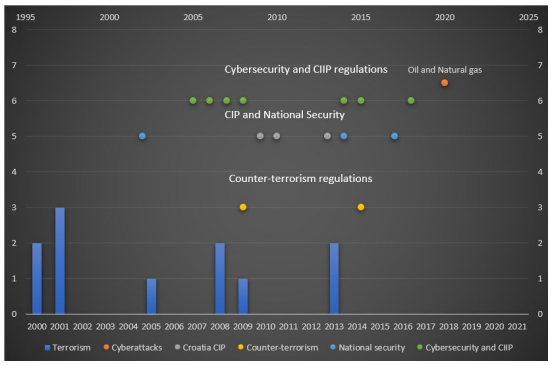
b)



c)



d)



e)

Graph 1: a) the EU, b) France, c) Sweden, d) the Czech Republic, e) Croatia

The 2019 evaluation showed that the questionees perceived the cyberattacks as posing the biggest threat to CI in the EU, then the energy supply disruption, natural disasters, and terrorist attacks (European Commission 2020a). By setting targsubtype1_txt of the GTD dataset to cover the sectors from the NIS Directive (since it reflects the best consensus by Member States to date), the following proportions of targeting CI in terrorist attacks was drawn:

Table 3

State	**Total attacks**	**Attacks against CI**	**Portion**
The EU	2,401	339	14.1%
France	477	37	7.7%
Sweden	91	1	1.1%
Czech Republic	21	4	19%
Croatia	11	2	18%

In neither case did the attacks against CI cross the threshold of 1 out of 5. In Czech Republic and Croatia, the level is the highest, but these are also the states with the lowest rate of terrorism. Although the statistic does not reflect the magnitude of attacks, the focus of counter-terrorism policies on CIP does not have a strong representation in the empirics. The same can be seen on Graph 1:

CIP regulation started after 9/11 and accelerated after 2004 (Madrid bombings), but then the representation stopped altogether until 2013 (which might correspond with the rise of ISIS, although the regulatory trend did not last anyway). The number of cyberattacks has indeed been on a rise for the past 8 years; the regulation, however, has been consistent since 2005 (the securitisation of cyber).

In France, the terrorist threat has been persistently high, but CIP regulation is not truly correlated with it. If anything, CIP in cybersecurity shows correlation with the terrorist trend instead of the cyberattacks against CI, especially since a new wave started in 2010-2011. A similar picture is observed in Sweden: counter-terrorism regulations correlate more with the ones by the EU than the actual attacks, while CIP in cybersecurity started in 2007 (Estonia) and follows the trend closely. In Czech Republic, although the 2014 incident is called 'state terrorism' by the media, the circumstances have just recently been revealed and are yet to take effect which will most likely be strictly diplomatic. Otherwise, the number of attacks has been indeed consistently low; nevertheless, the CIP trend started with the first EU policies in counter-terrorism regulations and then followed with a certain regularity, as well as coincided at least three times with CIP regulations themselves. The beginning of CIP in cybersecurity also coincided with the EU regulations but accelerated after 2013 (the 2013 cyberattacks). Finally, in Croatia all the regulations started a few years before joining the EU, while several cybersecurity regulations in a row after 2007 were likely released due to the attacks in Estonia. The following regulations are grouped within several years after becoming a Member State; with the national frameworks harmonised and the next ECI Directive not released yet, CIP has been almost absent from the Croatian discourse for the past few years.

To summarise, with the exception of the Czech Republic's reaction to the 2013 cyberattacks and the surge of cyberattacks in the EU, for all the talk about 'increasing threats', national trends and thresholds do not seem to correlate with the timeline of CIP regulations adoption in any Member State or the EU in

general. The frameworks adopted in the early 2000s do seem to have encouraged some national response. Since then, the regulations were issued either in a regular manner or as a reaction to milestone events (mostly Madrid and Estonia, so not even on the states' own soil).

The analysis of the CIP regulatory documentation allowed to identify the following topics and their occurrence (the values are the number of documents mentioning an expression):

Topics/Country	**FR**	**SW**	**CZ**	**CR**	**EU**
Threats to the entire society/societal functions	1	5	4	4	1
Vital to growth/development/economic stability/prosperity	1	2		2	6
Threat to democracy/democratic society	5	2	1	2	14
ICT used as means for (physical/terrorist) attacks/unconventional means	4	1	2	2	3
Fundamental interest/issue/freedom	3	3	3		2
Application in future technologies		2			3
Confidence in public institutions	1	1	3		7
The 2016 US presidential election	1	1			9
The 2017 DNC hack	2				
The 2019 EU elections			1		
Threat to international/global peace/security	2	1	2		2
A global phenomenon/threat/globalisation/connected world	1	2		1	1
Different actors/contexts/complex environments/increased sophistication	3	1	2	2	2
Everyone's interest/responsibility/cannot solve alone/solidarity/international cooperation is necessary/collective		2	2	2	12
The most/one of the biggest changes/challenges/attack		1	2		3
Cost-benefit/perceived cost of interference	2	1			1
Russia's attacks	4		4		10

Unexpected/cannot be predicted fully/as opposed to expected risks/beyond control (frequently connected to a proactive approach/proactivity)		1	1		1
Difficult to recover from	2	1			1
Limited resources		1			
Transparency/a unified stance/message/harmonised/consistency		1			3
Clear criteria			1	2	2
Increased/growing/critical dependence on ICT = increased vulnerability	2	2	4	2	4
Strategic/key/primary interest(s)/priority	5	2	6	3	6
Asymmetric/emerging/not emerging/new	1	1	2	2	4
Political leverage/at the expense of the state	1		1		1
Vital/essential/crucial/substantial/serious(ly)/particular/high level of/special/constant/long-term/dominant threat/vulnerability/incontestable importance (when not in the definition)	8	3	7	9	18
Critical elections/'red zone'/as an emerging threat	3		3	1	2
Basic/daily functions/services/infrastructures/needs			3		2
No borders/far-reaching/transnational/transborder/cross-border implications/pan-European	3		2	1	12
Appalling/terrifying/brutal/deadly/devastating/severe/heavy (casualties)/hateful/violent/shocking/tragic/barbarism/destructive/massacre /atrocity(ies)/nightmare/dramatic/striking/anarchy/unique	9		5	2	3
Euroscepticism/putting individual interests above those of NATO and the EU/Brexit			2		5
Potential spillover of conflicts beyond the EU border/neighbouring countries (within the EU)/cascading			1	1	9
Backbone/linchpin/keystone/underpinning/epicentre	3			1	2
Core values				1	
Interdependence/interoperability	2	1	1	1	10
Significant for both/bilateral				1	

Large-scale destruction/attack/damage	2			1	1
The Madrid bombings	1				4
Can be us next/not naïve anymore	4				4
A wake-up call/turning point/milestone	1				1
The 2007 crisis/incident/attack in Estonia	1		1		5
Dynamic	1	2	2	1	2
The Covid-19 pandemic					4
Internal/single market					3
Gaps/differences between/fragmented national approaches/criteria are an issue					7
The failure of electricity grids in 2003, 2006					2
A leading role of the EU					2
The 2017 cyberattack in France					3

The analysis of the topics allows to find several distinct groups of expressions and patterns of their use. First, the consequential chains 'fundamental interests – increased sophistication and complexity – more difficult to protect', 'complex environment + dynamic + difficult to recover from + unexpected – inevitable', 'transborder + globalisation + a threat to the international security – in everyone's interest', and 'Russia – US – democracy – confidence' are the most common.

Overall, the 'strategic interest' and the 'vital' securitising groups are used a lot. A distinct group consists of comparing the situation to the crises that already happened: the US presidential election, the attack on DNC, Estonia 2007, France 2017 (except for France itself), Madrid 2004 (London 2005 only once). A general conclusion is that a threat is less of a fundamental issue until it happens to someone, which is a classic case of positive risk underestimation. 'Threats to the entire society' and 'fundamental interests' are related to a notion

that CI is part of the nature of the modern society, where millions of people are served by the same networks (Langenohl 2020); therefore, the threat is existential and inevitable.

There is distinct group of highly emotional language: words like appalling, terrifying, brutal, shocking, tragic, barbarism, nightmare, striking, and unique are rather 'loud' even by the securitisation standards. A peculiar piece of research might help explain the value of such language. The most frequent emotional reaction to an attack is anxiety or anger (Huddy & Feldman 2015). Here, 'we can be next' reflects anxiety; however, it was rather anger in the American populace that made the people support a foreign invasion. After the 2015 attacks in Paris, a study showed that only a small part of the population felt vulnerable, like the next victims. Instead, the attack was seen as an attack on the nation, which resonated with national identities and elicited anger (Huddy & Feldman 2015). Even the academic literature in the break between 9/11 and London and Madrid was highly emotional, while afterwards it became much more pragmatic (Wilson 2004). Securitising by appealing to the anger is a powerful political justification tool.

There are also observable case-specific patterns. First, one distinct group is used predominantly by the EU: France 2017, the 2003 and 2006 electric grid failures, gaps/differences between/fragmented national approaches/criteria, threats to the internal/single market, and the Covid-19 pandemic. As for the latter, the EU is the only actor to have highlighted the increased vulnerability to what we consider as low-probability events (European Commission 2020d). Next, comparison to Estonia is often added by the examples of Ukraine and Georgia. This might be explained by the wider political neighbourhood that is of concern to the EU but not so much the Member States. The national use of 'interdependence' is added by the 'interoperability', 'no borders' and 'everyone's interest' combine into 'no one can solve it within their national context', 'everyone's interest' turns into 'everyone's responsibility', and the use of 'globalisation' and 'threats to the international security' is rather rare, which

might indicate the priority of the EU. 'Democracy' is used twice as much as 'confidence' – a combination jointly utilised by Member States to explain the value of democracy, while in the EU it appears a reason enough in itself. Finally, as opposed to Member States (more so in France and Czech Republic), the EU does not use much of the emotional language; instead, the trends are 'the US', 'confidence', 'the collective interest', 'cross-border', and 'interdependence', but little of 'consistency' and 'a unified message', likely not to impede the recognition of diverse approaches. 'Russia's attacks' is frequent too, while the 'potential spillover' is used more than by anyone else and might be a reflection of the famous cascading effect.

As for the national patterns, Czech Republic is the only other state to use 'Euroscepticism', even if in the EU it mostly takes a form of 'the tragedy of Brexit'. By the distribution of expressions, France is the closest to the EU with a predominant counter-terrorism focus ('ICT as physical threat', 'threats to democratic societies', mostly from terrorism, and 'the first major/suicide/the deadliest attack on French soil') and more emphasis on the DNC hack than the presidential election. Both France and Czech Republic, having suffered from cyberattacks, openly attribute them to Russia, while Croatia and Sweden do not. After all, in the election interference assigning blame for an attack is, ultimately, a political decision. On the emotional language, France uses it for political pressure against disinformation and cyberattacks, Czech Republic – the economic and resource dependence (also the only one to use 'basic functions'), Sweden does not use it much at all except for the threats 'to the entire society' and 'democracy', while unique to Croatia is 'core values', which might correlate with their designation of national values and monuments as critical and the focus on tourism, as well as the Cold War past (likely reminiscent of the predominant Czech combination of 'asymmetric' and 'strategic'). Said explicitly in France, in Czech Republic 'can be us next' takes a form of 'show of solidarity' to indicate that the mentioned threats are not personal.

Common to all states, a pair ‘emerging/not emerging’ is in one case used to indicate a threat that is unpredictable and beyond the ‘safe’, known risks, while in other it is used to almost shame the establishment for lacking in the defence against the threats that are not new at all. ‘Elections’ and ‘fundamental’ seem to be put together more and more. Finally, cybersecurity as a concept seems to work as a discursive practice with a unique threat representation. Dunn Cavelty (2013) argues that the very image of space as in ‘cyberspace’ reflects the concept of lawlessness and disorder that needs to be organised. The complexity of ICT systems, both technical and logistical, as well as the message that the development of technology is beyond our control, is something the public speech capitalises on to create the ‘too complex – cannot be predicted or completely secured – need more protection’ securitising chain. The ‘increased dependence = increased vulnerability’ stems from there too, as do ‘no borders’, different expressions on the lack of attributability, ‘a basic/daily function’, ‘cost-effectiveness’ and others. When technology is seen as a pre-requisite for the modern life, threats to technology become threats to the entire society (another securitising expression). Additionally, the cyberspace rhetoric is increasingly linked to the defence community. The ‘can be us next’ expression sometimes takes it to an extreme: attacks are either presented as ‘devastating’ or as “Cyber 9/11” and “Electronic Pearl Harbour” (Dunn Cavelty 2013). The idea is simple and reflected in the move by NATO to recognise cyberspace as another operational domain: domain is a space, *our* space is a territory, and the territory needs to be secured by all means necessary.

Results

First of all, a few observations are worth noting. A distinct pattern among Member States is designation through institutionalisation: in Sweden, anything placed under the authority of MSB becomes de facto critical, similarly to the National Protection and Rescue Directorate that coordinates CIP in Croatia. The

Copenhagen School authors claim that securitisation can be institutionalised, too, so that a securitising move does not have to justified every time as long as it falls within the current political reality (Buzan et al. 1998). In the case of the EU, the 2005 Green Paper suggested establishing a single agency to coordinate the European CIP, which was later rejected. The only viable example is ENISA which, considering the increasing securitisation through cybersecurity, is getting more and more regulatory power.

Another pattern is an origin in the defence sector: attacks on food and water supply are sometimes considered in terms of spreading poisoning and other CBRN effects, cybersecurity is essential for the "legal entities subject to special regulations concerning critical infrastructures and defence", and in Czech Republic and Croatia CIP explicitly started as a military matter etc (Crisis Management Act 2000; Official Gazette 2015). Some Member States came out of the Cold War era preparing for a conflict which is considered unlikely in the EU. Even France with a tendency to 'legislate' against the threats regulates the majority of matters through the Defence White Papers and Military Programming Law, while the explicit CIP documentation is almost absent as evident from the regulations timeline (Annex A).

More specific trends can be only explained within the national contexts. For instance, Sweden sees itself as part of the EU but even more so the Nordic strategic environment. The Counter-terrorism strategy of 2014 emphasises the importance of the Nordic cooperation (Government Communication 2014), the 2017 seminar in Helsinki involved the cooperation on CIP between Finland, Norway, and Sweden, where they consider ICT, energy, food, transport, financial infrastructure, and the health sector critical (Aula et al. 2020), and Sweden participates in the Nordic-Baltic Eight (NB8)-US Roundtable on Cyber Security where it specialises on the critical supply chain (Critical Nordic Flows 2020; Cyberwiser 2021b). Nordic States are comparatively small economies with advanced digital and infrastructural networks, which makes them difficult to maintain especially in terms of retaining skill and personnel. A shift to new

energy sources creates some economic balance but requires further coordination. Betting on minimal complexity might be the Swedish strategy, considering that the NIS Directive transposition was not harmonised with the national regulations, while the national counter-terrorism legislation highly correlates with the timeline of the EU regulations adoption. This might mean that for Sweden a wider designation will mean more (unwelcome) requirements, but possibly also more external funding.

To expand on terrorism, which closely correlates with the use of emotional language, it is commonly viewed as a communication strategy (Rashid & Olofsson 2021), so the securitisation is basically inherent to the matter. In case of Sweden, the state did not suffer from terrorism in the late 20th century, which left it rather unprepared for the 9/11 events in the regulatory sphere. Therefore, terrorist attacks against CI are not a trend. Although in the immediate aftermath of 9/11 the public opinion converged with the others, the threat remained low and it plummeted to 3% of the respondents in various studies perceiving the terrorist threat as 'very high' (to compare, in France it was 54% and in Germany – 31%) (Rashid & Olofsson 2021). Although higher now, it is also still lower than in all the Western Europe. Consequently, securitisation of the terrorist threat to CI is reluctant, which correlates with basically lack of the highly emotional language in the discourse.

Similarly, the Czech Republic had no terrorist attacks or other major physically disruptive purposeful events prior to 9/11; the only related risk comes from being involved in the counter-terrorism efforts (CODEXTER 2007; Strategy 2013). As can be seen from the use of 'basic functions/services', 'dependence' tied to 'strategic interests' and emotional language (and less so 'democracy', for example), dependence on the resource supply is a more securitised risk. Geographical position in the middle of the EU makes the state a transit hub, therefore they see resource dependence as a political lever and securitise 'asymmetric' threats (Centre Against Terrorism and Hybrid Threats for counterpropaganda and counterterrorism together), including Euroscepticism or

putting individual interests before the interests of NATO and the EU as a strategic threat back in 2011. The extensive use of 'spillover' might point to the 2014 crisis in Ukraine: the gap between the first two Security Strategies of 2003-2011 was replaced by a much shorter 2011-2015. Furthermore, in early 2000s the emergency response legislation was updated almost every year, which was replaced by bi-annual Counter-Terrorism Action Plans. Recently however, or more precisely since the 2013 cyberattacks, cybersecurity is developed not only through its own sectoral regulations, but in all counter-terrorism and security strategies (the use of language, especially before the elections, also points to the clear priority). Consequently, since Czech Republic had quite a developed CIP framework before 2008 and CIIP before 2016, the NIS Directive was likely welcome, but not necessarily in such a tight regulatory schedule. What Czech Republic is likely to support is the designation of the supply chain as CI.

Moving forward, Croatia constitutes a separate case since the security sector reforms were first carried out as part of the NATO Membership Action Plan (MAP) in 2002 (Peresin 2013). The state did not, however, retain most of the military focus: the topics both before and after joining the EU include 'society', 'democracy', and 'interdependence'. Arguably, Croatia had to adopt CIP regulations instead of arriving to this question itself, which can manifest in the current lack of interest and political will for development. In fact, the 2013 CI Act is a copy of the 2008 Directive transposed to the national context except for the identification part, which hardly counts as harmonisation. This case might be projected at the other states joining the EU in the future: there is no mechanism to verify if the regulations are simply transposed or harmonised within the national frameworks, while the states will seek the EU legislation rather than technical guidance, and some only when it is compulsory.

In Croatia, terrorism is also considered a low probability which led to a very formal counter-terrorism policy. To be considered safe means to attract tourism, as claimed in the Security Strategy, which might explain the use of 'core values' and the designation of symbols and monuments as CI. The border control is a

trend since the state considers itself a southern EU frontline. This explains the use of 'spillover' similarly to Czech Republic, and the only other one at that. The situation with "the Republic of Croatia and the neighbouring countries" (SOA 2017) is non-trivial: Croatia and Albania signed a Declaration for the construction of the Ionian Adriatic Pipeline (IAP) (Blueprint Energy Solutions 2019), but then, although Slovenia and Croatia have common trans-European roads, they designated no ECI because found "nothing significant for both countries", while Hungary claimed that "their first priority … (is) carrying out the processes of identification and determination of their national CI prior to discussing cross-border impacts" (Mikac & Cesarec 2016). For all the 'spillover', 'cross-border', and 'bilateral' language, this showcases another drawback of the 2008 Directive, which the current proposal for a new directive is repeating: the EU established the bilateral criteria to identify assets critical to *the EU*. Some roadways and energy systems can hold value for the entire formation of the EU, but if two designating states do not consider that they meet the bilateral criteria, they will not be designated as ECI.

Unlike the rest of the cases, France has been a major victim of international and domestic terrorism for decades. Its response has been consistently two-fold: the public criminalisation and the military response. Even so, policies of indiscriminate detention and surveillance introduced in early 1970s were then fiercely criticised by the public (Shapiro & Suzan 2003), and only became tolerated post-9/11. France uses the 'Madrid bombings' as a milestone more than any other case; however, judging by the regulations timeline (Annex A), even then did they continue to focus on criminalisation and surveillance, while CIP was meaningfully added to the framework after the 2015 bombings, and already together with CIIP and disinformation, since media campaigns and other use of technology was a highlight (and continues to be) of the counter-terrorism strategies. The language representation is somewhat territorial: "Security in digital spaces must, therefore, be provided with as much determination as in our cities and all our territories" (Vitel & Bliddal 2015) and "if it's forbidden on the

streets, it's forbidden online" (Poon & Basu 2019), which is reminiscent of the 'worst/first attack *on the French soil*' rhetoric about the 2015 bombings. Therefore, the French CIP policy is rather reactive and the language is highly emotional. The same way it is used to justify deployment of troops to the nuclear power stations, it supports an intrusive, assertive mandate of the ANSSI. Any 'soft' EU governance is unlikely to add value in this regard, as much as the funding is unlikely to impress the operators who are forced to spend a lot of money (by French standards) on CIIP to meet the requirements. However, after the 2017 hack and other interference, especially considering how it correlates with the activity in social media (Saragerova 2020), France is likely to keep pushing for (somewhat controversial) online content regulation.

As for the EU CIP in counter-terrorism, a year after 9/11 the perception was that the response, especially military, was not by the EU, but rather through the initiatives of individual Member States (Walker 2001). While they employed a fragmented approach, the EU went from the counter-terrorism proposal straight to CIP. For instance, back in 2001-2002, France supported the judicial mechanisms but not the CIP protection. While now their approach is more comprehensive, it is still jurisdiction- and surveillance-based, so deriving CIP from the counter-terrorism policy miscalculated Member States' position from the start.

It should not come as a surprise that the initial enthusiasm for a common framework slowed down. A certain historical moment was not accounted for either: since a large part of the EU used to suffer from terrorism in the 20th century, the question itself was politically sensitive. The difference between 'modern' and 'new' terrorism (indiscriminate rather than selectively political) was precisely what initiated the CI securitisation (Argomaniz 2011). Yet, the strategic documentation followed rather than preceded the counter-terrorism policies, and while the EU could have managed at least one of the issues (either CIP or counter-terrorism), the hurdled approach to accommodate divergent national visions only created suspicion and unwillingness to surrender part of

the regulating authority. An exception is France which has lived so long under the threat of terrorism that neither state officials nor the public view the problem as passable. Since the overarching idea is to minimise the risks rather than eliminate them, (Shapiro & Suzan 2003), France is likely the EU's best bet in finally harmonising counter-terrorism and CIP approaches.

Transparency and the culture of relations between the state, the sectors, and the public also vary. In France operators themselves decide what their critical assets are and use ministerial criteria, e.g. the 2016 separate sectoral orders for the critical sectors, while in Czechia the criteria are more universal and publicly available, set in the regulations for the operators. The imposition of unified criteria in more sectors will work differently in such varying environments.

As for CIP in cybersecurity, ICT was de facto considered critical from the start, even if it was not included in the 2008 Directive. To impose at least somewhat comprehensive sectoral regulations on the national governments, the EU adopted the NIS Directive, but with a different list of sectors. Coincidentally enough, all four states released a national cybersecurity strategy within a year prior to the NIS Directive, which begs a question regarding the poor timing (a year after harmonised amendments were unlikely) or communication (how many of the resulting provisions did Member States expect?). The Directive is still the most comprehensive EU CI (CIIP) regulation, but Member States ended up transposing it as if in a regulatory vacuum, even though all the respective strategies contained CIIP provisions and securitised the matter through the majority of the 'vital/essential' group, 'backbone', 'keystone', and 'linchpin'. As it stands, while Croatia is still working towards a unified regulatory system, Sweden and Czech Republic have expressed their expectation for the NIS 2 Directive in the late 2021, and France is likely to remain self-reliant unless the disinformation topic is added to the case.

Finally, the election interference has been called an emerging threat and after the 2016-2017 incidents in the US experts started wondering if those were a new

norm (CSS 2017), which is not, in fact, new at all. In 2006, Harri Hursti demonstrated a cyberattack to influence the voting system in Florida (Grunemwald 2018). Since then, cases have happened in Brasil, the United Kingdom, Costa Rica, Nicaragua, and other Latin American states, Philippines, and Australia among others (Radware 2017). Judging by the language and the establishment of ANSSI in 2007 right after the attack against Estonia (Vinocur 2017), this case is considered a milestone. Nevertheless, it was the US elections that shocked the European community, quite possibly precisely because 'the backbone' of democracy failed. As a measure of precaution, some states simply rolled back to the manual procedures: Sweden, Ireland, Netherlands, France, Finland, and Germany (Dunn Cavelty 2013). In this case 'security' was prioritised over the 'innovation'.

The topic first appeared in the cybersecurity discourse (Helmbrecht 2017), but more and more of the 'political' language moved it to a separate realm. Only Sweden decided not to wait until the next attack and designated the elections infrastructure as critical. It was France, however, whose elections were the closest from the 2016 case, so it was the first to face a potential trend as it was trying to avoid "a nightmare scenario" of the DNC attack just a few months prior (Chebil 2017). At the time, the US attacks were securitised enough in the discourse, so it was likely the lack of time before the elections that made the following Macron's campaign hack treated as inevitable or at least expected.

When in 2018 the next-year elections were closing up, the 'us next' narrative became pervasive. The states managed to agree on a number of things: the EU-led security network for electoral commissions, action plans, budget plans, communications, declarations, a compendium on cybersecurity of elections, and a voluntary code of practice (van der Staak 2021). Ahead of the elections, even private companies agreed under a non-binding obligation to take protective steps; the German Marshall Fund began tracking Russian efforts to influence U.S. public opinion through Twitter (Dorell 2018), while Facebook and Google monitored their content and activity (Brattberg 2019; Cerulus 2021). An extent

of the policy is the project “Countering Elections-related Cyber Threats and Disinformation Campaigns in Ukraine” (ECEP 2019), where the EU followed the neighbouring state’s presidential election almost at the same time as theirs. Positively, the election-devoted disinformation framework led to the establishment of ENISA’s permanent mandate and, for the first time, a certification framework for the protection of CI (Bendiek & Schulze 2019).

In the retrospect, the elections went as well as was possible. Neither a record-high turnout (50.66%) nor almost 14 million of the voters eligible to vote in a Member State other than their nationality (European Commission 2020c) led to any major disruption. The consensus was that the cybersecurity efforts paid off. However, political parties remain the weakest, unregulated link, especially considering that they are not usually willing to share information about security breaches and especially information leaks (van der Staak 2021). The top-level problem is that spending the EU funding on the governmental systems is one thing, but spending on the political parties is completely another. All things considered, the danger is not over. The panel discussion in (Dempsey 2019) presents an interesting case. Out of 14 experts discussing cybersecurity of elections and disinformation, the highlights were supported by: the problem is not just the external interference but rather based on the internal pre-disposition – 7, an agency will not fix everything – 3, failing democracy – 3, risks of regulating speech – 3, media should be designated as CI nationally and in the EU – 1, crisis of trust and confidence/Euroscepticism – 4, on the level of Member States the defence of democracy is the weakest – 4, cybersecurity is key – only 1 (Dempsey 2019). Therefore, expert consensus is that the threats to democracy are not per se election interference, which is presented as emerging, but rather the very much ‘conventional’, known, ‘old’ threats, enabled by technology like anything else. Without addressing these inward-looking issues, the elections and democracy will remain in risk.

The inertia is already evident: France, as a victim to frequent attacks, is advocating for the European Democracy Action Plan. It might be joined by

Czech Republic after the 2014 explosion revelations considering how harsh the reaction language was: “state terrorism that goes far beyond the Salisbury incident”, “appalling crime holds two terrifying primacies”, “the biggest attack on the country in its history”, “the most violent breach of the sovereignty of the EU and NATO members since the end of the Cold War”, “the tip of the iceberg of all the influence operations the Kremlin is conducting in the Visegrad 4 countries”, and “it does not think twice to meddle with their internal affairs brutally” (Kleckova 2021). However, Sweden and Croatia remain silent about the elections and disinformation, whereas the EU is still going through the elections and disinformation framework on the remnant energy. Surely, some might simply think that if nothing happened this time, then the threat is less serious than it really is, while others do not see the threat as realistic at all or are careful not to antagonise Russia.

Implications

If infrastructure is what turns a space into a territory by enabling relations between the actors (Turner & Johnson 2017) and one of the key elements of securitisation is an audience, then to answer the research question we need to identify what the EU considers as the space to control and the audience to address.

An observation might support the answer: in the recent CIP programme (EC CIP), in the context where the states themselves use ‘the society’ (“threats to” or “interests of”), the EU indicated ‘Member States’ instead. Additionally, the analysis has shown a considerably less frequent use of emotional language by the EU as opposed to the states. Certainly, the EU strives to protect the citizens, but ultimately, its primary interest is to secure itself as a supra-national formation: the audience are Member States. It means that while the EU acknowledges the ‘mainstream’ threats (terrorism, cyberattacks), their implications are unique to the actor. For instance, election interference might

result in unfair outcomes, but the EU's ability to fill in the Parliament's seats ensures its political value as a formation and, therefore, existence. Similarly, Euroscepticism might be indirectly damaging to a state if the government's policies align with those of the EU, but for the EU itself it is a question of survival. The EU securitisation problem in a nutshell is that for a state, survival means sovereignty (Waever 1996), while for the EU it is a combination of sovereignty, political and social identity, and integrative function. Since any EU regulation basically involves some infringement of a Member State's sovereignty, the important questions are how exactly the EU can do it and where Member States draw the line of tolerance.

Aradau (2010) claims that the securitisation of CI is primarily "about the protection of objects". For the EU, though, it is predominantly about the protection of interests. First, in a sense, 'criticalisation' depoliticises a sector (security of the society is above politics), which allows to easier manage the conflicting interests of Member States. Next, formally designated critical infrastructure falls under the protection of international law (Eichensehr 2017); thus, the EU can exercise its mandate to impose legal consequences in a more guaranteed, pragmatic manner. If there is something the EU is successful at, that is an "extensive capacity for institutionalisation, normalisation and regulation" (Neal 2009), which is, as observed in the Analysis section, already a trend in CIP.

A comprehensive policy recommendation is beyond the scope of this dissertation. What follows is a set of observations related to generic potential actions. While covering France, Sweden, Czech Republic, and Croatia as case studies cannot represent the entire EU, it provides a vivid sample of fragmentation among Member States' contexts and interests. First the treatment of risk in the discourse should be considered. In the EU, a conventional military attack is considered unlikely, so any exhibition of physical destruction is used as a securitising case to attract funding. The states decide what they have enough reasons and resources to be afraid of: France is a strong economy with a

terrorism problem, to an extent where it would engage the military to protect its critical assets. Sweden does not consider terrorism as much of a threat, but their extensive ICT networks require protection, so the CIIP is a more relevant topic. Then, there is political vulnerability highlighted by Czech Republic, so if the EU could clearly link strong infrastructures (specific sectors) to the political stability, Czech Republic would follow suit. Lastly, Croatia can serve as a case for the states to join the EU in the future, so the system needs to be comprehensive enough to be considered for the harmonisation at all, but also dynamic to allow for the adjustment to national contexts.

As it stands, the infrastructural mandate of the EU balances between the necessity to secure the transnational infrastructures and the aversion of Member States to overregulation, all without any standard to substantiate it. One of the problems is Member States' scepticism over the added value from the EU-level CIP. As mentioned above, the EU does not use emotional language extensively, since for the states it is not sufficient to label something vital' and 'fundamental'. CI designation usually expected to ensure consistent attention and dedicated resources, but in practice the EU does not have such an obligation. Without evident benefits of designation, a longer list of sectors and stricter requirements in the new Directive will only lead the states to do a formal bare minimum, especially with the EU's further actions unclear, the sectors seemingly protected, and since the new Directive is not supposed to replace the domestic legislation. A reciprocity mechanism could greatly benefit the situation: there are already existing funding projects (e.g. Horizon 2020) dedicated to CIP. Reluctance of Member States might be decrease if the projects were organised under a single CIP framework. From a securitisation standpoint, the states do use the language of 'consistency' and 'long-term commitments', which is precisely what the EU could project. By designating CI, the EU should not just assign, but also assume responsibility.

The EU does not use the 'international' language much and understandably so, since overly high attention to the outside feeds Euroscepticism. However, states

seem to prioritise the same national-foreign-international events pattern: France reacted very strongly to the 2016 US election but introduced its measures after the 2017 incident of its own. The states condemned 9/11 attacks, but most of the counter-terrorism frameworks mention Madrid as a turning point. Other examples include Ukraine, Estonia, Georgia, France, and the United Kingdom. The 'us next' language seems to have worked well enough to mobilise the protection of the 2019 elections. An effective way to translate international events into the EU context could be beneficial, as well as clear communication of vulnerabilities when their cross-border effects are not as evident as, for example, for energy and transportation.

Insufficient data is now rarely a problem, it is rather a lacking capacity to process it. According to Kapellmann and Washburn (2019), practitioners in CIP prioritise quality of data in information sharing over anything else, while the question about a list of dams shows an example of interest. The EU could make it explicit that designation of a sector would entail access to the best-quality information – timely, specific, operationalised, attributable, and gathered in one place. ENISA, for instance, is not an intelligence agency and would not risk the same information sharing repercussions, which can be utilised to everyone's benefit.

Finally, attention should be paid to the securitising language used by Member States and its correlation with the pragmatic risk to find a way to support the nationally designated sectors (what Member States consider critical and not vice versa). Surely, funding opportunities might lead to oversecuritisation, but if the upcoming Directive manages to introduce the proposed common methodology for risk assessment, the EU will have a collectively agreed on verification mechanism.

Conclusions and Further Discussion

The present research paper aimed to analyse how and why the EU Member States use securitisation in their national CI identification and designation. On the cases of France, Sweden, Czech Republic, and Croatia the analysis has shown that the states do not use empirical trends to designate certain sectors as critical as much as resounding, 'securitisable' events to launch policies, which is not reflected in the current EU CIP common approach.

For all its drawbacks, the 2008 Directive did raise awareness and improved collaboration on the matter: half of the MSs did not have a definition of CI and ten did not have a mechanism for CI-related information sharing prior to 2008 (European Commission 2020a), and as compared to twelve in 2012, today all Member States have a formal cybersecurity strategy (Helmbrecht 2017). If anything, the Directive made CIP a matter of the EU-level importance. Nevertheless, the actual ECI designation was very fragmented and uneven, while Member States with CIP frameworks developed by 2008 did not see much added value in the Directive (European Commission 2020a). Is good enough result good enough when it comes to something as 'vital' and 'fundamental', as Member States themselves put it, as CIP? Are the short-term measures, like the rollback on e-voting, to become a trend of technologically regressive decisions?

Looking forward, in the upcoming months we will observe the run and regulation of the elections in Germany (26th September) and Czech Republic (8-9th October) (Anderson 2021). Another interesting case for further discussion is the way that the concept of CI was handled at the beginning of the ongoing Covid-19 pandemic, more specifically – the formal use of the expression 'essential workers' when in early 2020 the states started to restrict the popular mobility within their borders. The US issued a guideline "Identifying Critical Infrastructure during Covid-19" providing a clear list of sectors to which certain limitations did not apply and referencing the official national CI list (CISA 2021b). In neither of the studied states did the list of essential workers directly

correlate with the national CI designation, even though ‘the provision of essential services’ sounds exactly like the definition of CI. What is more, as highlighted in the analysis, criticality of the elections morphed out of (and is still closely related, although not limited to) cybersecurity; both the latter (e.g. Deloitte 2021), CII, and the role of disinformation arisen very quickly as the topics within the pandemic discourse.

The relation between infrastructure and the pandemics is a topic that requires further research. Normatively, as an enabler of flows, CI facilitates not only the establishment of relationships and the movement of goods, but also the spread of malicious things like drugs and, in this instance, diseases. As a precedent, historians agree that the road connection played a defining role in the spread of the Black Death (Turner & Johnson 2017). The ongoing pandemic, however, was the first such ‘reality check’ since the formal introduction of CIP in early 2000s. Time might have to pass for the quality data, to appear, but the seemingly ad hoc nature of the ‘essential services’ designation, the use of the term separately from the CI itself, and more broadly the use of securitisation by Member States during the pandemic could provide interesting insights.

Amidst the pandemic, a proposal was issued for a new CI Directive. While it is much more comprehensive and rectifies many drawbacks of the previous regulations, it still does not take into account all of the suggestions from the 2019 Evaluation Report, especially in the way it falls short of the provisions suggested in the NIS2 Directive proposal. Furthermore, in its current form (which will not necessarily reach the adoption), the proposal addresses national CIP but not the way its provisions should be harmonised with the national legislation, and if Member States’ approach has not changed, there is no guarantee that the new directive will not end up outside of the national CIP framework.

In individual cases (the NIS Directive, Galileo) Member States have shown considerable preparedness to cooperate. Certainly, it is a compromise between

politically and practically feasible solutions and innovative drives, so first problem the EU needs to tackle is scepticism towards ambitious cooperation projects. When combined with the political interest, CI securitisation did stimulate progress; for the strong future policies, the EU could empower regional groups of like-minded states to lead in resilience from what they perceive as threats: terrorism for Spain and France, interdependence for the central region etc. Since CI identification is still voluntary, a political process should include a transformation of threats to individual homelands into a common interest.

The ultimate question is, for all the emphasis on 'the EU leadership', if the EU sees itself as a governing security actor. If not, if it is to remain a fragmented security community (Wilson 2004), then patching regulations that, in practice, do not fit in the national frameworks as much as the broader EU picture will only serve to create confusion. As Delpech (2002) put it in 2002, "It must be hoped that it will not take another catastrophe on European soil to rouse Europe from its current slumber."

Acknowledgments

The author would like to express gratitude to Dr. Rhyner Washburn and Dr. Steve Sin from the National Consortium for the Study of Terrorism and Responses to Terrorism for supplying the updated Significant Multi-Domain Incident against Critical Infrastructure dataset.

Bibliography

Aagedal, J.O., den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D. & Stolen, K. (2002), "Model-based risk assessment to improve enterprise security", IEEE, , pp. 51.

Abernethy, J., Anderson, C., Dai, C., Farahi, A., Nguyen, L., Rauh, A., Schwartz, E., Shen, W., Shi, G., Stroud, J., Tan, X., Webb, J. & Yang, S. (2016), "Flint Water Crisis: Data-Driven Risk Assessment Via Residential Water Testing".

Adedigba, S.A., Oloruntobi, O., Khan, F. & Butt, S. (2018), "Data-driven dynamic risk analysis of offshore drilling operations", *Journal of petroleum science & engineering,* vol. 165, pp. 444-452.

Agence Nationale de la Securite des Systemes d'information (2020). *The French CIIP Framework*. [online] ANSSI. Available at: <https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/> [Accessed 7 November 2020].

Anderson, E. (2021). *European elections to watch in 2021*. [online] POLITICO. Available at: https://www.politico.eu/article/2021-elections-to-watch-europe/ [Accessed 3 May 2021].

Andrea, R. & Bernhard, H. (2010). *Protecting critical infrastructure in the EU: CEPS task force report*, Centre for European Policy Studies.

Anglmayer, I. (2021). European critical infrastructure Revision of Directive 2008/114/EC. *European Parliament*. [online] Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf [Accessed 27 Mar. 2021].

ANSSI (2016). *Sharing the French approach to Critical Infrastructure Protection at CyberGov 2016 (Warsaw)*. [online] ANSSI. Available at: https://www.ssi.gouv.fr/en/actualite/sharing-the-french-approach-to-critical-infrastructure-protection-at-cybergov-2016-warsaw/ [Accessed 3 Apr. 2021].

ANSSI (2021). *Cybersecurity in France*. [online] ANSSI. Available at: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ [Accessed 12 Mar. 2021].

Aradau, C. (2010), "Security That Matters: Critical Infrastructure and Objects of Protection", *Security dialogue,* vol. 41, no. 5, pp. 491-514.

Archick, K., Ek, C., Gallis, P., Miko, F.T. and Woehrel, S. (2006). *European Approaches to Homeland Security and Counterterrorism*. [online] CRS Report for Congress. Available at: https://fas.org/sgp/crs/homesec/RL33573.pdf [Accessed 15 May 2021].

Argomaniz, J. & ProQuest (Firm) (2011), *The EU and counter-terrorism: politics, polity and policies after 9/11,* Routledge, London;New York.

Auchard, E. (2017). Macron campaign was target of cyber attacks by spy-linked group. *Reuters*. [online] 24 Apr. Available at: https://www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200 [Accessed 21 May 2021].

Aula, I., Amundsen, R., Buvarp, P., Harrami, O., Lindgren, J., Sahlen, V. and Wedebrand, C. (2020). Critical Nordic Flows: Collaboration between Finland, Norway and Sweden on Security of Supply and Critical Infrastructure Protection. *National Emergency Supply Agency*.

Bendiek, A. and Schulze, M. (2019). *Disinformation And Elections To The European Parliament*. [online] Swp-berlin.org. Available at: <https://www.swp-berlin.org/10.18449/2019C16/> [Accessed 14 November 2020].

Blaauwbroek, N., Nguyen, P. & Slootweg, H. (2018), "Data-driven risk analysis for probabilistic three-phase grid-supportive demand side management", *Energies (Basel),* vol. 11, no. 10, pp. 2514.

Blueprint Energy Solutions (2019). *Final Report - Study on cyber security in the energy sector of the Energy Community*. [online] Available at:

https://www.euneighbours.eu/sites/default/files/publications/2020-02/Blueprint_cyber_122019.pdf [Accessed 5 Mar. 2021].

Brangetto, P. (2015). *National Cyber Security Organisation: France*. [online] *CCDCOE*. Available at: https://ccdcoe.org/uploads/2018/10/CS_organisation_FRANCE_032015_0.pdf [Accessed 3 Feb. 2021].

Bossong, R. (2014), "The European Programme for the protection of critical infrastructures - meta-governing a new security problem?", *European security (London, England),* vol. 23, no. 2, pp. 210-226.

BSA The Software Alliance (2014). *Country Report: Croatia*. [online] BSA. Available at: www.bsa.org/EUcybersecurity [Accessed 25 Feb. 2021].

Bulckaert, N. (2018). *How France successfully countered Russian interference during the presidential election*. [online] euractiv.com. Available at: https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/ [Accessed 13 May 2021].

Bures, O. (2006), "EU Counterterrorism Policy: A Paper Tiger?", *Terrorism and political violence,* vol. 18, no. 1, pp. 57-78.

Buzan, B., Wilde, J.d., Wŷver, O. & ProQuest (Firm) (1998), *Security: a new framework for analysis,* Lynne Rienner Publishers, Boulder, Colorado.

Cederberg, G. (2018). *Catching Swedish Phish: How Sweden Is Protecting Its 2018 Elections*. [online] Belfer Center for Science and International Affairs. Available at: <https://www.belfercenter.org/publication/catching-swedish-phish-how-sweden-protecting-its-2018-elections> [Accessed 18 November 2020].

Cerulus, L. (2020). *US calls out Russia for Macron campaign hack, even as France stays silent*. [online] POLITICO. Available at:

https://www.politico.eu/article/us-russia-macron-campaign-hack-2017-election-france-attribution-gru/ [Accessed 5 Mar. 2021].

Cerulus, L. (2021). *Facebook promises to ramp up security for German election*. [online] POLITICO. Available at: https://www.politico.eu/article/facebook-promises-to-ramp-up-security-for-german-election/ [Accessed 1 Jun. 2021].

Cesarec, I. (2020), *Beyond Physical Threats: Cyber-attacks on Critical Infrastructure as a Challenge of Changing Security Environment – Overview of Cyber-security legislation and implementation in SEE Countries*, Veleučilište Velika Gorica.

Chatzky, A. and McBride, J. (2020). *China's Massive Belt and Road Initiative*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative [Accessed 13 May 2021].

Chebil, M. (2017). *France takes steps to prevent an election hack attack*. [online] France 24. Available at: https://www.france24.com/en/20170114-france-vulnerable-cyber-attacks-hacking-presidential-elections [Accessed 17 Jun. 2021].

CIPedia (2021). *Critical Infrastructure Sector - CIPedia*. [online] websites.fraunhofer.de. Available at: https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector#cite_ref-22 [Accessed 12 Feb. 2021].

CODEXTER (2007). *Czech Republic: National Legislation*. [online] Available at: https://rm.coe.int/16806415ef [Accessed 5 Mar. 2021].

CODEXTER (2012). *Czech Republic: Profiles on Counter-Terrorism Capacity*. [online] Available at: https://www.legislationline.org/download/id/4207/file/Czech_CODEXTER_Profile_2012.pdf [Accessed 12 Mar. 2021].

CODEXTER (2014). *Sweden: Profiles on Counter-Terrorism Capacity*. [online] . Council of Europe. Available at: https://rm.coe.int/1680641033 [Accessed 23 Mar. 2021].

CODEXTER (2016a). *Croatia: Profiles on Counter-Terrorist Capacity*. [online] Council of Europe. Available at: https://rm.coe.int/168064100f [Accessed 29 Apr. 2021].

CODEXTER (2016b). *France: Profiles Nationaux Relatifs a la Capacite de Lutte Contre le Terrorisme*. [online] Council of Europe. Available at: https://rm.coe.int/16806ed4f6 [Accessed 29 Apr. 2021].

Copeland, C. (2008), *Terrorism and Security Issues Facing the Water Infrastructure Sector*, Library of Congress. Congressional Research Service.

Corredoira, L., Bel Mallen, I. & Cetina Presuel, R. (2021), *The Handbook of Communication Rights, Law, and Ethics,* John Wiley & Sons, Incorporated, Newark.

Council of Europe (2014). *EU macro-regional strategies*. [online] Routes4U Project. Available at: https://pjp-eu.coe.int/en/web/cultural-routes-and-regional-development/eu-macro-regions [Accessed 23 Dec. 2020].

Counter Extremism Project (2015). *France: Extremism & Counter-Extremism*. [online] Counter Extremism Project. Available at: https://www.counterextremism.com/countries/france [Accessed 12 Mar. 2021].

Counter Extremism Project (2020). *Sweden: Extremism and Terrorism*. [online] Counter Extremism Project. Available at: https://www.counterextremism.com/countries/sweden [Accessed 17 May 2021].

Coward, M. (2009), "Network-Centric Violence, Critical Infrastructure and the Urbanization of Security", *Security dialogue,* vol. 40, no. 4/5, pp. 399-418.

Crisis24 (2021). *Croatia, Europe | Country Profile | Crisis24*. [online] crisis24.garda.com. Available at: https://crisis24.garda.com/insights-intelligence/intelligence/country-reports/croatia [Accessed 1 Jul. 2021].

Crisis Management Act.240/2000 Coll.

Critical Infrastructure Protection. Executive Order 13010 (1996) [online] Available at: https://www.govinfo.gov/content/pkg/FR-1996-07-17/pdf/96-18351.pdf.

The Croatian Parliament (2007), *DECISION ON PROMULGATING THE INFORMATION SECURITY ACT*. Official Gazette, 79/2007 [online] Available at: https://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/Information-Security-Act.pdf [Accessed 15 Jan. 2021].

CSS Cyber Defense Project (2017). Hotspot Analysis: Cyber and Information Warfare in elections in Europe. *ETH Zurich*. [online] Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-08.pdf [Accessed 10 Feb. 2021].

Cybersecurity and Infrastructure Security Agency (2020a). *Election Infrastructure Security | CISA*. [online] Cisa.gov. Available at: <https://www.cisa.gov/election-security> [Accessed 25 November 2020].

Cybersecurity and Infrastructure Security Agency (2020b). *Identifying Critical Infrastructure During COVID-19 | CISA*. [online] Cisa.gov. Available at: <https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19> [Accessed 17 November 2020].

Cybersecurity and Infrastructure Security Agency (CISA) (2021a). *Election Infrastructure Security | CISA*. [online] www.cisa.gov. Available at: https://www.cisa.gov/election-security [Accessed 15 Jun. 2021].

Cybersecurity and Infrastructure Security Agency (CISA) (2021b). *Identifying Critical Infrastructure During COVID-19 | CISA*. [online] www.cisa.gov.

Available at: https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19 [Accessed 3 Jan. 2021].

Cyberwiser (2021a). *France (FR) | CYBERWISER.eu*. [online] www.cyberwiser.eu. Available at: https://www.cyberwiser.eu/france-fr [Accessed 13 Jun. 2021].

Cyberwiser (2021b). *Sweden (SE) | CYBERWISER.eu*. [online] www.cyberwiser.eu. Available at: https://www.cyberwiser.eu/sweden-se [Accessed 5 Jun. 2021].

Deloitte (2021). *COVID-19: The impact of cyber on critical infrastructure in the next normal | Deloitte Global*. [online] Deloitte. Available at: https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/covid-19-the-impact-of-cyber-on-critical-infrastructure-in-the-next-normal.html [Accessed 8 Jul. 2021].

Delpech, T. (2002). International Terrorism and Europe. *Chaillot Papers*.

Dempsey, J. (2019). *Judy Asks: Is Europe Doing Enough to Protect Its Democracy?* [online] Carnegie Europe. Available at: https://carnegieeurope.eu/strategiceurope/78578 [Accessed 3 May 2021].

Den Boer, M. (2003). 9/11 AND THE EUROPEANISATION OF ANTI-TERRORISM POLICY: A CRITICAL ASSESSMENT. [online] Available at: https://institutdelors.eu/wp-content/uploads/2018/01/policypaper6.pdf [Accessed 2 Jan. 2021].

Dettmer, J. (2021). *France, Britain Fearful of Resurgent Jihadist Threat After Lockdown | Voice of America - English*. [online] www.voanews.com. Available at: https://www.voanews.com/europe/france-britain-fearful-resurgent-jihadist-threat-after-lockdown [Accessed 21 May 2021].

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2016). *Concerning measures for a high common level of security of network and information systems across the Union*.

Dorell, O. (2017). *Alleged Russian political meddling documented in 27 countries since 2004*. [online] USA TODAY. Available at: https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/ [Accessed 1 Jul. 2021].

Dorell, O. (2018). *Russia's pattern of meddling abroad exposes threat to 2018 U.S. elections: report*. [online] USA TODAY. Available at: https://www.usatoday.com/story/news/world/2018/01/10/russias-pattern-meddling-money-laundering-and-murder-influence-abroad-poses-threat-2018-u-s-election/1019012001/ [Accessed 3 May 2021].

D'Souza, D. (2021). *France unveils new counterterrorism bill that boosts surveillance of extremist websites*. [online] France 24. Available at: https://www.france24.com/en/europe/20210428-france-presents-counter-terrorism-bill-to-boost-surveillance-of-extremist-websites [Accessed 27 May 2021].

Dunn Cavelty, M. 2013, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review,* vol. 15, no. 1, pp. 105-122.

O'Dwyer, G. (2019). *Sweden's Protective Security Act targets cyber risks*. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/news/252466148/Swedens-protective-security-act-targets-cyber-risks [Accessed 10 May 2021].

Estonian Center of Eastern Partnership (2019). *Post-Election Assessment of the Cybersecurity Infrastructure and Interagency in Ukraine with Related Recommendations*. EU Project Countering Election-Related Cyber Threats and Disinformation Campaigns in Ukraine.

Eichensehr, K. (2017). *Political Parties as Critical Infrastructure?* [online] Just Security. Available at: https://www.justsecurity.org/42470/political-parties-critical-infrastructure/ [Accessed 23 May 2021].

European Commission (2005). *Green Paper on a European Programme for Critical Infrastructure Protection*.

European Commission (2006), *COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection*.COM(2006) 786 [online] Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF [Accessed 13 Dec. 2020].

European Commission (2008). *COUNCIL DIRECTIVE 2008/114/EC On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*.

European Commission (2009), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience."*COM/2009/0149 [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0149 [Accessed 5 Mar. 2021].

European Commission (2011), *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security."*COM(2011) 163 [online] Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF [Accessed 7 Mar. 2021].

European Commission (2017). *EU cybersecurity initiatives working towards a more secure online environment*. [online] Available at: https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf [Accessed 6 May 2021].

European Commission (2018a). *Code of Practice on Disinformation*. Available at: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation [Accessed 5 Mar. 2021].

European Commission (2018b). *Europe that protects: Countering terrorist content online*. [online] Available at: https://ec.europa.eu/info/sites/default/files/soteu2018-factsheet-terrorist-content_en_0.pdf [Accessed 12 Jan. 2021].

European Commission (2018c), *COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*.ST 12104 2018 [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1537456063362&uri=CONSIL%3AST_12104_2018_ADD_5 [Accessed 3 Feb. 2021].

European Commission (2019). *Trans-European Transport Network (TEN-T)*. [online] Mobility and Transport - European Commission. Available at: https://ec.europa.eu/transport/themes/infrastructure/ten-t_en [Accessed 3 Apr. 2021].

European Commission (2020a). *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: final report,* Publications Office, Luxembourg.

European Commission (2020b). *Proposal for measures to enhance the protection and resilience of critical infrastructure*. [online] Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en [Accessed 11 Nov. 2020].

European Commission (2020c). *Reports on 2019 European elections: fostering European debates and securing free and fair elections*. [online] European Commission - European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1123 [Accessed 3 Apr. 2021].

European Commission (2020d), *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities*.COM(2020) 829 [online] Available at: https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf [Accessed 3 Jun. 2021].

European Commission (2021a). *Cybersecurity Policies | Shaping Europe's digital future*. [online] digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies [Accessed 1 Jul. 2021].

European Commission (2021b). *Electoral rights*. [online] European Commission. Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights_en [Accessed 23 Jun. 2021].

European Parliament (2019). *EU Member States test cybersecurity preparedness for free and fair EU elections | News | European Parliament*. [online] www.europarl.europa.eu. Available at: https://www.europarl.europa.eu/news/en/press-room/20190404IPR35103/eu-member-states-test-cybersecurity-preparedness-for-free-and-fair-eu-elections [Accessed 21 Jul. 2021].

European Parliament (2021). *New rules adopted for quick and smooth removal of terrorist content online | News | European Parliament*. [online] www.europarl.europa.eu. Available at: https://www.europarl.europa.eu/news/en/press-room/20210422IPR02621/new-rules-adopted-for-quick-and-smooth-removal-of-terrorist-content-online [Accessed 1 Jul. 2021].

European Union Agency for Network and Information Security (2014). *Methodologies for the identification of Critical Information Infrastructure assets and services Guidelines for charting electronic data communication networks*. ENISA.

European Union Agency for Network and Information Security (2015). *Guideline on Threats and Assets Technical guidance on threats and assets in Article 13a*. [online] Available at: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf [Accessed 3 Feb. 2021].

European Union Agency for Cybersecurity (2016). *CIIP Governance in the European Union Member States*. [online] Available at: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex [Accessed 11 Dec. 2020].

European Union Agency for Cybersecurity (2019). *ENISA Makes Recommendations On EU-Wide Election Cybersecurity*. [online] Enisa.europa.eu. Available at: <https://www.enisa.europa.eu/news/enisa-news/enisa-makes-recommendations-on-eu-wide-election-cybersecurity> [Accessed 14 November 2020].

Export.gov (2019). *export.gov*. [online] www.export.gov. Available at: https://www.export.gov/apex/article2?id=Sweden-Cyber-Security [Accessed 2 Mar. 2021].

Fekete, A. (2011). "Common criteria for the assessment of critical infrastructures", *International journal of disaster risk science,* vol. 2, no. 1, pp. 15-24.

Fischer, E.A. (2018). "The designation of election systems as critical infrastructure", *CONGRESSIONAL RESEARCH SERVICE*.

Ford, N. (2015). *New German Cyber Security Law To Protect Critical Infrastructure*. [online] IT Governance Blog En. Available at: <https://www.itgovernance.eu/blog/en/new-german-cyber-security-law-to-protect-critical-infrastructure> [Accessed 10 November 2020].

FP Insider (2020). *Cybersecurity and U.S. Election Infrastructure*. [online] Foreign Policy. Available at: https://foreignpolicy.com/2020/10/27/election-cybersecurity-cyberattack-critical-infrastructure-voting/ [Accessed 3 Mar. 2021].

France Diplomacy (2019). *France and cyber security*. [online] France Diplomatie - Ministry for Europe and Foreign Affairs. Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/ [Accessed 3 Jun. 2021].

FRENCH national digital security strategy (2015). [online] Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf [Accessed 12 Feb. 2021].

GardaWorld (2019). *Croatia: Presidential runoff election set for January 5*. [online] GardaWorld. Available at: https://www.garda.com/crisis24/news-alerts/299731/croatia-presidential-runoff-election-set-for-january-5 [Accessed 21 Jun. 2021].

Gleick, P.H. (2019), "Water as a Weapon and Casualty of Conflict: Freshwater and International Humanitarian Law", *Water resources management,* vol. 33, no. 5, pp. 1737-1751.

Goud, N. (2021). *National Cyber Security Centre for Sweden*. [online] Cybersecurity Insiders. Available at: https://www.cybersecurity-insiders.com/national-cyber-security-centre-for-sweden/ [Accessed 12 Jun. 2021].

Government Communication 2014/15:146 (2014). *Prevent, preempt and protect – the Swedish counter-terrorism strategy*. Skr. 2014/15:146, Riksdag. Stockholm, 27 August 2015.

Grunemwald, B. (2018). *Piratage de la démocratie : les processus électoraux peuvent-ils être protégés ?* [online] Les Echos. Available at: https://www.lesechos.fr/idees-debats/cercle/piratage-de-la-democratie-les-processus-electoraux-peuvent-ils-etre-proteges-130933 [Accessed 21 May 2021].

Hasicsky Zachranny Sbor Ceske Republiky (HZSCR) (2021). *Population protection and Crisis management division - Fire rescue service of the Czech republic*. [online] www.hzscr.cz. Available at: https://www.hzscr.cz/hasicien/article/crisis-management-in-the-czech-republic.aspx?q=Y2hudW09Mg%3D%3D [Accessed 5 Jun. 2021].

Haemmerli, B. and Renda, A. (2010). *Protecting Critical Infrastructure in the EU*. [online] CEPS. Available at: https://www.ceps.eu/ceps-publications/protecting-critical-infrastructure-eu/ [Accessed 5 May 2021].

Helmbrecht, U. (2017). EU strategies to secure the EU cyber space and critical infrastructure against hackers. AECA Round-Table Conference-Luncheon.

Hirst, N. (2017). *France braces for election cyberattacks*. [online] POLITICO. Available at: https://www.politico.eu/article/france-braces-for-election-cyber-attacks-russia-hacking/ [Accessed 30 May 2021].

Horizon 2020 - European Commission. n.d. *What Is Horizon 2020? - Horizon 2020 - European Commission*. [online] Available at:

<https://ec.europa.eu/programmes/horizon2020/what-horizon-2020> [Accessed 25 November 2020].

Hou, D., Ge, X., Huang, P., Zhang, G. & Loáiciga, H. (2014), "A real-time, dynamic early-warning model based on uncertainty analysis and risk assessment for sudden water pollution accidents", *Environmental science and pollution research international,* vol. 21, no. 14, pp. 8878-8892.

Huddy, L. and Feldman, S. (2015). *What France can learn from how the U.S. reacted to 9/11*. [online] the Washington Post. Available at: https://www.washingtonpost.com/news/monkey-cage/wp/2015/11/18/what-france-can-learn-from-how-the-u-s-reacted-to-911/ [Accessed 12 May 2021].

Idea.int. (2019). *International IDEA*. [online] Available at: https://www.idea.int/ [Accessed 15 Jan. 2021].

IGF (2018). *Croatian IGF 2018 - Final report*. [online] Available at: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3568/1634 [Accessed 7 Mar. 2021].

International Foundation for Electoral Systems (IFES) (2020). *Elections in Croatia 2020 Parliamentary Elections Frequently Asked Questions*. [online] Available at: https://www.ifes.org/sites/default/files/ifes_faqs_elections_in_croatia_2020_parliamentary_elections_june_2020.pdf [Accessed 5 Apr. 2021].

International Republican Institute (2000). *Republic of Croatia Parliamentary Election January 3, 2000 Election Observation Mission Report and Recommendations*. [online] Available at: https://aceproject.org/ero-en/regions/europe/HR/croatia-parliamentary-elections-observation-report [Accessed 3 May 2021].

INSTRUCTION GENERALE INTERMINISTERIELLE RELATIVE A LA SECURITE DES ACTIVITES D'IMPORTANCE VITALE.N°6600/SGDSN/PSE/PSN du 7 janvier 2014 [online] Available at:

https://www.legifrance.gouv.fr/download/pdf/circ?id=37828 [Accessed 15 Feb. 2021].

Izuakor, C. & White, R. (2016). "Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis," *Springer International Publishing*, Cham, pp. 27-41.

JOINT STAFF SUFFOLK VA JOINT AND COALITION OPERATIONAL ANALYSIS DIV (2014). *Multinational Experiment 7. Outcome 3 - Cyber Domain Objective 3.1: Threats and Vulnerability Methodology Version 1.0*.

Jonesday (2016). *France Moves Forward on Cybersecurity Framework*. [online] www.jonesday.com. Available at: https://www.jonesday.com/en/insights/2016/12/france-moves-forward-on-implementation-of-cybersecurity-framework-for-operators-of-critical-infrastructures [Accessed 3 Jun. 2021].

Kadlecova, L., Bagge, D.P., Borovicka, V. and Semecká, M. (2017). The Czech Republic: A Case of a Comprehensive Approach toward Cyber Space. *CCDCOE*. [online] Available at: https://ccdcoe.org/uploads/2017/05/The_Czech_Republic_A_Case_of_a_Comprehensive_Approach_toward_Cyber_Space.pdf [Accessed 12 Mar. 2021].

Kapellmann, D. & Washburn, R. (2019), "Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure", NATO CCD COE, pp. 1.

Kirkpatrick, D.D. (2017). Signs of Russian Meddling in Brexit Referendum. *The New York Times*. [online] 15 Nov. Available at: https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html [Accessed 1 Jul. 2021].

Kleckova, A. (2021). *Russian State Terrorism Has Triggered the Biggest Fallout with the Czech Republic since 1989*. [online] The German Marshall

Fund of the United States. Available at: https://www.gmfus.org/blog/2021/04/26/russian-state-terrorism-has-triggered-biggest-fallout-czech-republic-1989 [Accessed 15 May 2021].

Knight, B. (2019). *Europe's Cybersecurity Gap Threatens Infrastructure, Elections | DW | 15.02.2019*. [online] DW.COM. Available at: <https://www.dw.com/en/europes-cybersecurity-gap-threatens-infrastructure-elections/a-47529189> [Accessed 14 November 2020].

Langenohl, A. (2020), "Articulating Sovereignty within the Infrastructural Imagination: The Case of the Securitisation of Finance as 'Critical Infrastructure'", *Politikon,* vol. 47, no. 1, pp. 4-23.

Lewis, T.G., Darken, R.P., Mackin, T. and Dudenhoeffer, D. (2012). Model-based risk analysis for critical infrastructures. *Critical Infrastructure Security*, 54, pp.3–19.

Lukáš, L. & Hromada, M. (2011), "Management of protection of Czech Republic critical infrastructure elements".

Lucke, R. (2016). 9/11 and Paris Compared: The Same Old Securitization Story? In: *Challenges in International Security*. ECPR General Conference.

Markopoulou, D. & Papakonstantinou, V. (2021), "The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular", *The computer law and security report,* vol. 41, pp. 105502.

Mattioli, R. & Levy-Bencheton, C. (2014). *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks,* ENISA, Heraklion.

Mauro, C.D., Bouchon, S., Logtmeijer, C., Pride, R.D., Hartung, T. & Nordvik, J.P. (2010). "A structured approach to identifying European critical infrastructures", *International journal of critical infrastructures,* vol. 6, no. 3, pp. 277.

Mendizabal, A.P., Holmes, J.S., Ortiz, N., Callenes, M. & Cardenas, A. (2021), "A hotspot analysis of critical hydrocarbons infrastructure in Colombia: ELN (Ejército de Liberación Nacional) and FARC (Fuerzas Armadas Revolucionarias de Colombia) attacks on Colombian pipelines", *Applied geography (Sevenoaks),* vol. 126, pp. 102376.

Maillet-Contoz, J. (2018). *Terrorism and Counterterrorism: French Policy after the 2015 Attacks*. [online] E-International Relations. Available at: https://www.e-ir.info/2018/12/07/terrorism-and-counterterrorism-french-policy-after-the-2015-attacks/ [Accessed 21 Mar. 2021].

Maurice, E. (2021). *Disinformation and electoral interferences: how European democracy protects itself*. [online] https://voxeurop.eu/en/. Available at: https://voxeurop.eu/en/disinformation-and-electoral-interferences-how-european-democracy-protects-itself/ [Accessed 23 Feb. 2021].

Mihaljević, B. (2018), "PROTECTION OF CRITICAL NATIONAL INFRASTRUCTURE: CHALLENGES FOR THE PRIVATE SECURITY SECTOR", *Annals of Disaster Risk Sciences : ADRS,* vol. 1., no. 1.

Mikac, R. and Cesarec, I. (2016). Critical Infrastructure Security and Resilience of the Republic of Croatia. *Center for Infrastructure Protection & Homeland Security, George Mason University*. [online] Available at: https://cip.gmu.edu/2016/08/18/critical-infrastructure-security-resilience-republic-croatia/ [Accessed 12 May 2021].

Ministerstvo Vnitra Ceske Republiky (2021). *Centre Against Terrorism and Hybrid Threats - Terorismus a měkké cíle*. [online] www.mvcr.cz. Available at: https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx [Accessed 3 Jun. 2021].

Mitrevska, M., Mileski, T. and Mikac, R. (2019). Critical Infrastructure: Concept and Security Challenges. *Friedrich Ebert Stiftung*.

Molina, J. (2018). Integrating risk management through data, analytics and infrastructure: Our perspective. *Grant Thornton*.

Moteff, J., Parfomak, P. & LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE (2004). *Critical Infrastructure and Key Assets: Definition and Identification*.

Mtibaa, A., Harras, K.A. & Alnuweiri, H. (2014), "Malicious attacks in Mobile Device Clouds: A data driven risk assessment", IEEE, pp. 1.

National Consortium for the Study of Terrorism and Responses to Terrorism (START) (2020). *The Global Terrorism Database (GTD)* [Data file], University of Maryland. Available at: https://www.start.umd.edu/gtd. [Accessed 08 November 2020].

National Consortium for the Study of Terrorism and Responses to Terrorism (START) (2019). "Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) Dataset." Available at: https://www.start.umd.edu/pubs/START_UWT_SignificantMultiDomainIncidentsAgainstCriticalInfrastructure_Dec2019.pdf. [Accessed 07 November 2020].

National Cyber Security Strategy. Skr. 2016/17:213 [online] Available at: https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213 [Accessed 10 May 2021].

NATO (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf [Accessed 21 Jul. 2021].

NATO (2021). *Strategic Concepts*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_56626.htm [Accessed 21 Jul. 2021].

Neal, A.W. (2009), "Securitization and Risk at the EU Border: The Origins of FRONTEX", *Journal of common market studies,* vol. 47, no. 2, pp. 333-356.

Niesen, T., Houy, C., Fettke, P. & Loos, P. (2016), "Towards an Integrative Big Data Analysis Framework for Data-Driven Risk Management in Industry 4.0", IEEE, pp. 5065.

Norell, M. (2005). Magnus Norell Swedish National Counter Terrorism Policy after nine eleven. *Swedish Defence Research Agency*, ISSN 1650-1942.

Novotny, P., Rehak, D., Markuci, J. and Almarzouqi, I. (2015). Proposal of Systems Approach to Critical Infrastructure Determination in European Union Countries. TRANSCOM 2015, 22-24 June 2015.

Official Gazette (2015), *THE NATIONAL CYBER SECURITY STRATEGY OF THE REPUBLIC OF CROATIA*.108/2015 [online] Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf [Accessed 5 Apr. 2021].

OSCE (2020). *Croatia, Parliamentary Elections: ODIHR Election Assessment Mission Final Report*. [online] Available at: https://www.osce.org/odihr/elections/465120 [Accessed 5 Mar. 2021].

Parhizkar, T., Hogenboom, S., Vinnem, J.E. & Utne, I.B. (2020), "Data driven approach to risk management and decision support for dynamic positioning systems", *Reliability engineering & system safety,* vol. 201, pp. 106964.

Paris Call (2018). *The call and the 9 principles — Paris Call*. [online] pariscall.international. Available at: https://pariscall.international/en/principles [Accessed 15 Feb. 2021].

Past, L. (2019). *European Elections Suggest U.S. Shouldn't Be Complacent in 2020*. [online] GovTech. Available at: https://www.govtech.com/security/european-elections-suggest-us-shouldnt-be-complacent-in-2020.html [Accessed 3 Jul. 2021].

Peresin, A. (2013). CROATIAN COUNTER-TERRORISM STRATEGY: CHALLENGES, PREVENTION AND RESPONSE SYSTEM. *RIEAS*. [online]

Available at: https://www.files.ethz.ch/isn/160221/rieas160.pdf [Accessed 12 May 2021].

Polisen (2021). *Terrorism awareness | The Swedish Police Authority*. [online] polisen.se. Available at: https://polisen.se/en/the-swedish-police/Raising-general-awareness-of-terrorism-related-issues/ [Accessed 21 Jun. 2021].

POLITICO (2018). *Is Europe Cyber Ready?*. [online] Available at: <https://www.politico.eu/event/is-europe-cyber-ready/> [Accessed 14 November 2020].

Poon, Y.X. and Basu, M. (2019). *Exclusive: France warns of "poisoned data" threat*. [online] GovInsider. Available at: https://govinsider.asia/connected-gov/france-guillaume-poupard-henri-verdier-cybersecurity-ambassador-digital-affairs-poisoned-data/ [Accessed 12 May 2021].

Privacy International (2019). *EU elections – protecting our data to protect us from manipulation*. [online] European Digital Rights (EDRi). Available at: https://edri.org/our-work/eu-elections-protecting-our-data-to-protect-us-from-manipulation/ [Accessed 13 May 2021].

Protective Security Act.1996:627 [online] Available at: http://www.notisum.se/rnp/document/?id=19960627.

Public Safety Canada (2020). *Critical Infrastructure*. [online] Publicsafety.gc.ca. Available at: <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx> [Accessed 23 November 2020].

G. Quijano, E., Ríos Insua, D. & Cano, J. 2018, "Critical networked infrastructure protection from adversaries", *Reliability engineering & system safety,* vol. 179, pp. 27-36.

Radware (2017). *Elections in France*. [online] radware.com. Available at: https://www.radware.com/security/ddos-threats-attacks/elections-in-france [Accessed 1 Jul. 2021].

Rashid, S. & Olofsson, A. (2021), "Worried in Sweden: the effects of terrorism abroad and news media at home on terror-related worry", *Journal of risk research,* vol. 24, no. 1, pp. 62-77.

RECIPE (2015). *Resilience of Critical Infrastructure Protection: Guidelines*. [online] Available at: https://ec.europa.eu/echo/sites/default/files/recipe_guidelines.pdf [Accessed 15 Mar. 2021].

Rehak, D., Hromada, M. & Novotny, P. (2016), "European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice", *Chemical engineering transactions,* vol. 48.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). (2019). Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj [Accessed 5 Dec. 2020].

Reuters (2017). Czech election websites hacked, vote unaffected -Statistics Office. *Reuters*. [online] 22 Oct. Available at: https://www.reuters.com/article/us-czech-election-cyber-idUSKBN1CR0RQ [Accessed 12 May 2021].

Romanova, A. (2020). *Where is cyber disarmament?* [online] The Security Distillery. Available at: https://thesecuritydistillery.org/all-articles/where-is-cyber-disarmament [Accessed 21 May 2020].

Rubio-Hervas, J., Gupta, A. & Ong, Y (2018), "Data-driven risk assessment and multicriteria optimization of UAV operations", *Aerospace science and technology,* vol. 77, pp. 510-523.

Sabor (2021), *The Republic of Croatia European Parliamentary Elections Act*.[online] Available at: https://www.sabor.hr/en/republic-croatia-european-parliamentary-elections-act [Accessed 1 Jul. 2021].

Sakerhetspolisen (2021). *Counter-terrorism - Säkerhetspolisen*. [online] www.sakerhetspolisen.se. Available at: https://www.sakerhetspolisen.se/en/swedish-security-service/counter-terrorism.html [Accessed 23 Jun. 2021].

dos Santos, P. & Tavares, A. (2015), "Basin Flood Risk Management: A Territorial Data-Driven Approach to Support Decision-Making", *Water (Basel),* vol. 7, no. 12, pp. 480-502.

Saragerova, B. (2020). *France: Towards stronger counter-terrorism regulation online*. [online] Global Risk Insights. Available at: https://globalriskinsights.com/2020/11/france-towards-stronger-counter-terrorism-regulation-online/.

Security Council Report (2019). *Protection of Civilians, May 2019 Monthly Forecast*. [online]. Available at: https://www.securitycouncilreport.org/monthly-forecast/2019-05/protection-of-civilians.php [Accessed 30 Jan. 2021].

Security Research (2020). *Policy Themes | Security Research*. [online] Securityresearch-cou.eu. Available at: <https://www.securityresearch-cou.eu/thethemes/Critical-infrastructure-protection> [Accessed 20 November 2020].

SGDN (2017). *The Critical Infrastructure Protection in France*. [online] Available at: http://www.sgdn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf [Accessed 15 Mar. 2021].

Simic, Z., Lugaric, L. & Krajcar, S. (2009), "Integrated approach to energy security and critical infrastructure in Croatia", IEEE, pp. 1.

Shapiro, J. & Suzan, B. (2003), "The French Experience of Counter-terrorism", *Survival (London),* vol. 45, no. 1, pp. 67-98.

SOA (2017), *THE REPUBLIC OF CROATIA NATIONAL SECURITY STRATEGY*.[online] Available at: https://www.soa.hr/files/file/National-Security-Strategy-2017.pdf [Accessed 3 May 2021].

van der Staak, S. (2017). *News | International IDEA*. [online] www.idea.int. Available at: https://www.idea.int/news-media/news/europe%E2%80%99s-upcoming-elections-cybersecurity-show-watch [Accessed 21 Jul. 2021].

van der Staak, S. (2021). *The weak link in election security: Europe's political parties*. [online] POLITICO. Available at: https://www.politico.eu/article/european-election-security-political-parties-cybersecurity/ [Accessed 15 Jun. 2021].

van der Staak, S. and Wolf, P. (2019). *Cybersecurity in Elections: Models of Interagency Collaboration*. International Institute for Democracy and Electoral Assistance.

Steiner, E. (2005). Legislating Against Terrorism – The French Approach. *Chatham House*.

STRATEGY OF THE CZECH REPUBLIC FOR THE FIGHT AGAINST TERRORISM from 2013 onwards, Ministerstvo Vnitra Ceske Republiky.

Swedish Civil Contingencies Agency (MSB) (2014). *Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure*. Available at: https://www.msb.se/RibData/Filer/pdf/27412.pdf [Accessed 15 Apr. 2021].

Tait, R. (2017). *Czech cyber-attack: Russia suspected of hacking diplomats' emails*. [online] the Guardian. Available at: https://www.theguardian.com/world/2017/jan/31/czech-cyber-attack-russia-suspected-of-hacking-diplomats-emails [Accessed 17 May 2021].

Tannam, E. (2017). *DDoS attack takes down two election websites in Czech Republic*. [online] Silicon Republic. Available at: https://www.siliconrepublic.com/enterprise/czech-election-ddos [Accessed 12 Jun. 2021].

Tannenwald, N. (2018). "How Strong Is the Nuclear Taboo Today?", *The Washington quarterly,* vol. 41, no. 3, pp. 89-109.

Tantawy, A., Abdelwahed, S., Erradi, A. & Shaban, K. (2020), "Model-based risk assessment for cyber physical systems security", *Computers & security,* vol. 96, pp. 101864.

Telecompaper (2019a). *Swedish government announces establishment of national cyber security centre in 2020*. [online] www.telecompaper.com. Available at: https://www.telecompaper.com/news/swedish-government-announces-establishment-of-national-cyber-security-centre-in-2020--1310211 [Accessed 3 Feb. 2021].

Telecompaper (2019b). *Swedish network attack simulation Telo 19 takes place*. [online] www.telecompaper.com. Available at: https://www.telecompaper.com/news/swedish-network-attack-simulation-telo-19-takes-place--1317228 [Accessed 1 Mar. 2021].

Telecompaper (2020). *Swedish govt earmarks SEK 440 mln for new national cyber-defence centre*. [online] www.telecompaper.com. Available at: https://www.telecompaper.com/news/swedish-govt-earmarks-sek-440-mln-for-new-national-cyber-defence-centre--1365250 [Accessed 1 Mar. 2021].

Theoharidou, M., Kotzanikolaou, P. & Gritzalis, D. (2009). *Risk-Based Criticality Analysis,* Springer Berlin Heidelberg, Berlin, Heidelberg.

Turner, C., Johnson, D. & Edward Elgar Publishing (2017), *Global infrastructure networks: the trans-national strategy and policy interface,* Edward Elgar Pub, Northampton, MA.

UNIDIR (2021a). *Czechia | UNIDIR Cyber Policy Portal*. [online] unidir.org. Available at: https://unidir.org/cpp/en/states/czechia [Accessed 30 Apr. 2021].

UNIDIR (2021b). *France | UNIDIR Cyber Policy Portal*. [online] unidir.org. Available at: https://unidir.org/cpp/en/states/france [Accessed 30 Apr. 2021].

UNITED STATES (2001). *The USA PATRIOT Act: preserving life and liberty: uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism*. [Washington, D.C.], [U.S. Dept. of Justice]. Available at: https://purl.fdlp.gov/GPO/LPS39935 [Accessed 25 November 2020].

UNODC (2021). *Counter-Terrorism Module 5 Key Issues: European Region*. [online] www.unodc.org. Available at: https://www.unodc.org/e4j/en/terrorism/module-5/key-issues/european-region.html [Accessed 5 May 2021].

U.S. Department of State (2019a). *Country Reports on Terrorism 2019: Croatia*. [online] United States Department of State. Available at: https://www.state.gov/reports/country-reports-on-terrorism-2019/ [Accessed 12 Mar. 2021].

U.S. Department of State (2019b). *France*. [online] United States Department of State. Available at: https://www.state.gov/reports/country-reports-on-terrorism-2019/france/ [Accessed 21 May 2021].

Varin, C., Abubakar, D. & SpringerLink (Online service) (2017), *Violent Non-State Actors in Africa: Terrorists, Rebels and Warlords,* Springer International Publishing, Cham.

Vašková, M. (2015), *Protection Of The Object Of The Critical Infrastructure In The Czech Republic*, Zenodo.

Vinocur, N. (2017). *France at risk of being next election hacking victim*. [online] POLITICO. Available at: https://www.politico.eu/article/cybersecurity-

hackers-france-at-risk-of-being-next-election-hacking-victim/ [Accessed 4 Mar. 2021].

Vitel, P. & Bliddal, H. (2015), "FRENCH CYBER SECURITY AND DEFENCE: AN OVERVIEW", *Information & Security,* vol. 32, no. 1, pp. 1.

Vlada Republike Hrvatske (2013), *ODLUKU O ODREĐIVANJU SEKTORA IZ KOJIH SREDIŠNJA TIJELA DRŽAVNE UPRAVE IDENTIFICIRAJU NACIONALNE KRITIČNE INFRASTRUKTURE TE LISTE REDOSLIJEDA SEKTORA KRITIČNIH INFRASTRUKTURA*.2411 [online] Available at: https://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html [Accessed 5 Mar. 2021].

Vukina, S. (2020). *The Law Reviews - The Privacy, Data Protection and Cybersecurity Law Review*. [online] thelawreviews.co.uk. Available at: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/croatia [Accessed 21 Jun. 2021].

Waever, O. (1996), "European Security Identities", *Journal of common market studies,* vol. 34, no. 1, pp. 103-132.

Walker, M. (2001), "Post 9/11: The European dimension", *World Policy Journal,* vol. 18, no. 4.

Westerberg, K., Broberg-Hansen, E., Sejergaard, L. & Nilsson, B. (2013), "Model-based risk analysis of coupled process steps", *Biotechnology and bioengineering,* vol. 110, no. 9, pp. 2462-2470.

Wilkinson, P. (2005). International Terrorism: the Changing Threat and the EU's Response. *Chaillot Paper*. [online] Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp084.pdf [Accessed 5 Mar. 2021].

Wilson, E. (2004), *Europe's 9/11*, Edinburgh University Press.

Woollacott, E. (2019). *Authorities in France tackling cyber-attacks on all fronts – ANSSI*. [online] The Daily Swig | Cybersecurity news and views. Available at: https://portswigger.net/daily-swig/authorities-in-france-tackling-cyber-attacks-on-all-fronts-anssi [Accessed 12 May 2021].

Xu, G., Qiu, X., Fang, M., Kou, X. & Yu, Y. (2019), "Data-driven operational risk analysis in E-Commerce Logistics", *Advanced engineering informatics,* vol. 40, pp. 29-35.

Zabyelina, Y. & Kustova, I. (2015), "Energy and conflict: Security outsourcing in the protection of critical energy infrastructures", *Cooperation and conflict,* vol. 50, no. 4, pp. 531-549.

Zakon o kritičnim infrastrukturama. 56/13 [online] Available at: https://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama [Accessed 3 May 2021].

Annex A – Regulation Timelines

The EU

Year/topic	CIP	Security/Defence	Terrorism	Cyber	Elections
2002			Council Framework Decision on Combatting terrorism		
2004			Communication on Critical Infrastructure Protection in the Fight against Terrorism		
2005	Green Paper on a European Programme for Critical Infrastructure Protection		The European Union Counter-Terrorism Strategy	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems	
2006	Communication on a European Programme for Critical Infrastructure Protection			Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment"	
2008	The 2008 Directive on the Identification and Designation of ECI				
2009				Commission adopted a Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and cyber disruptions: enhancing preparedness, security and resilience' setting out a plan (the 'CIIP action plan')	

2010				The Digital Agenda for Europe	
2011				Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'	
2012	Review of the 2008 Directive				
2013	The New CIP Framework			Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace	
2014				Methodologies for the identification of Critical Information Infrastructure assets and services	
2015		European Agenda on Security	Directive on Combatting terrorism	Guideline on Threats and Assets (CIIP)	
				Digital Single Market Strategy	
2016				Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry	Joint Communication and a Joint EU Framework for Countering Hybrid Threats (elections?)
					Report of the constitution committee of the European Parliament (AFCO) on 'potential and challenges of e-voting in the European Union
2017		Comprehensive Assessment of EU Security Policy	Directive on Combatting Terrorism	Communication by the European Commission (ICAS)	
2018					Compendium on Cybersecurity of Election Technology

					Code of Practice on Disinformation
					Recommendation on Election Cooperation Networks, Online Transparency, Protection against Cybersecurity Incidents and Fighting Disinformation Campaigns in the Context of Elections to the European Parliament
					Securing free and fair European elections
2019	The Green Paper on a European Programme for Critical Infrastructure Protection			Cybersecurity Act	
	Review of the 2008 Directive				
2020				Cybersecurity Strategy	The Action Plan for European Democracy

Alpine: France

Year/topic	CIP	Security/Defence	Terrorism	Cyber	Elections
2001			Internal security law on November 15th		
2004				Loi no 2004-575 pour la Confiance dans l'Economie Numerique	
2005			Anti-Terror Bill		
2008		The White Paper on Defence and National Security			
2011				The Information Systems, Defence and Security Strategy	
2013		White Paper: Defence and National Security		Military Programming Law	

				CIIP Framework	
2014	Instruction General Interministérielle Relative a la Sécurité des Activités d'Importance Vitale 6600			Classification Method and Key Measures: Cybersecurity for Industrial Control Systems	
				Cyber Defence Pact	
2015				French National Digital Security Strategy	
2017		Strategic Review of Defence and National Security		International Digital Strategy	
2018				French Security Act 2018-133 (transposition of the NIS Directive)	
				Strategic Review of Cyber Defence	
2019				The Military Programming Law 2019-2025	
				Cyber Defence Policy	
				Cyber Norm Initiative April 2019	

Baltic: Sweden

Year/topic	CIP	Security/Defence	Terrorism	Cyber	Elections
2003	The Civil Protection Act (2003:778)		The Act on Criminal Responsibility for Terrorist Offences (2003:148)		
2006	The Emergency Preparedness and Heightened Alert Ordinance - 2006:942			Regulation 2006:949 (Cybersecurity)	
2007			The Government Communication National responsibility and international commitment – A national strategy to meet the threat of terrorism (Govt. Comm. 2007/08:64)		

2009				The Swedish Civil Contingencies Agency's Regulations on Government Agencies' Information Security	
2010	The Installations Protection Act (2010:305)		The Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crime (2010:299)	The first National Cybersecurity Strategy	
2011	(March) MSB presented the National Strategy for the Protection of Vital Societal Functions		Responsibility and commitment – a national counter-terrorism strategy (Government Communication 2011/12:73)		
	(December) A functioning society in a changing world – The MSB's report on a unified national strategy for the protection of vital societal functions				
	(month) the Ordinance for the planning of the prioritization of vital societal electricity users (2011:931)				
	A guide to be implemented in 2014 to identifying VSF & CI and assessing acceptable downtime for VSF & CI (unclear report)				
2014	(July) The Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure		Government Communication 2014/15:146 Prevent, preempt and protect – the Swedish counter-terrorism strategy		

2015	The report on A new Protective Security Act (SOU 2015:25)		The Government Communication Actions to make the society more resilient to violent extremism (Communication 2014/15:144)	The report Cyber security in Sweden (SOU 2015:23)	
				A Strategy for Societal Information Security 2010-2015	
2016		Sweden's Defence Policy 2016 to 2020		A national cyber security strategy Skr. 2016/17:213	
				Cyber security for essential and digital services (SOU 2017:36)	
2017					Election infrastructure implicitly recognised as CI
2018	The Protective Security Act (2018:585)				
	The Protective Security Ordinance (2018:658)				
2019				(March) Comprehensive cyber security action plan 2019–2022	
2020	(March) The report Critical Nordic Flows – Collaboration between Finland, Norway, and Sweden on Security of Supply and Critical Infrastructure Protection				

Danube: Czech Republic

Year/topic	CIP	Security/Defence	Terrorism	Cyber	Elections
2000	The Crisis Act				
2002			National Action Plan to Combat Terrorism		

2003	The Committee for Civil and Emergency Planning material titled "Project Analysis of the principal functions of the state, including the protection of critical infrastructure in the event of emergencies"	The Security Strategy of Czech Republic			
2004	The Emergency Management Training Concept				
	Proposal of Protection Levels of the Information Systems Necessary for Functioning of the Critical Infrastructure in the Czech Republic				
2005	(July) The Strategy of Crisis Management in Transport Until 2013		The National Action Plan to Combat Terrorism 2005-2007	National Strategy of Information Security of the Czech Republic	
2007			The National Action Plan to Combat Terrorism 2007-2009		
2010	The Government Decree 432 on Criteria for (the) Identification and Designation of Critical Infrastructure Elements		The Czech Counter-Terrorism Strategy 2010-2012		
2011	Crisis Management Act	The Security Strategy of the Czech Republic			
2012				Strategy of the Czech Republic in the field of cybernetic security for 2012 – 2015	
2013	(January) Updated Information concerning the Implementation of the National Programme for the		The Strategy of the Czech Republic for the Fight Against Terrorism		

	Protection of Critical Infrastructure				
2014				Act on Cyber Security/ Cyber Security Strategy of the Czech Republic 2015-2020	
2015		The Security Strategy of the Czech Republic		Action Plan for the National Cyber Security Strategy 2015-2020	
		The Long-Term Perspective for Defence 2030			
2018				Cyber Defence Strategy of the Czech Republic 2018-2022	
2019				Report on the State of Cyber Security in the Czech Republic in 2019	
2021				National Cyber Security Strategy of the Czech Republic 2021-2025	

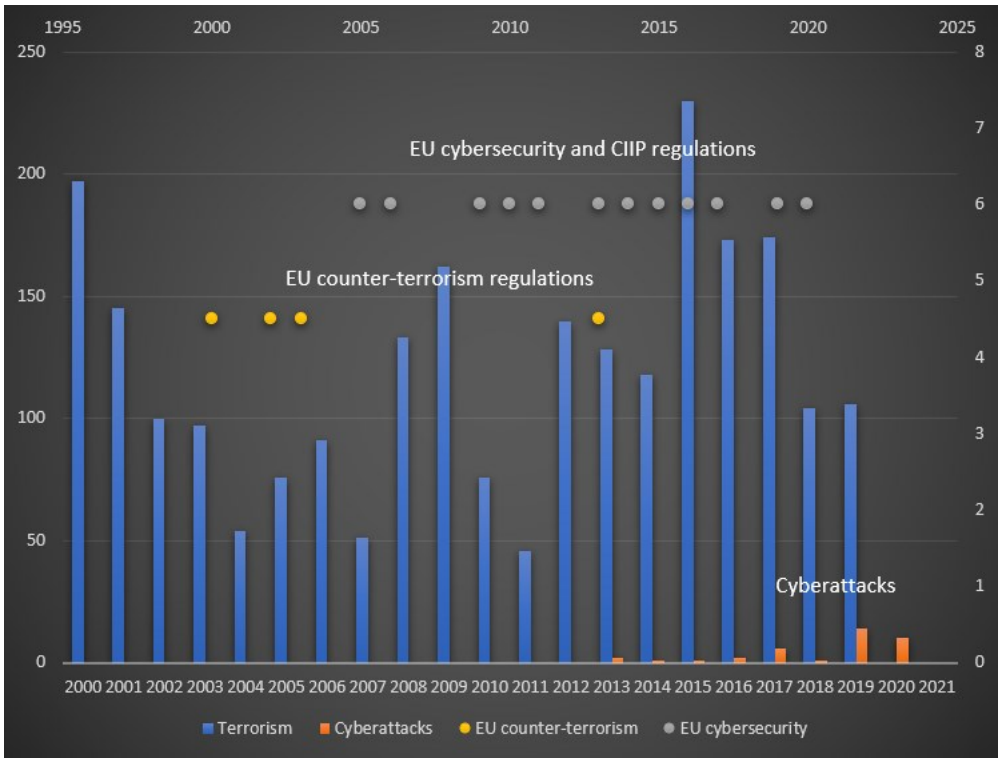
Adriatic/Ionian: Croatia

Year/topic	CIP	Security/Defence	Terrorism	Cyber	Elections
2002		The National Security Strategy			
2005				The National Information Security Program	
2006				The Security and Intelligence System Act	
2007				Information Security Act	
2008			The National Strategy for the Prevention and Countering of Terrorism	The Regulation on Information Security Measures	
				Rulebook on Standards of Organisation and	

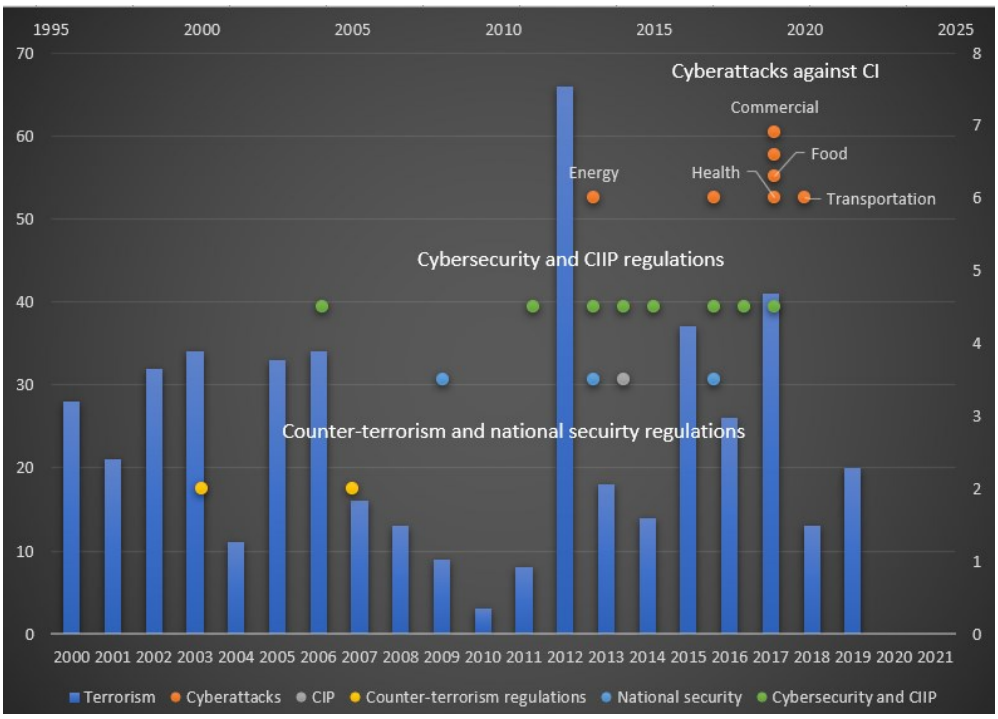
				Management of Information System Security Areas	
2009	Risk Assessment of the Croatian Natural and Technical and Technological Disasters and Major Accidents				
2010	Protection and Rescue Plan of the Republic of Croatia				
	Private Protection Act				
2013	The Critical Infrastructure Act				
	The Decision on designation the sectors from which the central state administrative bodies identify national critical infrastructure and lists of the order of the sectors of critical infrastructures				
	Rules on the methodology for drafting business risk analysis of critical infrastructure				
	The Ordinance on Risk Assessment Methodology for Critical Infrastructure Protection				
2014		The Croatian Armed Forces Long−Term Development Plan 2015−2024		Law on State Information Infrastructure	
2015			National Strategy for the Prevention and Suppression of Terrorism	The National Cyber Security Strategy of the Republic of Croatia and an Action Plan for its implementation	
				Regulation on Organisational and Technical Standards for	

				Connecting to the State Information Infrastructure	
2017		The Republic of Croatia National Security Strategy			
		Homeland Security System Act			
2018				Act on Cybersecurity of Operators of Essential Services and Digital Service Providers	
2019					The Republic of Croatia European Parliamentary Elections Act

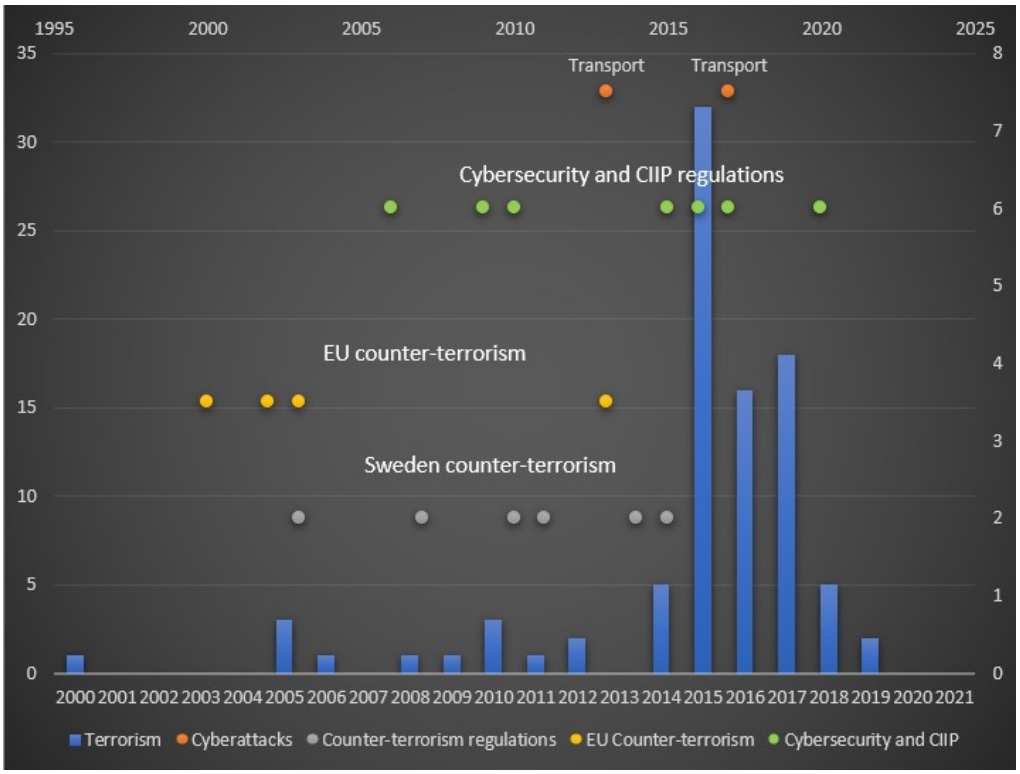
Annex B – Full-size regulations graphs



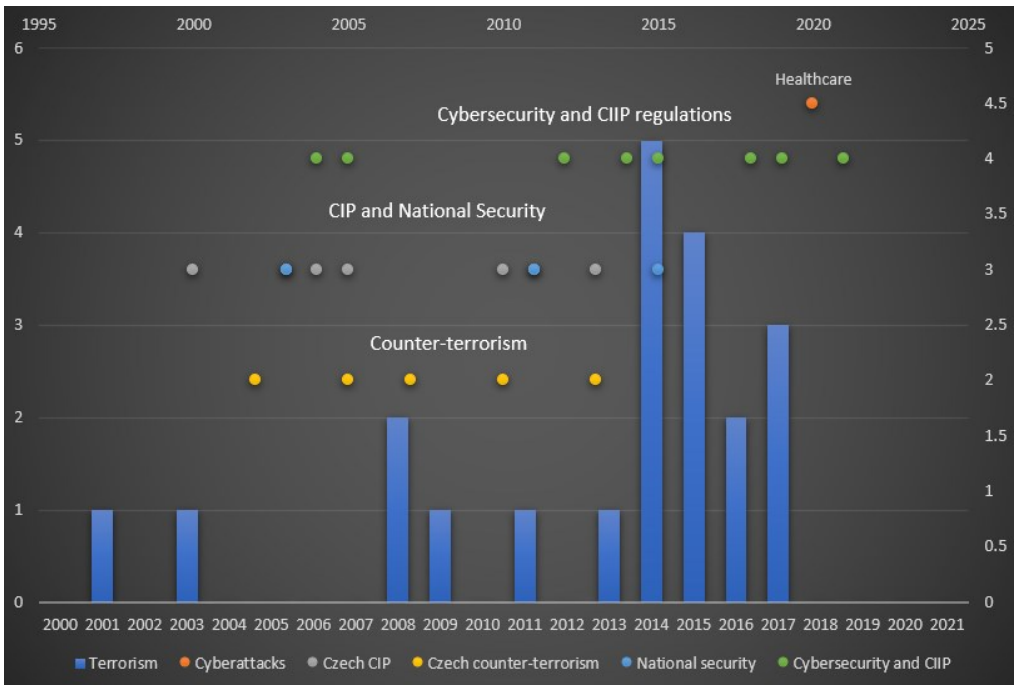
Graph 1. CIP Regulations in the EU



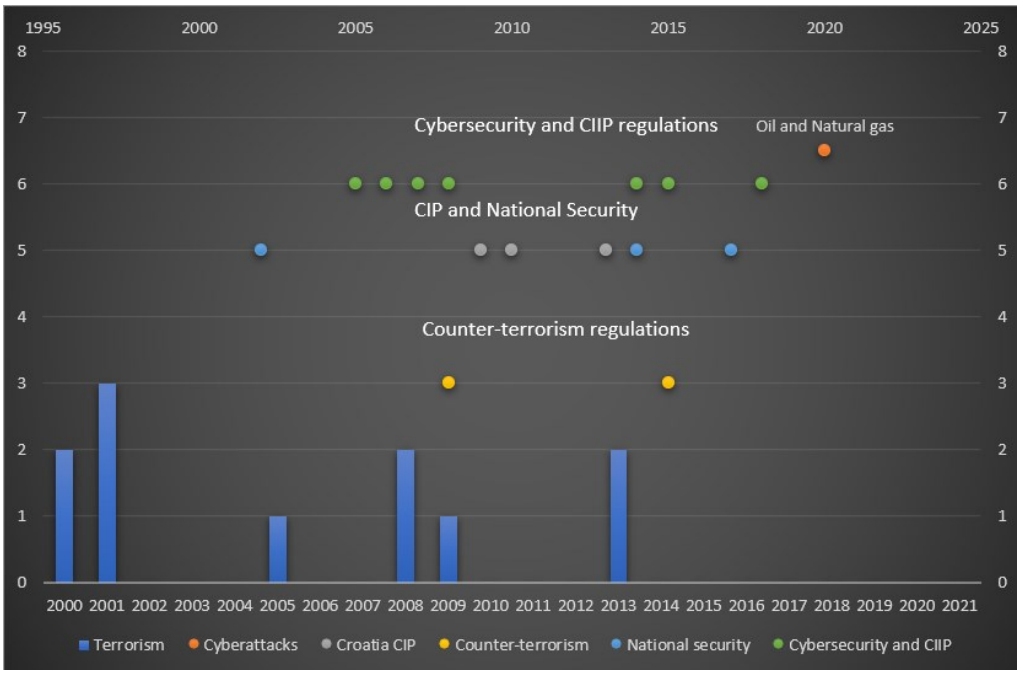
Graph 2. CIP Regulations in France



Graph 3. CIP Regulations in Sweden



Graph 4. CIP Regulations in the Czech Republic



Graph 5. CIP Regulations in Croatia