The cyber-transition of the electricity sector and V-4 energy cooperation

From pipeline politics to grid governance – finding the nexus between energy- and cybersecurity

Abstract

With our societies undergoing an energy transition which favours increased electrification over the use of fossil fuels, electric grid governance may in the future be of greater importance than traditional pipeline politics. Parallel to the energy transition, critical infrastructure is witnessing a process of digitalisation, opening up a range of new security threats as illustrated by the 2015 hack of the Ukrainian electricity grid. This research uses a socio-technical approach to highlight the relationship between technology and politics at the nexus of energy- and cybersecurity. By using the concept of imaginaries as an analytical framework, the effects of the cyber-transition in the electricity sector on V-4 energy cooperation are studied. Finally, this paper will argue that international political discourse surrounding the energy sector is still dominated by traditional energy security concerns, rather than incorporating newly emerging threats thereby emphasizing the role of politics over technology.

Submission Date: July 2019

Wordcount: 21.177

Supervisor: Dr. Eamonn Butler

Program: Security, Intelligence and Strategic Studies (IMSISS) 2017-2019

University of Glasgow	Dublin City University	Charles University Prague
2337955V	17116317	23550546

Contents

1. Introduction

A large share of energy security research and literature focuses on the gas and oil sectors, where the geopolitical dimension is prevalent. Electricity, on the other hand, is more 'fleeting', often taken for granted (EU, 2014). Yet, according to Szulecki and Kusznir (2017; 188) "the power [electricity] sector is arguably the most vital energy system in modern societies." To underline this point, they refer to the 1977 blackout in New York, which resulted in lawlessness, riots and mass looting. The disruptive potential of a loss of electricity in a modern society is enormous and affects emergency services, healthcare, heating/cooling, communications and so on. An effective regime to guarantee the stable functioning of the electric grid is crucial in guaranteeing societal and economic stability.

The electricity sectors of the Visegrád 4 countries (V4), Poland, Slovakia, the Czech Republic and Hungary, are facing several parallel challenges. Firstly, there is an increasing EU-led pressure to integrate, through processes of standardization and cross-country interconnections. The second development is the increasing integration of smart control systems in electricity structures. Such SMART systems (Self-Managing And Reliable Transmission (de Wilde, 2016) are often aimed at increasing efficiency and enabling the integration of 'irregular' production methods, such as intermittent renewable energy production. These systems create new opportunities for hackers. Smart control systems frequently work with Supervisory Control And Data Acquisition systems (SCADA) which are control mechanisms that are connected to the internet. This connection makes such systems easier to target, and therefore increases the risk that external actors gain control over the energy system. In other words: the smarter the grid, the more vulnerable it is (Jarmakiewicz et al., 2015, 2017; Fortinet, 2018). The third relevant development is that these beforementioned connections have more frequently been targeted in recent years by actors with malicious intentions. Considering the paramount importance of the stable functioning of the electricity grid and the need for international cooperation in achieving this, this research aims to distil the implications from cyber-related developments in the electricity sector on international political dynamics among the V-4 countries regarding energy governance. This study is guided by the central research question:

How do developments in the cyber dimension of the electricity sector influence V-4 energy policy and cooperation?

The overall objective of this research is to identify the effects of the so-called 'cyber-transition' on international political governance of the V4 electricity sector. By adopting the sociotechnical imaginaries approach as developed by Jasanoff and Kim (2009), this study acknowledges the impact of available technologies, and especially the physical infrastructure of those technologies, on the organization of social life. With this approach, this research aims to analyse how complex technologies actively influence social processes by setting the framework for possible imagined futures and thereby shape the range of available policy options. This analysis requires the assessment of three perspectives: the technical debate, the domestic energy policy debate and the international political energy governance debate. It is therefore uniquely fit to contribute to our understanding in two ways. The first is conceptually, by enhancing out understanding of the relationship between technology and politics. The second is empirically, by illuminating the specificities of cyber- and energy security concerns in the V4.

Firstly, the following chapter will provide an overview of the existing research in the field and define the scope of the cyber-transition within the electricity sector. Next, in chapter 3, the theoretical foundations of the socio-technical approach are set out. Chapter 4 will elaborate on the methodologies adopted. Then, in chapter 5, the technical debate regarding the cyber-transition is analysed, followed by an analysis of domestic energy policy debates, aimed at distilling the energy futures or 'national energy identities' preferred by domestic political elites in chapter 6 (Kuchler, 2018). These two elements, the technical debate and the respective national energy identities of the V4 countries, are then used as conceptual tools to analyse and illuminate processes in international political governance of the electricity sector in the face of the cyber-transition in chapter 7. Finally, this research will present the conclusion that despite the broadening risk profile of the electricity sector due to digitalization of grid management, cybersecurity considerations have not made their way on the political energy agenda. International cooperation in the energy sector within the V4 is still largely dominated by traditional energy security concepts such as affordability and availability within the gas and oil sectors. The electricity sector, besides a strongly shared desire to further develop nuclear energy capacity, plays a secondary role.

2. Literature Review

2.1 Visegrád 4 Cooperation

International cooperation in the Visegrád 4 (V4) has known significant changes in its internal dynamics since its official inception on 15 February 1991 (Visegrád Group, 2019). The states have been historically interconnected by shared traditions, similar cultures and comparable economic development (Střeleček et al., 2009; EU28 Survey, 2018). Interestingly enough, it used to have no formal organisational structures and did not have any funding up until 2000 when the International Visegrád Fund was established (Gyárfášová, 2016). Initial cooperation was centred around the pursuit of mutual objectives, the main ones of which were to join both NATO and the EU (Minarik, 2014). After the official accession to NATO in 1999 (with Slovakia lagging slightly behind by acceding in 2002) and their group entry into the EU as a part of the 2004 enlargement (Visegrád Group, 2019), the Visegrád Group gradually morphed into a flexible coalition group that could represent and amplify shared interests within the EU. Areas where the Group found common ground for cooperation include the eastern neighbourhood policy, agriculture, energy policy and digitalisation (Töró et al., 2013; Dostál and Végh, 2017).

Visegrád four member states are generally considered relatively inwards looking, valuing their internal relations significantly higher than outside relations (Dostál and Végh, 2017) but they unanimously point towards Germany as their largest cooperative partner on European policy matters outside of the V4 (EU28 Survey, 2018). This predominantly inward focus has been hailed as the ground for enabling and consolidating their integration into NATO and the EU as a group, but it is also considered a double-edged sword, hindering full integration within the European Community (Ghica, 2008). Additionally, some point towards the introduction of Qualified Majority Voting (QMV) in the Lisbon Treaty as further hindering this full integration. QMV is argued to allow for more robust decision-making, but also for causing a higher number of states of having their interests overruled. This is seen as stimulating a sense of disillusionment among member states and emphasizes the relevance of coalition-building, enhancing the power and relevance of the V4 as an institution (Nič, 2016). For outside relations the Group maintains the V4+ format: a flexible format where the relevant V4 representatives of state interests are joined by their respective colleagues from selected countries (Visegrád Group, 2019).

2.2 Energy Cooperation within V4

The energy sector provides a unique crossover of economic, geographical, political, environmental and social concerns. The debates surrounding energy governance address foreign relations, physical infrastructure, global warming and economic growth (Szőke, 2018). After the disintegration of the Soviet empire, the Visegrád 4 countries were endowed with an infrastructural legacy of this period. During the Soviet era, gas and oil pipelines had been set up to enable Moscow to individually leverage states by controlling their gas and oil supply. After the disintegration of the Soviet sphere of influence, Central and Eastern Europe wanted to prevent a newly emerged assertive Russia to use these supply lines to intimidate states (Stegen, 2011). Such a weaponization of energy supply is a strategy well acknowledged by NATO (2015, 2017a, 2017b) and academia alike (Ratsiborynska, 2018; Renz, 2016). During the process of EU accession, a dual strategy was initiated, aimed at both a diversification of energy sources and of energy suppliers (European Commission, 2014). The EU offers funding for infrastructure projects that work towards these aims. Early 2019 EU member states approved of an investment package of almost 800 million euros for the development of energy infrastructure projects, 97% of which will go to Central and South Eastern Europe (CEEP, 2019). Such grants have been indicated as a high priority for V4 officials and prove a fruitful area for cooperation (Dostál and Végh, 2017). However, the V4 group here feels constrained in initiating these projects by a sense of economic vulnerability. Whereas the Visegrád governments would prefer to stimulate internal interconnection first, European grants are often aimed at connecting the region with the rest of the EU community. V4 officials however fear that this will open up their markets against overwhelming competition – particularly from Germany (EU28 Survey, 2018).

Still, these diversification projects have reduced the ability of Russia to leverage their supply to certain countries individually. Because of increasing interconnections within the European market, Russia now has to leverage complex coalitions of states, complicating their geopolitical strategies. Nevertheless, ultimately the largest share of fossil fuel imports still comes from Russia (European Commission, 2014). Certain alternative sources are being explored or developed. The Romanian Black Sea gas is an example of a possible future source of diversification. However, the actual development of extraction capabilities is being held up by a political battle over tax laws (Gurzu, 2018). Another source of energy diversification comes from the LNG terminal in Swinoujscie, Poland. Poland has steadily been increasing the intake capacity of this terminal (Visegrád Group, 2019). Yet, LNG prices are simply not

competitive compared to Russian imports (Energy Charter Secretariat, 2014). This results in the situation that independence from Russian fossil fuel imports carries a monetary price. This became particularly evident during the height of the financial crisis, when European countries were once again looking towards Russia for cheap energy (Wen et al., 2012).

The dynamics of these pipeline politics have been extensively theorized in international relations literature as it provides analytically interesting geopolitical dilemmas (Mišík, 2012; Yergin, 1988; Proedrou, 2018). Either within Europe (Prontera 2017a, 2017b) or more specifically within Central and Eastern Europe (Minarik, 2014; Ostrowski and Butler, 2018) energy security in its broader sense continues to captivate academia. However, when considering the Energy Strategy proposed by the European Union, it can be argued that the future of the European energy mix will likely witness a significant shift towards the use of electricity. The EU Energy Roadmaps all point towards increased electrification of devices, decreased carbonisation, emission-free production and lower usage of fossil fuels (European Commission, 2012). This means that in the future pipeline politics may be of secondary relevance to grid governance.

2.3 The Undertheorized Electricity Sector

Due to increasing social pressure against the use of fossil fuels, technological innovation and a steady increase in renewable energy production, the share of renewable energy and electricity in the world's final energy consumption mix has increased, whereas the total share of petroleum products, solid fuels and gas has steadily decreased (European Commission, 2018). This is particularly impressive considering the massive growth in use of fossil fuels, which grew almost 37 percent over the period of 2000 to 2016. The use of renewable energy and electricity grew even faster with over 60% over the same period (International Energy Agency, 2019). EU member states have implicitly confirmed the increasing relevance of electricity by their approval of the latest investment package in European energy infrastructure projects; out of the 14 projects, nine were for electricity infrastructure (CEEP, 2019). If we assume that this trend continues, and there are currently no convincing signifiers to indicate a reverse in this trend, the electricity sector will become of increasing relevance to economic, social and political discussions, strengthened by the increasing efficiency of renewable energy production methods and social pressure on the phasing out of fossil fuels.

Despite these developments, electricity and grid governance are currently not as visible in public debates or high on the political agenda as one would expect. Discussions are usually held in technical circles and the first attempts towards establishing international electricity

connections were based on purely technological arguments (Lagendijk, 2018). Gradually, however, several developments have started to attract some academic attention towards (international) grid governance. One is the conception of the European Energy Union, stimulating an increasing interconnection of the electric grids throughout the European community (European Energy Union, 2019). The European Energy Union provides for an interesting institutional analysis by awarding energy a special status in the wider EU efforts to establish open and integrated markets (Lagendijk, 2018). Energy was long considered to be a 'natural monopoly' sector, but one of the pillars of the Energy Union was to break open the market for competition by separating production, transmission and distribution companies. Some researchers adopt a legal perspective in analysing the far-reaching consequences of the Third Energy Package (Roggenkamp et al., 2016; Talus, 2013) whereas others rather focus on the economics of electricity interconnections (Toritti, 2010; Silvast, 2017), but studies from a political or security perspective are difficult to find.

Some of the first studies that specifically focus on electricity governance regimes in Europe are provided by van der Vleuten and Lagendijk (2010a, 2010b) who studied European infrastructural vulnerability. Later they were followed by Puka and Szulecki (2014) and Bolton et al. (2016), who attempt to connect the wider policy goals and pragmatic constraints regarding the integration and international governance of the electricity grid. When reviewing the body of literature surrounding energy security it can be concluded that energy security as a concept is heavily theorized and researched, yet when we move towards the electricity sector, research suddenly becomes scarce. This is curious, considering that electricity plays no smaller role in our daily lives than oil and gas. Nevertheless, developments in the cyber-domain have brought back the attention of the security community to the vulnerability of the electric grid.

2.4 Cyber threats to Electricity Infrastructure

Another development worth noticing in this context is that of increasing malicious activity in the cyber domain. Cyberwar is arguably the new buzzword in the security community (Ducheine, 2016). The ability to conceal ones identity on the web makes cyber-tools very attractive for (state) actors in their strategic toolbox (Duyvesteyn, 2016). Cyberattacks can be globally disruptive as was the case during the 2017 Petya and Wannacry ransomware attacks, but can also cause severe physical damage, as witnessed in the use of Stuxnet in 2010. This piece of malware manipulated industrial control systems, causing severe damage to the Iranian centrifuges used to produce enriched uranium. This cyber-attack is an example of state-sponsored sabotage with far-reaching political consequences, where the US managed to disrupt

the Iranian nuclear programme. The cyber security of critical infrastructure is a subject grasping the imagination of many, conjuring doomsday scenario images of dams breaking and bridges collapsing (Maglaras et al., 2018). To an extent, there may be a foundation to these scenarios, as experts have speculated that cyber-attacks on critical infrastructure may increase exponentially in the years to come (Jay, 2017).

The vulnerabilities of the European electric grid have been amplified by the structural changes in its infrastructure. Several parallel developments are worth mentioning. Firstly, the 'breaking open' of the electricity market – as ordered by the Third Energy Package – has forced transmission operators to grant access to the grid to new producers. In the name of promoting competition, this has opened up the market for a proliferation of new connections and new energy producers (Roggenkamp et al., 2016). Secondly, the increasing competitiveness and promotion of renewable energy production methods has resulted in increasing bottom-up injections of electricity in the grid. Whereas traditionally energy was injected into the grid by large utility companies in an exclusively top-down direction, technological innovation has given rise to the concept of prosumers: consumers that also produce. In the case of overproduction of these individual solar panels, windmills or larger solar farms, electricity can be injected back into the grid, causing bottom-up energy streams (de Wilde et al., 2016).

Dealing with the increasing flows of energy in a multitude of directions places a larger burden on transmission operators, charged with balancing the grid. The expansion of decentralised renewable generation capacity requires enhanced information infrastructure to be integrated with the physical transmission infrastructure (WEC, 2016). To gather and process the relevant transmission data properly, transmission operators increasingly make use of Industry Control Systems (ICS) and more specifically Supervisory Control And Data Acquisition (SCADA) systems. Such SCADA systems communicate with central control centres over the internet. They send data about energy flows to the control centre, who sends back certain commands to execute (Jarmakiewicz, 2018). Such wireless communications are vulnerable to manipulation (Fortinet, 2017). Particularly advanced metering infrastructure containing two-way communication between the consumer and the utility provider have a relatively high vulnerability. Such communication systems can often be found in smart grids or smart grid devices. The World Energy Council even states that "the risk of potential attack surface grows with every device connected to the grid" (p. 36 WEC, 2016). In other words, there are an increasing amount of entry points for potential cyber intruders due to structural changes in the electricity grid. An additional complication is that many of the devices,

communication infrastructure or other services are outsourced to specialized providers. This complicates any complete value-chain assessment of cyber-security (EECSP, 2017). All of the above-mentioned developments ultimately contribute to an increased vulnerability of the electric grid to cyber-attacks.

For the purpose of this research, both the structural changes in the set-up of the grid (the integration of digital control systems in electricity infrastructure) and the increasing amount of malicious activity with either manipulative or destructive intent in the cyber-domain will be referred to as the cyber-transition. The scope of potential malicious activity will be limited to cyber-physical operational disruptions and will not include cyber-attacks such as data-breaches or espionage. Even though such data breaches are still considered to be data attacks and severe infringements of costumer privacy, not to mention the value that is gained in an age of big-data analytics (EECSP, 2017), such data theft is not considered within the scope of this research if it is not directly used with the intention of enacting damage on the operational working of the grid, for example by manipulating or destroying the data.

The vulnerabilities of the electric grid have not gone unnoticed and have been exploited during the Ukraine crisis. In December 2015 the Ukrainian grid was the victim of a cyber-attack where aggressors managed to temporarily disrupt Ukrainian electricity supply. The attack in 2015 was targeted at three separate distribution companies. Log-in credentials were stolen from grid operators through spear-phising attacks. These credentials were then used to grant the hackers access to the SCADA system. Subsequently, a modular type of malware was used to switch off about 30 substations, impacting approximately 225.000 customers (WEC, 2016; Cox, 2016a; 2016b). Even though the power was shut off for a couple of hours only, the malware had rewritten parts of the software on critical devices, leaving them unresponsive to remote commands. This led to certain stations having to be controlled manually for months after the hack. Not all systems have such a manual backup functionality – in a different setting this hack could have been much more disastrous (Zetter, 2016; NCCIC, 2016). The attack mainly affected households and a number of companies. Despite showing clear signs of preparation and coordination within the attack itself, digital forensics found proof of at least 6 months of preparations, the attack did not appear to be directly aligned with other types of attacks or events. However, analysts have noted that shutting down an electricity grid can be a large amplifying factor if integrated in a coordinated multi-pronged attack. It hampers communication technology, strains emergency services, disrupts economic flows and disturbs social order (NATO, 2016). In other words, the consequences of such a hack can be disastrous.

Technology companies and knowledge centres have realised the significance of these attacks and have published studies outlining SCADA and ICS risks (Fortinet, 2017) or have published their analyses with lessons learned concerning passive and active defences of electric grids (EISAC, 2016). But also industry expert platforms, such as the Energy Expert Cyber Security Platform have noticed the risk and published reports about cyber security in the energy sector (EECSP, 2017). Moreover, the trend has been picked up by policy-making institutions as can be witnessed by the Cyber Security Strategy for the Energy Sector publication of the European Parliament, who requested the study for the Industry, Research and Energy Committee (European Parliament, 2016). Yet, a comprehensive response from governments of international governmental institutions is not easily found. Whereas broader cyber security strategies have proliferated in the last couple of years, kicked off by the Estonians in 2008 after suffering severe attacks on their online infrastructure, these documents barely mention energy infrastructure. It is quite telling that in the 36 page document from the Estonians, energy is only mentioned three times and electricity only twice (Ministry of Defence of Estonia, 2008). Their latest Annual Cyber Security Assessment of 2018 does elaborate more on the energy sector (mentioning energy 15 times) but does not mention electricity at all (EISA, 2018). In reverse we see the exact same situations, energy strategies documents rarely discuss the cyber security of critical infrastructure. The Slovak Energy Policy does not mention cyber once (Slovak Ministry of Economy, 2016).

Within academia we can find some attention dedicated to the cyber security of the energy sector. Highly technical papers focus on the specific vulnerabilities of grid operating systems, elaborating for example on power generation systems (Xiang, Wang and Liu, 2017), control systems (Jarmakiewicz, 2018), sub-stations (Xiang, Wang and Zhang, 2018), or smart grids (Xie, Stefanov and Liu, 2016). What is missing, however, is a rigorous analysis bringing together technical and political perspectives. In the light of an increasingly interconnected European grid, an increased reliance on the electric grid to satisfy our daily energy consumption and an increased vulnerability of the supply infrastructure, there is a blatant gap between the work of political scientists focussing on the geopolitics of fossil fuels and the highly technical literature on the cybersecurity of the electricity sector. This research aims to address this gap by bringing together technical and political perspectives concerning the cyber-transition of the electricity grid within the Visegrád 4 group by using the socio-technical imaginaries approach. The V4 here provides an interesting case-study as an established international political sub-

entity which is part of both the EU and NATO and where the interconnectivity of the grid requires international policy responses.

2.5 Security and International Cooperation

Despite the V4 region not having suffered a massive coordinated cyberattack, such as Estonia, minor incidents do occur rather frequently. Targets include companies and media services but also systems of state administration (Visegrádinfo, 2018). Hungary scored the third-lowest value in the European Union in worrying about cyber-security, in addition to only 10% of small-and medium sized enterprises (SMEs) having addressed cyber security at all (European Commission, 2016). This is in spite of Hungary having held a top rank in in terms of cyber defence capabilities of NATO member states in 2015 (NATO, 2015). These indicators could imply that the private sector of the country is particularly vulnerable to cyber-attacks. With the increasing amount of SMEs involved in the technology and infrastructure managing the grid, this is even more concerning.

EU frameworks on cybersecurity have started to attempt to tackle these issues. The EU Directive on the security of Network and Information Systems (NIS), approved in 2016, came into force last year (NCSC, 2018). NIS requires the Member States to officially indicate their critical national infrastructure, set up Computer Security Incident Response Teams (CSIRT) and report any incidents to their EU colleagues. While the Directive has officially been implemented, no electricity infrastructure has been marked as critical national infrastructure. Cybersecurity remains a particularly complex area of international cooperation. Some countries consider cybersecurity to be a matter of homeland security, others of defence and some even of commerce (EUISS, 2017). For example, under the Orban government cyber defence became part of secret services, moving it away from public attention and becoming non-transparent (Visegrádinfo, 2018). Especially concerning security competences, governments are wary to delegate authority to supra- or international bodies, such as the EU or NATO.

Still, considering the cross-border nature and continuous integration of electricity structure, international cooperation is crucial in grid governance. Countries must balance their national interests versus international regulatory requirements, both in terms of energy policy and in terms of their cyber strategies. This intricate process is the centre of this research by analysing the effects of the cyber-transition on international electricity governance in the V4 countries. This requires an approach that manages to balance technical and political perspectives. The following chapter will set out how and why the socio-technical approach is the most appropriate theoretical framework to adopt in order to address this.

3. Socio-Technical Imaginaries

So far, the (cyber)security of the electric grid` seems to have received very little academic attention. Available literature is either highly technical (Jarmakiewicz, 2018; Sun, Han and Liu, 2018) or almost solely political (Vleuten & Lagendijk, 2010a and 2010b; Bolton et al., 2018). The overlap between technology and politics, and especially international politics, in the electricity sector is scarce and according to some, undertheorized (Jasanoff & Kim, 2009). In highly technical areas, there is a lot to be gained when studying the relationship between knowledge, its application and power. This research aims to bridge the gap in between the two areas and study the effects that technical 'realities' have on (international) governance.

An often-used approach when studying the energy sector, and mainly the oil and gas sectors, is securitisation theory. The argument is that political speech acts, if accepted by the relevant audience, have the potential to move political issues from the realm of low politics to the realm of extraordinary measures, bypassing standard procedures (Buzan et al., 2008). Yet according to Szulecki (2017) securitisation moves in the field of energy policy in the V4 countries are rarely ever successful. Moreover, its focus on political discourse does not allow for a proper focus on the technical specificities that are characteristic for the electricity sector and shape the debate surrounding cybersecurity. So, despite its insightful analytical value, this method seems inappropriate for the topic at hand.

An attractive alternative, preferred by Szulecki, might then be a related approach that calls itself riskification. The riskification approach focuses on the effect of the possibility of harm on governance. A successful act of riskification requires a precautionary measure resulting from a perceived potential source of harm (Corry, 2012; Szulecki, 2017). Even though cases of successful riskification in energy policy in the context of the Visegrád 4 countries are abundant (Szulecki, 2017), it focuses solely on perceptions and speech acts of politicians and mass media. It does again not allow for sufficient consideration of the highly technical nature of the electricity sector. What appears to be missing in both securitization and riskification approaches is room for a technological perspective and attention for the interaction between the technical and the political.

On the other side of the spectrum we find science and technology studies (STS), which studies innovation as an end in itself, somewhat paying attention towards the role of experts in technical decision making (Jasanoff 1995, Collins and Evans 2007). Other interesting phenomena, fleetingly treated by STS, are the role of the state in science and technology and

the resulting national technological 'identity' by asking questions such as: whose interests are served by investments in technology and what norms and values do national technological projects encode and enforce (Jasanoff 2005; Ezrahi 1990)?

Perhaps a compromise between the two ends of the spectrum and a more appropriate approach for this specific research can be found in the application of the concept sociotechnical imaginaries. It was coined in 2009 by Sheila Jasanoff and Sang-Hyun Kim as a response to the troublesome relationship between science and political power. Their approach acknowledges the impact of available technologies, and especially the infrastructure of those technologies, on the organization of social life. It highlights the capacity of inanimate things to actively influence social processes by setting the framework for possible imagined futures and thereby shaping the range of policy options. Research in this field focuses on the crossover between technical realities and social identities, which shape the socio-technical imaginary. This approach contains an outspoken constructivist perspective, by highlighting how technical and political influences jointly construct the final imaginary. Here, 'imaginaries' are defined as "collectively imagined forms of social life and social order reflected in the design and fulfillment of nation-specific scientific and/or technological projects" (Jasanoff and Kim, 2009, p. 120). An imaginary is, in essence, a though experiment – teasing the brain into conjuring up images that do not exist (yet). These images are constructed by ourselves and the socio-technical approach intents to deconstruct this image alongside a technical and a political analytical framework. The technical element is derived from the so-called material reality, and the political framework from proposed social identities.

Speaking of material realities raises certain ontological questions. Material or technological realities will, for the purposes of this research, refer to a widely-held consensus amongst scientific expert organisations. From this perspective, a proposed reality is not a suggestion of truth by the author, but rather a reference to a shared position or opinion held by technological experts on a certain topic. This perspective is an interpretation of the author. An elaboration on how this 'reality' is derived will follow in chapter 4. The social identity, on the other hand, more specifically refers to a preferred national energy identity. This identity reflects the dominant vision, or imagination, amongst a country's political elite of what a country's energy sector should look like. This refers not only to technological configurations such as infrastructure, but also to types of energy sources, import/export balance and to the preferred relationship between industry, government and costumer basis. All these elements carry certain norms and values that a country might wish to express. The decoupling of the energy sector

following the Third Energy Package can for example be interpreted as a measure aimed towards realising an imaginary where competition, the free market and liberalism are central features. The Dutch decision to scale down gas extraction in their northern provinces, blamed for causing local earthquakes, expresses a dominant imaginary where human-centred values such as safety and stability overpower those of economic gain (HCSS, 2018). Again, further elaboration on the construction of this identity will follow in the next chapter on methodology.

Working with sociotechnical imaginaries is a highly interpretive and constructivist exercise and builds on the assumption that our imagination is crucial in the development of policy (Jasanoff and Kim, 2009). In other words, we develop policy according to an imagined future that we wish to realize with the tools that we imagine to be at our disposal. This process provides a rich resource of insights in both individual minds and collective considerations as these are the core building blocks of such an imaginary. Analysing this construction of a collectively imagined future through public discourse then reveals its dominant values. Evident in the process of policy development as well as in the resulting policy itself, such imaginaries project certain norms and values and contribute to the development of systems of meaning.

The key to understanding the imaginary is then to deconstruct the elements that shape this scenario. The crucial aspect of the definition of a sociotechnical imaginary is 'collectively imagined'. This implies that at its core, an imaginary is a compound or aggregate socially constructed vision. Any analysis therefore needs to take a diverse range of perspectives into account (Levenda et al., 2018). The two central perspectives that will be studied are those of material realities and the preferred national energy identity. A historical analysis of the development of and interaction between the two can provide insights into construction of the wider socio-technical imaginary, illustrating the broader relationship between technology and (political) power.

Kuchler (2018) provides a very interesting example in studying the interaction between the two 'imaginaries'. He builds a very strong case in displaying how the existing energy infrastructure and expert discourse in Poland shapes and constrains possibilities in energy policy. He sets out how this 'material reality' viewed from the political perspective of the preferred 'national energy identity' forms a fundamental aspect in the development of energy policy (Kuchler, 2018; p. 121). Bolton et al. (2018) too emphasizes the important role of industry coordination bodies in sectors where certain infrastructure is 'inherited' with regards to understanding material realities. He argues that specific technological configurations limit future courses of action and thereby limit flexibility. In areas of rapidly developing technology,

such as the cyber-domain, this becomes even more complex. New innovative solutions in the management of the grid require new policy response.

Whether it is a specific type of change, innovation or general policy, there is always a process of change or transition involved. The development of policy indicates the desire to enact change or react to change in certain aspects of social organisation. When viewed from a technological perspective, this can for example refer to the political desire to respond to certain technological innovation. This can be to make use of new benefits that this technology offers or to counter any new threats that this technology may bring. Given the beforementioned power of technological realities to shape certain social processes, changes in technological realities in the form of innovation can demand a corresponding change in social processes (Geels, 2011). Subsequently, sociotechnical imaginaries are a very powerful tool or resource to create a perspective on societal or political responses to innovation (Jasanoff and Kim, 2013).

The transition or innovation that this study will focus on, consists of a set of developments. As discussed in the previous chapter, the electricity sectors in the V4 countries are facing rapid changes in the cyber-sphere. Not only are they experiencing changes in the structural set-up of the grid, grid operators are also witnessing increasing levels of hostile cyber-activities impeding their ability to carry out their tasks. These configurational and behavioural developments both take place in the cyber-domain and will therefore be referred to as the cyber-transition. This cyber-transition is the focal point and delineating element of this study. Both the technical realities and preferred national energy identity will be studied in as far as they relate and refer to the cyber-transition of the V4 electricity grids.

The sociotechnical imaginaries approach provides the conceptual tools and methods to delicately distinguish between cross-national variations in technical realities, national energy identities and the resulting sociotechnical imaginaries. Such a distinction and the interaction between said concepts can illuminate the implications of the cyber-transition within the electricity sector on V4 energy policy and energy cooperation. Having defined the relevant key terms with regards to the approach that this study will take, the next chapter will set out to operationalize said terms and elaborate on the methodology adopted in this research as well as the limitations inherent in this approach.

4. Methodology: Constructing the Imaginary

This section will elaborate on the sources used and methods adopted in this research. This research intends to use the socio-technical imaginary approach to develop an analytical lens through which to study developments in international governance. When constructing a socio-technical imaginary, two vital perspectives that need to be determined are the technical debate and the preferred national energy-identity debate. Whereas Tidwell and Tidwell (2018) emphasize the dominance of social values over the opinions of experts, thereby valuing the political perspective over the technical debate, Bolton et al. (2018) argues for a focus on industry bodies, placing the technical debate first. This research will discern both to determine their respective roles in shaping the final policy output and not pre-emptively leave either of the two out of the analysis so as to avoid a biased perspective.

The first step is then to analyse the technical debate surrounding cyber-developments in the V4 electricity sector to construct the dominant technical narrative on the cyber-transition. Such a dominant vision or imaginary can be distilled in several ways. This research will make use of a content analysis to construct this vision. Recurring linguistic markers or structures from different sources can signal a wide-held consensus, but this consensus can also be directly expressed in a shared communique from a coalition of experts. Sources that will be used for this analysis are: reports, statements, interviews and publications from industry-organizations, advisory boards, expert platforms, (technical) think tanks and academics that refer to the cyber-transition as defined in chapter 1. These sources can be directed at political bodies or at other technical organizations, but cannot originate from an organization with a primarily political purpose, instead of a primarily industry-oriented mission. This requires a strict screening of the publishing organization(s) and a sensitivity towards potential financing and/or commissioning structures. The publications used do not have to originate from one of the V4 countries directly, but do need to apply or refer to the V4 countries. This means that the sources used either have an EU-wide focus or a specific V4 focus.

After selecting the relevant documents according to the criteria set out above, these documents will be analysed on content in chronological order to uncover the development and construction of a dominant vision on the material reality concerning the cyber-transition of the electricity grids of the V-4 countries as put forward by technical experts. This technical reality directly describes the materialities of the electricity grid (accessibility, energy density, location, resources, resource quality, emissions, infrastructure quality (Kuchler, 2018) and the consequences of the cyber-transition on these factors (in terms of stability, security, efficiency,

etc.). The dominant vision is interpreted by the author based on recurring or widely supported elements within the breadth of the selected documents. Support can be expressed either by directly referring to (parts of) the content of other experts, or by proposing a similar vision independently. It should be noted that this final 'technical reality' is a product of the interpretation of the author and therefore potentially limited in its comprehension of highly technical aspects. However, since the majority of the documents is ultimately intended to inform policy and are therefore only moderately technical, this effect should be limited.

The second element constructing the final socio-technical imaginary is the preferred national energy identity. The next step is therefore an analysis of the wider national energy policy debates in order to uncover the dominant preferred national energy identity of the respective V4 countries by conducting a discourse analysis. A discourse analysis is integral to examining the values encapsulated in the language surrounding a nations' energy future. It requires a sensitivity to linguistic signifiers and structures that particularly resonate with the relevant audiences (Verloo, 2006). Linguistically focused approaches within discourse analysis include the assumption that most political phenomena are forms of text, either written or spoken. Discourse, from this perspective, is an expression of certain values by actively attaching meaning to certain practices. The analysis needs to find the right balance between scholarly rigor and linguistic sensitivity towards the subtle encapsulation of values whilst staying within the delineation of the topic at hand. However, considering that the topic is highly specific and does not provide for large data sets to allow for a more quantitative approach, methods such as the Gioia approach are excluded (Gioia et al., 2013).

Other potential approaches within in the ranks of discourse analysis include Critical Discourse Analysis (CDA). CDA argues for an approach to discourse analysis with a particular sensitivity towards power relations and dominance. Dominance is defined here as "the exercise of social power by elites, institutions or groups, that results in social inequality, including political, cultural, class, ethnic, racial and gender inequality" (pp. 249-250, van Dijk, 1993). Dominance is the key focal point from this perspective as it (re)produces certain power relations through different modes of discourse – structures, strategies or other characteristics of linguistic interaction. Cognitive power or control is one of the most essential categories as it can be the most effective. The ability to change the mind of others in one's own favour reduces or eradicates the need for the exercise of other types of power such as violence. Especially the cognitive power to successfully propose a dominant vision or more specific, a national energy identity is crucial in this study. Such an approach, with sensitivity towards dominance within

discursive performance, carries great potential when studying dynamics of power and knowledge, or politics and technology (Glynos et al., 2009; van Dijk, 1993, 1995).

Whereas a critical discourse analysis could shed an interesting light on structural inequalities and wider discourses of dominance, this is not the primary purpose of the analysis. If locating energy identities within wider structures of power and dominance had been the goal of this research, CDA might have been an appropriate choice. Here, on the other hand, the dominant energy identity is constructed as an analytical *tool*, with which to discern international governance structures, and not as an end in itself. Therefore, a textual discourse analysis with a Discourse Historical Approach (DHA) and including a sensitivity towards power and inequality structures is more appropriate. This analysis will be conducted with a specific macro level emphasis. A macro level emphasis is particularly useful in studying persisting structures across multiple texts (Lin, 2014). This implies a focus on intertextual and interdiscursive elements representing broader societal currents, rather than in-depth syntactic and rhetorical analysis.

Subsequently, a Discourse Historical Approach aims to analyse the processes of interaction between the subject and the actor suggesting a cognitive structure, in this case the proposed national energy identity. It highlights the need to consider social-psychological contexts of the relevant actors in the analytical process, including a sensitivity for memory and history. It calls for a delineation of the research area through a specification of (i) discourse; (ii) text; (iii) genre; and (iv) fields of action. More specifically, in the words of Glynos et al. (p. 20, 2009): "Discourses are instantiated inspecific texts, which are constitutive of and constituted by specific genres, which in turn are located within different fields of practices." [1] The study of V4 national energy identities will demarcate its sources within ways of talking about future scenarios of their country-specific energy sectors (discourses) as observed in political statements or publications from relevant actors (texts) proposing a belief system consisting of certain national values and a wider identity (genre) that are directed at enacting or promoting such a future scenario within the context of the cyber transition (fields of action) (van Dijk, 1993; Glynos at al., 2009; Wodak and Meyer, 2009). The wider national energy policy debate does not only refer to official parliamentary debates, but also to the wider societal debate located in the public sphere. More specifically, in this research sources amongst others include: primary

[1] An example: "Ways of talking about immigration (discourses) can be observed in government documents about immigration (texts) that can be taken to comprise a delimited set of linguistic practices (policy genre) within a broader socio-cultural field of action (such as a political campaign)." (Glynos et al. 2009, p. 20)

and secondary accounts of national policy debates, official V4 government statements in national or international contexts, media outlet statements, think tank publications, civil society organizations and other relevant academic publications.

The other side of the communication, then, is the acceptance or reproduction of said structures (van Dijk, 1993). Repetition and resonation are taken as a confirmation or acceptance of the discursive structure of such a proposed imaginary by the relevant audience. Identifying instances of such repetition and resonation are subsequently key factors in uncovering the dominant preferred national energy identity. These too need to be contextualized. This can be determined by the amount of 'traction' that certain terms gain in the public discussion. The final dominant national energy identity proposed is again an interpretation by the author of the most recurring and resonating values and preferences put forward by the wider public discourse surrounding the country's energy future. Levenda et al. (2018) hereby emphasize the importance that semantics play in distinguishing the values that speak from this debate; calls for energy independence can for example refer to a pride of domestic industries, a fear of dependence or a combination of both. In other words, it attempts to pin down representations of future societies through historically examining the formation process of such a belief system (Jasanoff, 2015).

The largest drawback in this section of the research is a linguistic barrier, limiting this study to English and German sources. Direct access to domestic discourse is limited from this approach. The selected case study group contains four different national languages, limiting virtually any researcher attempting to study all V4 countries in their native languages. The limitation to translated resources is severe, but will at the same time be perceived as serving as a natural threshold of relevance, assisting in the adoption of a macro-level analysis. Considering that the energy sector is an internationally interconnected sector, many top-level documents will be available in English. Next to that, with the ultimate research question in mind, that of researching international collaboration, it will support the delineation of this study in focusing on international collaboration in the energy sector as most international cooperation occurs in English. Nevertheless, it does limit the access of the author to a large share of relevant domestic discourse and it opens up a possibility for bias as international media platforms might not be fully representative of domestic discourse.

The third step of this research will use the concepts of technical realities and preferred national energy identities within the context of the cyber-transition as the primary perspective from which to analyse the international political governance on the electricity sectors of the V4

countries. To study the international political governance in the electricity sector, the following types of sources will be used: official V4 Presidency programmes and presidency reports, other official V4 statements, letters, non-papers and publications. This final element of the research will thus study the interaction between three elements: the cyber-transition, preferred national energy identities and international political governance in the electricity governance. The underlying assumption, according to the sociotechnical imaginaries approach, is that the first two are crucial components in the sense that the dynamic between the two is the constitutive component creating the latter. The analysis will make use of the content and structures distilled from chapter 3 and 4 as analytical tools to study the conduct of international cooperation within the V4 electricity sectors. This appears the most appropriate method to answer the research question: "How do developments in the cyber dimension of the electricity sector influence V4 energy policy and cooperation?"

Data from the period 2004-2018 will be collected. 2004 was chosen as this is the year of accession of the V4 countries into the EU. Even though it can be argued that in practice, integration in EU governance structures already took place in the years leading up to the official accession, the full participation of the V4 countries in EU governance processes only started after accession. Since international governance is the crucial element of this research and the EU is the single largest international actor involved in developing and implementing international governance in the electricity sector, 2004-2018 is the most appropriate temporal delineation of data collection for this study.

It has to be acknowledged that it is potentially problematic to separate technical sources from political sources. As van Dijk argues (1995, p. 13): "political discourse [includes] practices by all participants in the political process", hence including technical sources that act with a political purpose. Yet, in order to study dynamics between technological and political perspectives within the broader political process, this distinction has to be made to the best of the author's abilities. To be able to make this distinction, the study does have to adopt a more restrictive delineation of the political process with regards to establishing the dominant national energy identity. This distinction was elaborated upon earlier in this chapter by emphasizing the primary motivation of an actor – individual or organization. The final analysis, bringing the two perspectives together, will once again adopt a broader definition of the political process.

5. Technical Realities of the Cybertransition

In chapter 2, the technical or material reality, from hereon used interchangeably, was defined as a widely-held consensus amongst scientific expert organisations. This material reality is to be derived through a content analysis of statements and publications from expert platforms within the electricity sector within the limits of the cyber-transition. Subsequently, the sources used will be analysed – with a particular sensitivity for financing and commissioning structures – for recurring content or structures indicating the existence of a dominant technical imaginary concerning the cybertransition of the electric grid. A schematic overview of the findings can be found in Appendix I. The analysis is conducted alongside three main categories: (i) structural changes to the grid, (ii) changes in risk profile and (iii) required responses. Along these categories, this overview attempts to visualize instances of agreement amongst experts in order to uncover the dominant vision amongst experts on the technical reality concerning the cybertransition of the electric grid. This chapter will first discuss the content and context of the respective sources that are used and finally offer the analysis and the proposed technical imaginary. The purpose of this chapter is the construction of the technical imaginary, which is to be used as an analytical tool in chapter 7 to study international governance in the electricity sector. It will be used alongside the national energy identities, which will be discussed in the next chapter in order to discern the role of technology and politics in policy making.

5.1 Technical Discourse

The World Energy Perspectives, published in 2016 by the World Energy Council represents a broad coalition of companies and experts as it is the product of a collaboration between a network of experts from 40 countries, two transnational companies and the World Energy Council itself. As key takeaways, it refers to the cybertransition as having achieved immense gains in efficiency and reliability in exchange for an increased vulnerability. Cyber risk is characterized as a key operational risk. In the specific EU-context, it mentions the decoupling of production, transmission and distribution in the EU energy market to have increased competition, but also to have increased supply chain complexity, creating a need for effective cross-sectoral security and compliance cooperation. They draw particular attention towards the broad risk profile of cyber threats, as it ranges from economic espionage to service interruption through physical damage. They warn that increasingly modernised and automated equipment, characterized by interoperability, carries an increased exposure to cyber-attacks and requires an approach that goes beyond resilience (WEC, 2016).

A 2017 report from the Energy Expert Cyber Security Platform was requested by EU Directorate General Energy. DG Energy was collecting recommendations for the creation of an EU strategic energy framework. Nevertheless, the research was conducted independently and can therefore still be considered for this section of the research. The report has a distinguished focus on promoting customer rights, rather than promoting best industry practices. It offers a comprehensive overview of existing threats, strategic priority areas, existing legislation and recommended actions. Interestingly, the EECSP emphasizes the need for the establishment of a response framework and crisis management capacities. Both the WEC and EECSP point towards the need to develop more capacities, competences and knowledge and towards the need to foster more international collaboration. EECSP adds the involvement of international organizations to this recommendation, specifically the European Union Agency for Network and Information Security (ENISA), Europol and the European Defence Agency (EECSP, 2017).

The 2017 Kapersky Lab report on the cybersecurity of the electricity sector is a rather technical document setting out technical risks and technical solutions. It does not elaborate on national measures or international cooperation of any kind but takes an isolated industry-centred approach. Kapersky warns for the general openness in communication lines between power infrastructure facilities and illustrates a number of key weaknesses of digital control systems. The report mostly refers to poor staff awareness of cybersecurity ("cyber-hygiene"), observed through insufficient security protocols or software updating practices. The solutions that are set out include automated security systems, antivirus software and suggestions for security protocols (Kapersky lab, 2017).

The Kosciuszko Institute, a non-governmental research institute, published a comprehensive report on the cybersecurity of the Polish energy sector. Considering that this report also refers to V4 and EU-wide developments within the electricity sector, this report is still considered relevant for this research. It touches on issues ranging from the influence of artificial intelligence to advanced metering infrastructure and contains articles developed in close cooperation with industry organizations. The report distinguishes systematically between information technology and operational technology and argues that certain security policies for one category do not always prove sufficient for the other. It also emphasizes that some countries are better prepared for cyberattacks than others, pointing towards the cross-border dimension of the weakest link problem (Kosciuszko Institute, 2017).

The Council of European Energy Regulators (CEER), as an independent industry platform organization, has presented its 2018 report on the cybersecurity of Europe's Electricity and Gas Sectors with the purpose of informing EU policy development. The report is published in the midst of the implementation period of the EU Directive on Security of Network and Information Systems (NIS) and heavily refers back to the 2017 EECSP report in setting out challenges to the energy sector. It provides a regulatory overview and includes topics as sustainability, big data and cloud computing. Amongst others, it discusses the influence of the General Data Protection Regulation (GDPR) and Clean Energy Packages throughout the energy value chain (CEER, 2018).

The European Technology & Innovation Platform Smart Networks for Energy Transition (ETIP-SNET) is a platform organisation bringing together stakeholders in the energy sector. It published a technical position paper on the digitalization of the energy system with the purpose of supporting the wider energy transition, in which one section solely specifies on cybersecurity and resilience (ETIP, 2018). Much like the Kosciuszko Institute it distinguishes between operational technology and information technology, but does not necessarily continue this line when discussing risk profiles. Rather than going into specific cybersecurity related challenges, it argues for cybersecurity and interoperability to be considered early in the design stages of any element of energy infrastructure and calls for appropriate funding to realise such efforts.

On request of the European Economic and Social Committee, the Hague Centre for Strategic Studies has developed a report on cybersecurity of the private sector across Europe. It provides a comprehensive cross-sectoral report with frequent attention towards the electricity sector and particular emphasis towards methods of increasing awareness and skills training. It highlights the energy sector as one which has been familiar with cyber threats for a longer period of time and therefore as a source of best practices for other sectors. Interestingly, they point towards sector-specific networked models of cooperation enabling effective information sharing set within a wider national hub-and-spoke model. Such networks, they argue, hold a strong potential to also facilitate the implementation of educational activities. The state, in this model, holds a special role as coordinator of this model, linking it to international structures (HCSS, 2019).

The next sections will elaborate on the recurring elements discussed by the beforementioned sources on the cyber-transition of the electricity grid in terms of structural changes, changes in risk profile and required responses. A precise overview of this can be found

in Appendix I. The measure of agreement – or lack of agreement – will be contextualized in the respective subsections after which the final dominant technical reality as interpreted by the author is proposed.

5.2 Structural Changes

The first element that all sources agree on unanimously is that the European electric grid has witnessed an **increased digitisation of grid management**. This digitisation takes place on all levels of infrastructure, in production, transmission and distribution. This takes the form of an increased installation of physical and electronic sensing systems. These systems send data back to centralized control centres, which in turn process this information and send back decisions, information or other commands. This communication of data and commands often goes through Industrial Control Systems (ICS), which encompass Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are particularly well suited for this combination of data processing and the execution of commands. Such systems have been linked to increases in efficiency, optimising the production-consumption balance and enabling quick identification of potentially problematic structures in the system. Nearly all sources (six out of seven) also particularly point towards this **increase in communication** in terms of a dramatic increase of data flow. A bit more than half of the sources (four out of seven) also mention the **installation of automatic demand response programmes**. These are programmes that have the capability to independently process data and decide on necessary actions based on this analysis, hence limiting the need for any human interaction with the system to oversight functions. Such systems often already make use of artificial intelligence in their operations.

Another element that all sources agree on, is that these dataflows and control systems have enabled **increasingly integrated and interoperable systems**. Especially remote controlled ICS allow for a centralized control centre to manage an increasingly large system. Interestingly enough, the decoupling of the European Energy system has not resulted in a operationally fragmented system – as was feared by some – but due to the technological innovation, increases in data flows and institutional cooperation the European grid is more considered more connected than ever (HCSS, 2019). This is happening in spite of a **diversification of equipment and technology**, as indicated by six out of seven sources. They point towards the increased installation of new types of control systems and the rapid development of technology used in, for example, smart grids or advanced metering infrastructure. At the same time, this development points towards a **decentralized supply chain**, again indicated by six out of seven sources. The high number of different systems

involved in grid management and the high level of specialization involved in their respective operating systems requires a highly specialized technological industry. Subsequently, the complete energy value chain now involves many different actors. Due to the outsourcing of highly specialized technology and in terms of the decoupled operating systems a larger number of companies, individuals and other organizations are now involved in the sector.

5.3 Changes in Risk Profile

The structural changes in the European electricity grid have, besides overwhelming gains in efficiency and oversight, led to a changing risk landscape. Experts point towards a wide range of either new risks or existing risks with increased relevance within the context of the cyber-transition. The one risk that all expert platforms agree on relates heavily to the increased digitisation and increase in data flows and is a highly typical concern for this decade: **breaches in customer data privacy**. EECSP (2017) and ETIP (2018) emphasize that especially in the implementation period of the General Data Protection Regulation (GDPR) and the Directive on security of Network and Information Systems (NIS), both companies and end-users are highly concerned with the increase in data available on individual users and specifically the way this data is stored, used, shared and protected. Companies or other entities involved in using this data have a dual concern, not only for the privacy of their customers per se, but also in terms of compliance and the risk that is inherent in their operations.

A related risk that was indicated by a large majority of technical platforms is that of **data corruption** and **economic espionage**. Both can occur when an individual gains unauthorized access to data or makes unauthorized use of this data. This can occur when an outsider manages to infiltrate data sets and either steals, manipulates or deletes this data, but it can also occur when an insider with malicious intent misuses access credentials. This risk is not specifically new to the energy industry, but does have renewed importance within the cybertransition for two main reasons: firstly, the increase in available data has increased the relevance and value of this data and secondly, new information and communication technology, often dependent on the internet and wireless communication structures to allow for the increase of data flows, has enlarged the vulnerability of data in the cyber-sphere.

According to a (small) majority of the sources, increases in connected devices, communication structures and data flows have created a significant **increase in entry points for potential breaches**. The proliferation of physical devices, the Internet of Things, and digital structures connected to and involved with grid management have increased the risk of users gaining unauthorized access to critical operational processes. ETIP (2018) provides an elaborate

overview of the multitude of options that a hacker has at its disposal to either interrupt or manipulate or spy on data flows or control systems. The increase in entry points for potential breaches also functions as an amplifier for other risks, such as the **loss of control of key equipment** and **software corruption,** both were mentioned by a significant majority of sources as key risks. Software corruption is considered as a risk with increased relevance in the light of the installation of automated demand response programmes. A hacker manages to gain access and alter the code of control programmes, such discrepancies in demand responses can ultimate lead to energy supply disruptions but also to physical damage to appliances or infrastructure.

Finally, a risk almost unanimously indicated by technical experts is one that flows out of the decentralization and diversification in the supply chain in terms of equipment and technology. They argue that the high level of technological specialization and an increasing level of outsourcing in both services and technology has gradually led to a loss of understanding from the engineers that are ultimately responsible for operations. Another aspect of this issue is that certain pieces of software are not transparent or cannot be edited – this results in the situation that engineers are potentially not able to execute critical updates or changes in crisis situations. Ultimately this culminates in a **loss of control and understanding of the critical technology and equipment** used.

Next to the abovementioned changes in risk profile that were acknowledged by a majority of technical platforms, there are a number of interesting phenomena which were not widely supported. These will not form part of the final technical reality, as they do not represent a consensus within the technical elite, but some are still worth mentioning. One of those is found in the WEC report, which warns for 'monoculture risk' (p. 27, WEC, 2016). This occurs when systems across multiple levels of infrastructure rely on one type of software. If a hacker has managed to identify a weak element of this software and can infiltrate one system, he can now gain control of multiple systems at the same time by making use of that same weakness. It can therefore be argued to function as a risk amplifier. CEER (2018) specifically refers back to the WEB 2016 report to agree with the basic principles of monoculture risk, but does argue that it is slightly oversimplified. They argue that certain elements of the grid can be disconnected and operate in isolation, hence limiting the impact of a potential disruption.

The EECSP report (2017) introduces the weakest link problem, arguably a variation on the monoculture risk identified by WEC. The weakest link problem refers to the cross-border impact resulting from a single disruption in an interconnected system. The 2006 European blackout is an example of this phenomenon, where powerline disruptions in Germany impacted

electricity systems from Poland, France and the Benelux countries into Portugal, Spain and Morocco. The weakest link problem is different from monoculture risk, as monoculture refers to different systems adopting the same type of software. Subsequently, if a hacker discovers a weakness in one system, other systems with the same software are bound to have the same weaknesses, amplifying the reach of a hacker but requiring multiple attacks to make use of these weaknesses. The weakest link problem refers to one single attack that due to the interconnectedness of the system has a larger impact.

Interestingly, ETIP proposes a concept that is the reverse of the monoculture problem called "herd immunity". This refers to the adoption of similar structures of software across the industry that contain trusted measures of cybersecurity and information security management, leading to group security (ETIP, 2018). Such herd immunity is then the envisioned result of (EU-wide) cooperation, information sharing and standard and protocol setting. Again, since the reports do not seem to form a meaningful consensus on the concepts of monoculture risk, the weakest link problem of herd immunity, these will not be included in the final technical reality.

5.4 Required Responses

At the centre of all recommendations is the **stimulation of a risk awareness culture**, unanimously mentioned across all sources. Some emphasize the development of such a culture on the operational level, such as Kapersky (2017), whereas other emphasize top-level awareness programmes (EECSP, 2017) but the core argument is the same; many vulnerabilities result from poor 'cyber hygiene': poor password management, breaches of security protocols and connecting unauthorized devices to operational systems. 90% of hacks are initiated with simple spear-phishing attacks and even air-gapped systems are not immune to human error (ETIP, 2018). Training both employees and top level management on standard security protocols is argued to deliver large gains in terms of cybersecurity.

A second approach, argued for by all sources but one, is the **implementation of (international) standards and regulations**. Especially in a highly interconnected system with many different operators involved, adhering to a similar level of security standards is considered very relevant. Considering the cross-border nature of electricity infrastructure, **international cooperation** is also emphasized across a majority of the sources. An international approach is also considered necessary in setting up systems of **information sharing**, **setting up a response framework** and facilitating **knowledge and skill building** by a majority of the sources. When discussing information sharing platforms, levels of security and trust are highly emphasized as operators can share their vulnerabilities here to help other operators avoid or diminish these

vulnerabilities, but this information is highly classified and requires the appropriate, secure communication channels (EECSP, 2017).

One interesting proposal which did not manage to garner broad support amongst technical elites, is the promotion of value chain security coordination. Due to the decentralized nature of the decoupled value chain in the energy sector, some experts argue that coordination in terms of security standards along the entire value chain would be of high value. However, there does not appear to be a strong consensus on this proposal.

5.5 Dominant Technical Reality

A content analysis of publications by expert platforms has enabled the uncovering of a dominant vision on the material reality on the cybertransition of the (Central) European electricity grid. This material reality is constructed alongside three main pillars: structural changes, changes in risk profile and required responses. Concerning structural changes, expert platforms overwhelmingly agree that the cybertransition contains an increased digitisation of grid management and increasingly integrated and interoperable systems. Next to that we can witness the development of decentralized (remote) supply chains with more diversification in equipment and technology, enabling an increasing amount of communication and data flows. A small majority of the sources also points towards the installation of automated demand response programmes.

Regarding the risk profile of the industry, experts unanimously point towards the increased risk in customer data privacy breaches. To a lesser extent they indicate the increased relevance of economic espionage, data and software corruption and a loss of control and understanding of key equipment. A smaller majority also points towards an increase in entry points for breaches. Finally, in terms of required responses, technical platforms emphasize the need to stimulate risk awareness cultures throughout the layers of the industry. Next to that they also call for international cooperation in the development and implementation of standards and regulations, knowledge and skill building programmes, (risk) information sharing platforms and to a lesser extent also setting up a response framework.

6. V4 National Energy Identities

This chapter will set out to derive the discursively dominant national energy identities within the respective V4 countries through conducting a discourse analysis with a Discourse Historical Approach (DHA). The analysis will search for recurring language and structures and other representations used to describe possible future scenarios of the energy sector and historically examine the formation process of such a belief system. Of particular relevance for this analysis is the social context of the relevant actor – such as location, platform or the capacity in which the actor is speaking – and a sensitivity for memory and history. Each section will therefore start with setting out the historical context of the development national energy policy after which the contemporary discourse is analysed and discussed in order to discern the preferred national energy identity. The final proposed national energy identities will be used in the next chapter as an analytical framework through which to approach international energy governance in the V4. They will enable the distinction of specific national interests pushed forward in international governance.

6.1 Czech Republic

Post-Soviet Czechoslovakia was heavily endowed with an infrastructural legacy from the Soviet era. Gas and oil pipelines – often with only one-directional flow capacity – still connected the area with Russia. After the 1989 collapse of communism, Czechoslovakia sought to diversify both its supply sources and infrastructure. Pipelines were updated with the option to facilitate two-directional flows. After the 1993 peaceful disintegration into the Czech Republic and Slovakia, the Czech Republic continued to push for privatisation, mainly amongst small and medium enterprises. However, both privatisation and diversification efforts were met with only moderate successes. Despite having a small amount of natural resources, brown coal and uranium, the Czech Republic imported nearly the entirety of its gas and oil needs from abroad. Two thirds of its natural gas imports came from Russia and the remainder was complemented by Norwegian gas supplies. Around 60% of its oil supplies also came from Russia, with the remainder being supplied by Azerbaijan and Kazakhstan (Energy Union, 2015). Regarding privatisation, in spite of pressure from the EU and the legal decoupling of the market, the Czech government managed to retain a sense of strategic ownership within the sector. One of the most prominent examples of this strategic ownership is that of CEZ, which is one of Europe's major electricity providers, where the Czech government managed to retain control over major subsidiaries (Deloitte, 2015; Ostrowski and Butler, 2018).

Countering the pressure towards further electrification were the recurring Russo-Ukraine gas crises at the start of the 21st century, which led to an increased focus on the relevance of non-renewables and more specifically on the gas buffer. Supply disruptions to Ukraine were felt throughout Europe and drew attention to the sensitivity of the role of Ukraine as a transit country. The Czech Republic managed to display a high level of solidarity during this crisis. Due to the exceptionally high level of interconnectedness of their gas supply infrastructure they were able to help out neighbouring countries and the Ukraine during the crisis with their gas reserves. The situation also led to an emphasis on the need to further diversify supply infrastructure and an increased awareness of the relevance of alternative energy sources - most specifically nuclear energy (Ministry of Industry and Trade, 2012; 2014). With six nuclear reactors spread through the country, nuclear power currently accounts for roughly 20% of the Czech electricity mix, coal for about 60 % and renewables for the remaining 20% (Worlddata, 2015). According to national energy strategies, nuclear energy is intended to deliver up to 50% of all electricity in 2040 (Ministry of Industry and Trade, 2014).

In a public speech in 2014, Prime Minister Sobotka emphasized that the V4 countries have shared interests and built a case for cooperation within the development of north-south energy corridors. Energy diversification, both in supply infrastructure and in energy mix, were mentioned as key uniting elements (Vláda Cˇeské republiky 2014). Here, diversification does not necessarily refer to self-sufficiency but rather to avoiding an overwhelming reliance on one single supplier – or transit route. Hence, he expressed an interest in diversifying dependence rather than actively developing independence.

Later, in public comments in 2017 Prime Minister Sobotka specified that nuclear energy here would prove to be the key to both diversification and achieving climate commitments by replacing the large share of coal in the electricity generation, directly tying into the energy security debate (Euractiv, 2017). This emphasis came in the wake of the elaborate 140-page strategic document of the Ministry of Industry and Trade setting out a National Action Plan for the Development of the Nuclear Energy Sector in the Czech Republic (Ministry of Industry and Trade, 2017). Czech special ambassador for Energy, Vaclav Bartuska argued later that the Czech Republic might need 8 to 10 new nuclear reactors to phase out the large share of coal in electricity production. Nuclear energy is referred to as ‘vital’ and ‘irreplaceable’ in the Czech path to a cleaner and more diversified energy future. With reference to renewable energy sources, he remains ambivalent and argues that their impact will largely depend on the performance of new technologies and the development of economically viable electricity

storage capacity (Schuster, 2018). So whereas nuclear energy is assigned a clearly established and unquestioned role in the future of the Czech energy mix, renewable energy sources are considered more unpredictable.

The role of renewable energy sources remains fairly undefined within the wider discourse. The legal uncertainty of certification of renewable energy producers and the allocation of feed-in tariffs have led to higher priced electricity, which in turn has reduced the popularity of renewables for the public. This uncertainty is argued, both by industry confederations and former Minister of Industry and Trade Ian Mladek, to hurt the sector, as continuity and stability are crucial in ensuring long-term investment cycles (Euractiv, 2016). An Energy Union report also notes the stagnation of renewable energy development and point towards changes in the renewables support schemes (Energy Union, 2015). The Czech Communist MEP Kateřina Konečná even goes as far as to blame subsidies for renewables for distorting the market and damaging the prospects of nuclear energy. The Czech Ministry of Industry and Trade appears to agree with this statement to a certain extent, warning for market designs that distort the market and arguing for a "… level playing field … for all market participants." (Euractiv, 2017). Interestingly enough, both use almost the exact same wording when discussing market distortions. The argument that subsidies for the development of renewable energy are hurting the prospects for nuclear energy – which has been hailed highly as the future of the Czech electricity mix – is then conceptualized by both to argue against undemocratic practices damaging economic development, dipping into liberal values of free market development. In a radio interview on a public broadcaster in 2018, Czech President Miloš Zeman intensified this hostile attitude, directly referring to solar energy entrepreneurs as "solar barons" and "economic assholes", directly attacking the sub-sector on mainly economic grounds (Energy Transition, 2018).

Yet, some critical voices can be found about the preferred future role of nuclear and renewable energy. Whereas most top-level politicians seem to support the position that nuclear energy is the future of the Czech energy mix and that renewable energy will only play a limited role, a sociological study on the public opinion on renewables claims that over 60% of the Czech republic is in favour of an increased development of clean RES (Obnovitelne, 2018). The leader of the Green party claims that the political debate is lacking any critical discourse and does not match the public opinion about energy-related topics (Hockenos, 2013). Even though the Green Party was not represented in Parliament at the time of writing, the sociological study does present an interesting alternative to the dominant image of renewables as

underdeveloped, uneconomic and unstable. However, concrete political representation of a more optimistic view of the future of RES is lacking.

Former Prime Minister Mirek Topolánek has been cited to refer to Czech intentions within the EU as towards achieving a strong joint Energy Policy and towards cooperation in achieving a diverse supply of energy raw materials. In these publications, he tied this diversification of supply directly to values such as freedom and independence. This emphasis on EU cooperation is in line with statements from the Czech special ambassador for energy, Vaclav Bartuska. In an interview he pointed towards the need for cooperation within the European Union and argued that the Visegrád group is useful in finding common positions but that the group is not the most effective platform for operationalising such a consensus into concrete coordinated legislative action. In part, he argues that this is because of the exceptional position that the Czech Republic holds in the V4 group. Bartuska points towards a higher level of privatisation and integration with north-western markets, rather than being integrated with eastern and southern markets (Schuster, 2018). This notion of exceptionality can also be found rather formalised in the Czech State Energy Policy of 2015, where the vision describes a modern country that has a leading role both within the region and within Europe (NSA-NCSC, 2014).

6.2 Hungary

Much like the Czech Republic, Hungary was left with significant connections to Russia in terms of energy infrastructure. Despite efforts towards diversification of supply, Russia remains their largest supplier in terms of gas, oil and both finance and fuel in the nuclear sector. While the first post-1991 governments tried to redirect their country's economic orientation towards Europe and away from Russia, the energy sector initially held a slightly exceptional position in these efforts. After leaving the Soviet Bloc, Hungary lost access to special rates for gas and oil from Russia which used to be far below market prices. The new sharp increases in prices caused massive uproars and led to the largest public protests since 1956, causing the government to treat access to affordable energy more carefully. Towards the turn of the century, the country had made some strides in terms of privatisation and liberalisation. Yet, despite the introduction of the Third Energy Package, Hungary managed to retain a sense of strategic ownership within the gas sector (Butler, 2018).

The Paks Nuclear Power plant currently produces around 40% of Hungary's electricity consumption. The remainder is produced from hydrocarbon plants, a lignite fired plan and some renewable power generators. The Hungarian government has published several strategic

documents concerning their energy sector, including a national renewable energy action plan and a national energy efficiency plan. Central to the discourse within these strategic documents is decreasing energy dependence through increasing efficiency, increasing the share of renewables and nuclear and through further developing integration into European energy infrastructure (Levego, 2015). Foreign Minister Péter Szijjártó pointed towards the long history that nuclear energy has in Hungary and confirming the government's plan to increase this share in the future (Hungary Today, 2018). By pointing towards this 'long history' he integrates values such as tradition into the discourse and by referring to the future expansion of nuclear energy, he hints towards the development of self-sufficiency.

Much like the Czech Republic, the strategy to achieving energy security does not necessarily refer to self-sufficiency but rather towards reducing dependency on a single supplier through diversification of suppliers and supply infrastructure. This too is closely connected to the events of the 2006 Ukraine Gas Crisis, which impacted Hungary particularly severely. During the crisis, former prime minister Ferenc Gyurcsany indicated his preference to additional supplies over alternative supplies; security through fragmented and flexible distribution (Dempsey 2007). The current Foreign Minister Péter Szijjártó is actively exploring such diversification efforts. He is pushing for the development of a two-way Hungarian Croatian interconnector, importing LNG through the Krk terminal. Hungary is also exploring the possibility to purchase stakes in the terminal that is being built. Next to exploring options in LNG imports, they are also exploring the option to buy gas fields in the Black Sea, starting offshore production in Romania (Hungarymatters, 2018; 2019).

In 2014, natural gas made up the largest share of Hungary's energy mix, representing 33 per cent of the country's energy use. Beyond gas, other energy types within the energy mix included oil (28 per cent), nuclear (19 per cent), coal (11 per cent), and renewable energy sources (9 per cent). In 2018, the country was for 84 percent dependent on imported oil, from which about three quarters came from Russia (IEA, 2018). Concerning gas, imports had risen to an estimated 78 per cent of total demand, from which virtually all imports came from Russia. Before, almost 90% of coal was produced domestically. However, the domestic industry saw severe reductions due to environmental pressure and a EU-pressured halt to subsidies for unprofitable mines. Research indicates some modest potential in geothermal and biomass energy production, but the Hungarian National Energy Strategy 2030 clearly emphasized that 'For the time being, we [Hungary] cannot afford giving up fossil fuels' (Hungarian Government 2012: 11).

In 2010, the Fidesz government was installed with a supermajority in parliament and strongly proclaimed a 'Hungary First' strategy. This strategy was operationalized with increasing state ownership in crucial energy companies and a renewed interest in the Russian energy market. Such dealings were justified on a mainly economic basis: Russia offered cheap prices and the European Union had failed to deliver on promised diversification projects, such as the Nabucco pipeline (Levego, 2015). Russian investments were once again promoted under the slogan 'gaining back the Russian markets', accompanied by calls for an unprejudiced approach. These positions were voiced by Hungarian Prime Minister Peter Medgyessy and Anita Orban (Ambassador-at-Large for Energy Security). Such an approach fits within the wider strategic outlook that Hungary holds; Hungary has regarded itself as a potential bridge between Russia and the West, actively emphasizing that the Russian-Hungarian relations should serve as an example towards the rest of Europe (Socor, 2006). Foreign Minister Péter Szijjártó confirmed this image by stating that Central Europe tends to get stuck in the middle between 'the East and the West'. On various platforms he emphasized the right of countries to decide on their own energy mix, listing values such as sovereignty and independence in deciding on policy within such a strategic sector (Hungarytoday, 2018).

This close relationship with Russia can be observed in the Hungarian approach towards the development of nuclear energy. Nuclear energy accounts for roughly a half of Hungarian electricity. Yet, within 20 years, the existing nuclear reactors in Hungary have to be closed. The government is planning a new power plant at Paks, but this project has not been without its critics. Both green, left-wing and moderate opposition parties have criticised the project but could not prevent the classification of all data surrounding the project, keeping the deals, actors and money flows hidden from the public eye for at least the next 30 years. The classification was passed through parliament with a wide majority from Fidesz MEPs (Hungary Today, 2015). Green MEP Benedek Jávor warned of mismanagement surrounding the project and pointed towards the extensive Russian presence in all aspects of the project. Russia is responsible for the largest share of the funding and Russian company Rosatom would be responsible for fuel and waste disposal. Even though they are strategically locked out of legal ownership structures, it is likely that they will be able to exercise a certain measure of influence. As an alternative to nuclear energy, he recommended renewable energies, but analysts doubt that the technology is far enough to substitute the total capacity. Yet, the debate seems underdeveloped. András Deák, a senior research fellow at the Institute of World Economics,

confirms the lack of public debate in examining possible energy futures; “the alternative to Paks I is Paks II.” (Szalai, 2017; Szőke, 2018).

The role of renewable energy remains relatively small in these developments. The largest share of renewable electricity production comes from biomass. Recently, however, solar power generation is expected to see significant short-term growth due to a feed-in tariff scheme (Végh, 2018). Considering the high political sensitivity of utility costs, most politicians emphasize that renewables need to be competitive in order to really make their way into the Hungarian energy market. Despite this precarious balancing between market forces and environmental considerations, Hungary’s largest new solar plant was just opened outside the Paks area by Péter Kaderják, Minister of State for Energy and Climate Policy, with about a third of the funding coming from the European Union (Hungary Today, 2019). Whereas former strategic documents were moderate in their enthusiasm and support for renewable energy development, Péter Kaderják has stated that the Hungarian government is currently ‘redesigning’ their energy strategy (Végh, 2019). He emphasizes that combinations between carbon-neutral and non-neutral sources are being explored next to efficiency strategies and the application of new technologies. So the initial hesitant attitude towards renewable energy sources has become slightly more favourable. However, doubts remain as ambassador-at-large for Energy Security Pál Ságvári warns that infrastructural development needs to be on track to support these developments (Varsányi, 2017).

6.3 Poland

Interestingly enough, whereas the Polish share a strong dependency on Russian oil and gas supplies, combined with a strong infrastructural integration with the Hungarians, their attitude towards Russia can be characterised as more divided. Some downplay the sector’s vulnerability by pointing towards strategic ownership of the Polish state of energy companies and towards the only moderate dependency in the gas sector. Others still carry largely sceptical sentiments towards Russia. An additional historically relevant element was the revelation of a series of corruption scandals involving both Russian and Polish actors in the 90s. This caused all subsequent developments in the energy sector to be viewed through ‘the prism of the Russian lobby narrative’ (p. 142 Ostrowski, 2018). The Russian-Ukrainian gas conflicts in the late 00s further strengthened the security narrative in this prism. Still, the 2010s saw some rapprochement between Russia and Poland as the first bilateral deals were struck without any middle companies and without the accompanying hostile language (Ostrowski, 2018).

In both the oil and gas sector, Poland has managed to diversify its reliance away from Russia. Whereas Russia accounted for more than 97% of crude oil imports to Poland in 2005, this percentage starting decreasing rapidly after 2013. Estimates from the Financial Observer indicate a relatively low share of 67.2% of Russian oil imports for 2018, with the remainder being supplied by Kazakhstan, Nigeria and the United Arab Emirates (Financial Observer, 2019). The gas sector can be considered as more resilient due to the recent opening of the LNG terminal in Świnoujście. With this terminal, the Polish can switch out almost a third of their gas consumption with LNG imports and even up to 50% if necessary. Currently, plans are in place to even further expand the capacity of the terminal, having received approval and funding from the European Commission (INGWorldNews, 2019). Next to that, the country has some potential in extraction of shale gas – however, extraction is not likely to be realised in the near future – and the country is working together with Denmark in reinforcing the Poland-Denmark interconnection Baltic Pipe with significant EU funding (CEEP, 2019).

The electricity sector, and then specifically the role of coal in electricity generation, holds a somewhat exceptional position. From the 90s onwards, domestically produced coal provided for more than 90% of Polish electricity. However, in the last couple of years domestic production has fallen because of decreases in investment in the state mines. This decrease in production has been replaced with mostly Russian and to a lesser extent US coal imports (Barteczko, 2018). Currently, with increasing EU pressure to de-carbonise, coal accounts for around 80% of electricity. The remainder is generated by renewable and nuclear energy. Gas-fired generation serves as a back-up (Chestney, 2018). Yet, returning to coal, the Polish coal sector is regarded as highly politically organized and represented, with a significant political influence. The sector carries an image of tradition, hard work and national pride (Szulecki, 2017; Euractiv, 2017). The cultural, political and not to mention socio-economic repercussions of attempts to restrict the use of coal are significant in Poland. Next to that, the coal industry serves as a strong guarantee of a measure of energy independence in the electricity sector. This is not irrelevant for a country who has a long history of unstable relations with its main raw energy material supplier, Russia. In 2014, then Polish prime minister Donald Tusk even stated that “coal is synonymous with energy security” (Tusk, 2014). In 2017 still, energy minister Krzysztof Tchórzewski emphasized the vitality of the coal-fuelled plants. He also pointed towards the future potential of nuclear power plants, arguing that these investments are necessary for the stability of the Polish energy mix (Euractiv, 2017). At this point, he carefully

avoids directly opposing the coal industry, but rather focuses on the necessity of stability and diversification.

When making the case for nuclear energy, energy minister Krzysztof Tchórzewski emphasizes that nuclear power produces as little emissions as renewable energy, but has a more reliable and steady production. Next to that he warns for the need of quick ramping capabilities of additional generation capacities to balance the intermittent production of renewables in the absence of economically viable electricity storage capacities (World Nuclear News, 2018). The plans, however, have not been finalised. Former deputy energy minister Michal Kurtyka estimates that the future nuclear power plant will not be operational before 2030 (Barteczko, 2018). In the meantime Krzysztof Tchórzewski has eased his hesitance towards renewables. This is likely due to both the introduction of the new 35% renewable energy quota passed by European lawmakers, and the new (draft) Energy Strategy of Poland, setting out plans for more renewable energy and more nuclear energy (Jakobik, 2018). In a speech at a university symposium he stated that the government wants to invest in renewable energy sources, mainly photovoltaic and biogas. He does emphasize that this needs to happen sensibly and rationally, pointing towards potential distortion of the energy market.

Regarding the role of coal, he states that the very last extension and investment in a coal-fired power plant has been made by the government (First News, 2019). Just a few weeks later, during a session of the Energy and Treasury Committee of the Polish Sejm, he specified further that the development of nuclear and renewable energy are expected to occur in parallel. Tchórzewski warns for the need to also invest in transmission and storage capacities, without excessively burdening the economy (Biznesalert, 2019). According to statements from the prime minister's office, the government is currently implementing mechanisms that are supposed to ensure the stability of electricity prices in the future (Premier, 2018). Critics, on the other hand, warn that these measure will hinder the development of private enterprises, limit competition and ultimately result in low levels of innovation and higher prices (Laszek and Trzeciakowski, 2018)

6.4 Slovakia

As former part of Czechoslovakia, Slovakia shared its strong Russian infrastructural legacy with the Czech Republic. It still imports most of its natural gas (95%) and mainly from Russia. They have, however, made significant strides in cutting their total gas consumption, bringing it down with approximately a third compared to their consumption in 2005 (Knoema,

2018). Next to that, the country has also seen elaborate renovation of its gas infrastructure after the 2009 crisis, installing two-directional flow capacity. These updates were intended to increase the capacity for interconnecting flows within the European continent in the case of gas shortages. Next to that, in 2018 a new project was implemented to increase the connection between Poland and Slovakia, a crucial part of the North-South Corridor (Biznesalert, 2018). This is in line with the 2014 Slovak Energy Policy, which lists diversification of supply infrastructure as its main strategic pillar (Ministry of Economy, 2014). Over the last 25 years, Slovakia has imported a steady quantity of oil from Russia, covering nearly all of their demand (Eurostat, 2018). The country has nearly no potential for domestic oil or gas production. In terms of electricity, Slovakia is particularly independent. It produces about 95% percent of its own usage. More than half of this electricity is nuclear and almost a quarter was covered by decentralised renewables, the rest is made up out of fossil fuels (Worlddata, 2018). Plans announced late 2018 included a phasing out of subsidies for coal mines from 2023, ultimately aimed at decarbonising the electricity sector (Jancarikova, 2018).

In May 2017, Slovak Prime Minister Robert Fico emphasized the increasingly important role of nuclear in the future Slovak energy mix in a public speech (Denkova, 2017). Interestingly, he did not only emphasize self-sufficiency and economic advantages, but also grid security and stability. He referred to a combination of economic, environmental and technological elements in making his push for nuclear energy. Whereas the economic and environmental reasons are quite commonly used, referring to grid security is a rare reference to the technological advantages that nuclear energy production holds over renewable energy sources. These remarks came just months after an agreement being concluded on the construction of a cross-border electricity line between Slovakia and Hungary (Kormany, 2017). In the public statements, security, stability and trade were mentioned as the central values connected to the project.

Also in May 2017, Economy Minister Peter Ziga indicated plans to increase government ownership of strategic energy companies in an interview. The government now holds shares in several electricity and gas companies and plans to moves these shares under the roof of one company and give this company the room to buy more assets. His arguments centre around security considerations, mentioning ‘companies of national importance’ (Jancarikova, 2017). This strong emphasis on security is consistent with another interview that Peter Ziga gave in 2017, where he indicated that energy security is the first priority in the energy sector (TheReport, 2017). In the same interview he also emphasized the relevance of interconnected

networks and in the long-term, he points towards renewables, on the condition that they become more economically viable. Official statements indicate some scepticism towards subsidies as the Ministry is fearful of both market distortion and grid stability. The concerns for market distortion are widely shared within the V4, but the concerns regarding grid stability are not found that often – only fleetingly mentioned within the Hungarian discourse. In Slovakia, however, distribution operators have refused to connect renewable capacities to the grid that supersede a certain capacity, indicating that these concerns are shared throughout society.

6.5 Overview: Towards a V4 Energy Identity?

Previous commentators have argued that a distinct V4 energy policy is hard to uncover. To a certain extent, this appears to be true. There are still, however, some common features of the V4 preferred national energy identities that can be identified. The most prominent one is the shared pursuit of diversification of energy supplies away from their historically main supplier, Russia. Especially the Czech Republic and Poland have made impressive steps by decreasing their dependency on Russia with roughly a third over the last ten years by searching for new suppliers. Slovakia has also reduced their dependency with a third, but rather through efficiency measures than supply diversification. Diversified dependence, rather than self-sufficient independence, is still a strategic goal that is pursued by all four countries, both through diversified infrastructure and diversified suppliers. Some look towards Western markets, such as the Czech Republic, whereas other look towards Asia, such as Hungary and Slovakia.

Another common element in V4 energy policy is that of strategic ownership within the sector. The Czech Republic, Hungary and Poland have strong government ownership structures of key utilities, giving them a strong grip on the sector. Slovakia is currently solidifying their portfolio to be able to effective leverage their ownership. The Hungarian example, however, has indicated that such ownership structures are relatively prone to corruption, resulting in sensitive public oversight. Additionally, the EU is attempting to break open such ownership structures in their endeavour to establish an open market. The Third Energy Package and the decoupling of the market is the prime example of these efforts. Still, a desire for autonomy in choosing one's own energy mix and control over key elements in the sector is decidedly present in the Visegrád countries.

Another largely recurring theme within the V4 energy identities is the strong appetite for the development of nuclear production capacity. Slovakia currently already draws 50% of its

electricity use from nuclear energy. Hungary and the Czech Republic have plans in place to reach a 50% share of nuclear energy in their electricity mix between 2030 and 2040 and Poland has also begun to indicate its interest towards the development of nuclear energy. Common arguments for this focus on nuclear energy are its economic competitiveness, compatibility with climate commitments and diversification aspirations. Particularly the argument of its economic advantages are emphasized relatively often. Renewable energy sources are generally considered less competitive and less stable in their production, which also increases the burden on grid management. Yet, even in the case of nuclear energy development, there are concerns regarding grid stability. Hungary, with its ambitious Paks nuclear ambitions, has noted that their development plans do require substantial investments in their not-too-modern electric grid. The projected increase in electricity production capacity will likely even exceed their domestic demand, requiring additional international transmission capabilities.

Such cross-border integration plans exist throughout the V4. All the V4 countries are currently exposed to overcapacity loop-flows originating from Germany, placing a large burden on transmission operators charged with re-dispatching such charges. EU funded projects intended to facilitate such cross-border exchanges have the added benefit of preparing the grid for future thermal and RES generation facilities (Energy Union, 2015). Next to that, Hungary and Slovakia are planning the development of a cross-border electricity transmission line and the Czech Republic is planning the Czech North South corridor, transmission infrastructure that is supposed to increase the connection between Czechia and Germany. Such international integration projects concerning grid governance will be studied in more depth in the next chapter through the lens of both the technical reality proposed in chapter 4 and the national energy identities constructed in this chapter. The final purpose of this analysis is to uncover the influence of the cyber-transition in international grid governance by making use of the socio-technical imaginaries approach, which allows for a dual focus on the influence of both technology and politics in international governance in highly technical sectors.

7. International Governance in V4 Electricity Sectors

In this final section of this study, the last step will be taken in order to answer the research question: how do developments in the cyber dimension of the electricity sector influence V-4 energy policy and cooperation? By constructing a technical reality concerning the cyber transition and holding this next to the analytical framework of national energy identities, international governance structures can be analysed for evidence of security concerns regarding the cyber dimension of grid governance. This section will first discuss V4 initiatives, statements and approaches regarding the matter. The main sources that will be used are the V4 Presidency programmes and annual reports from 2004 onwards. These will be supplemented with other statements and official documents. Throughout this discussion, the content will directly be analysed from the socio-technical perspective as set out before. There will also be attention for EU policies but only to the extent that these are relevant in illuminating V4 behaviour.

Ever since the first V4 Presidency programmes were published, energy has been on the agenda. The 2003-2004 Czech presidency program discusses issues ranging from EU energy legislation to cross-border power exchange. Whereas the energy and raw material sections take up a relatively large share of the program, cyber is not mentioned (Visegrád group, 2004). In the final report, however, energy had moved down the list significantly and was only represented through a short mentioning of a meeting of a working group for energy that had taken place in January 2004. Shortly after, the Polish presidency of 04-05 re-emphasized the relevance of the energy sector by listing it as fifth of their six priorities (Visegrád Group, 2005). Interestingly, they immediately emphasize the electricity sector by specifying the need for cooperation concerning the Trans-European Electricity Network. This can perhaps be attributed to the Polish coal industry, at that time still producing significant quantities of electricity. The final presidency report does not mention energy (or industry, for that matter, since energy working groups are considered to be part of Ministries of Industry), much like the previous presidency year. This period was marked by a stronger emphasis on EU accession and the following transition. Whereas there was initial enthusiasm about cooperating more in the field of energy, real initiatives did not (or barely) materialize.

The 05-06 Presidency program of Hungary appears to be modelled on the Czech one from two years earlier. It includes an energy section which elaborates more on the interconnection of electricity grids, referring to the ambitions of the previous Polish presidency, and harmonizing tariffs on cross-border transports (Visegrád Group, 2006). The final report, which takes the form of a listing of intergovernmental meetings, lists two specific V4+ format

meetings on the ministerial level regarding the energy sector. This indicates a slight stepping up in efforts to promote V4 energy cooperation. Cyber is still not a part of either document. The following 06-07 Slovak Presidency is again more elaborate in its discussion of its plans in the energy sector. There is a renewed focus on diversification of supply and the coordination of interests in order to more effectively pursue them at the EU level (Visegrád Group, 2007). The emphasis on diversification of supply is likely a result of the first serious Ukraine-Russian gas dispute, as it is accompanied by the recommendation to develop strategic natural gas emergency reserves. Here, traditional energy security concerns are clearly visible. Also for the first time, the development of renewable energy sources, efficiency strategies and nuclear development are mentioned. All three fit particularly well with the Slovak profile – a relatively high share of nuclear energy in their energy mix, large efficiency gains and a relatively high share of renewable energy sources.

The Presidency of 2007 to 2008 was held by the Czech Republic and energy moved down the priority list. On the other hand, this presidency program was the first to list energy as a security matter, instead of using more neutral terms of energy policy or energy cooperation. The adoption of this security terminology is likely due to the persevering Ukraine-Russian gas dispute. It is however not accompanied by the same urgency as in the previous year. Another newcomer in the presidency program is climate change, which is mentioned to emphasize the relevance of efficiency strategies and the development of renewable energy sources. In this context, the Environment and Industry ministers eventually met to discuss renewable energy sources and efficiency mechanisms. According to the presidency report, the Czechs also sought to organize a V4 Economy ministers meeting regarding energy security, with the intention to set up a V4 working group, but this failed due to a lack of interest.

The 2008-2009 Polish Presidency continued the environmentalist trend and introduced the concept of a 'Green Visegrád', centred around energy conservation and environmental issues (Visegrád Group, 2009). Especially conservation and efficiency are topics that fit well with Polish interest. In addition, projects of connecting transmission grids were mentioned as an area of interest – much like the previous Polish presidency. Ukraine is also mentioned quite specifically, the Presidency programmes encourages the V4 to support Ukraine's aspirations to join the Energy Community. This is in line with the wider Polish stance of displaying strong solidarity towards Ukraine against the 'Russian threat' and is in line with the wider political aftermath from the Ukraine-Russian gas conflict. Climate and energy security considerations are strongly represented throughout the document, referring the 3rd energy legislation package

and energy infrastructure integration. Due to the 2009 Russian-Ukrainian energy crisis and growing climate concerns, energy became a prominent issue on several ministerial meetings (Agriculture, Foreign Affairs, Industry, Transportation). Interestingly enough, this presidency saw the first meeting of the V4+ format with Russia as a guest. The final V4 group meeting even established a V4 task group of governmental plenipotentiaries for energy security, reinforcing independent institutional power of the V4 in the energy sector. Interestingly enough, cyber security was still not a part of the program or final report – despite the severe cyberattack that Estonia suffered during the Polish Presidency. Considering the frequent collaboration between the V4 and Baltic groups, some concern or solidarity in this regard could have been expected.

The 2009-2010 Hungarian Presidency placed energy security as its third priority out of the five identified key areas. This is again likely a consequence of the 2009 Russian-Ukrainian energy crisis. Ukraine held a special position in this presidency program with a range of cooperation activities proposed within the V4+ format. Energy cooperation and energy safety are listed within the propositions. Within this presidency program, energy policy and energy security are steadily reoccurring themes, whereas environmental concerns seem to have moved to secondary importance. This is in line with the concerns after the financial crisis, where access to cheap fuel was prioritised over long term concerns about climate change. Previous emphasis on the interconnectivity of electricity transmission also seem to have taken a step back in favour of interconnectivity of the gas market. This period was marked by a V4+ energy security summit of the prime ministers. This is in terms of attendees a step up from previous working groups and ministerial meetings. Two additional 'regular' high level energy security meetings took place in the same presidency year. The main topics that were discussed were resilience in the case of gas disruptions, gas pipelines and LNG potential. In the wake of the 2009 gas disputes, gas security has taken the forefront of V4 energy concerns.

The subsequent 2010-2011 Slovak presidency aptly named the 2009 gas dispute 'the energy crisis' and places it next to the economic crisis in painting the broader security landscape that Europe is facing at the time. Interconnection and efficiency are keywords in setting out the Slovak intentions for their presidency. Again, considering their low levels of diversification but successes in terms of efficiency measures, these are in line with Slovak preferences. Interestingly enough, the electricity sector is the first to be mentioned in their broader energy section. This is likely due to the implementation of the Third Energy Package taking place around this time. The Slovak presidency report of this period is one of the most extensive V4

presidency reports published up until that moment. One of the more specific outcomes of V4 coordination was a joint letter of the V4 Economy Ministers sent to the European Commissioner for Energy regarding regional initiatives and infrastructure development. The period also saw a ministerial meeting and several high level working groups specifically on the North-South Interconnections. This presidency report is the first document that mentions cybersecurity – and it mentions it only once – in the context of a joint statement by the V4 Prime Ministers in Bratislava in 2011.

The 2011-2012 Presidency was passed on to the Czech republic, who listed energy as a major Visegrád theme – not only in terms of formulating common positions within the EU, but also in the promotion of a common external European energy policy (Visegrád Group, 2012). There is a strong emphasis on projects of common interests in terms of infrastructure and diversification efforts in terms of oil and gas. Renewable energy sources are referred to as 'unconventional resources', which is in line with the Czech scepticism towards decentralized renewable energy sources both in terms of prices and reliability. Later on, the interconnection of electricity is also touched upon, with regard to cooperation with ENTSO-E countries. Cybersecurity has disappeared from the program. As set out in the presidency report, energy was high on the agenda during two Prime Minister summits. This is another step up in terms of urgency attached to the topic. The main issues discussed centred around route diversification and 'a rational approach to the energy mix'. Such a careful wording is again in line with the Czech policy of diversification of dependence, rather than actively establishing energy self-sufficiency. The V4 State Secretaries for EU affairs also met to discuss energy security and nuclear energy, the latter being a strong common theme between the individual V4 energy preferences.

The Polish took responsibility for the 2012-2013 Presidency and moved energy security slightly down the line of priorities (Visegrád Group, 2013). In line with Polish preferences, it discusses shale gas extraction, nuclear power cooperation and security of oil supplies. A separate section is dedicated to energy security, where the natural gas and oil sectors are heavily emphasized. In the electricity sector section, concerns regarding loop flows are shared, next to the development of Projects of Common Interests. Concerns regarding loop flows are also strongly shared between the V4 countries as they affect all their grids. This presidency year witnessed a V4 Energy ministers meeting and several other high level group meetings in V4 and V4+ format. Cyber security is mentioned once, alongside energy security on the range of topics where the V4 sees cooperation possibilities with the Baltic states, Romania and Bulgaria.

It is not further elaborated upon. According to the presidency report, another joint letter was sent to the European Commission by the V4 economy ministers regarding energy and climate policy. The letter emphasized that this policy should take competitiveness of the European economy into account. Such an emphasis on competitiveness is typical for the Polish, who have often underlined the need for affordable energy supplies, particularly in the context of pressure to reduce their coal mining. Another shared statement from Industry ministers emphasized integration of the regional mas market and the internal electricity market. When discussing the electricity market, the danger of loop flows were discussed as 'a real and actual threat to energy security'. Renewable energy is tentatively mentioned as a potential future source of energy if they prove competitive in the future. This appears to be a continuation of the position outlined in the letter of the V4 economy ministers and fits in the energy preferences of multiple V4 states.

The Hungarian Presidency of 2013-2014 put energy security squarely at the top of the agenda and listed it as its number one priority area. This is highly likely due to the rising tensions between Russia and the Ukraine, ultimately leading up to the Russian annexation of Crimea. The primary strategy that Hungary proposes in its program is that of minimizing dependency through establishing interconnections and most crucially, the Hungarian-Slovak interconnector. Especially with the prospect of Ukraine of a reliable interconnector dwindling quickly, these concerns are very understandable. Cooperation with the USA is mentioned in the field of developing nuclear energy. This is particularly interesting as this took place in the process towards the development of the Paks nuclear power plants. Interestingly, the program also emphasises cooperation with the Baltic countries in the fields of energy security and cyber security. Cyber security plays a larger role in this program. The program even sets out the aim of setting up a V4 cyber security cooperation mechanism. Most of the discussion of cyber security squarely takes place within the security and defence policy section.

The final report sheds more light on its definition of energy security and places it within the context of reducing dependence and the main strategy for reducing it is integrating the European gas market. During the 2013 Visegrád Prime Ministers Summit it was also agreed that the production of shale gas and further development of nuclear capacity were desirable. The emphasis on nuclear capacity was to be expected, considering the strong shared preference among the V4 countries towards nuclear energy, but the mentioning of shale gas development specifically indicates the ability of Poland to gather support and solidarity for their agenda during other presidencies. The presidency year saw a number of high level meetings on energy

and saw energy issues integrated in multiple agendas. Cyber security, on the other hand, despite the attention it received in the presidency program, was barely acted upon as only two expert meetings took place. Besides the mentioning of these meetings there was no further elaboration.

The subsequent 2014-2015 Presidency was held by Slovakia. They continued the line set out by the previous presidency and kept energy security at the top of their agenda. The program emphasizes modernizing transmission infrastructure in both the gas and electricity sectors. Climate receives an exceptional amount of attention, compared to the other programmes. This environmental focus fits relatively well with the Slovak profile. Compared to the rest of the Visegrád group members, Slovakia is a front runner in terms of renewable energy. The document also emphasizes the need for competitiveness of the industry in the face of climate measures, here the influence of Hungarian and Czech concerns can be distinguished. The program is also increasingly elaborate in its treatment of cybersecurity. The Slovaks introduce the 'Digital Agenda', which combines the digital economy and the area of cyber security. For the first time, cybersecurity is lifted from the security and defence section and integrated in the economic agenda. In the final report, however, the initiatives from the Digital Agenda were not heavily represented. Cyber security moved back into the security and defence sections, as a part of CSDP initiatives. V4 efforts on climate and energy policy, on the other hand, were well represented. This included cooperation on the implementation of the post-2020 European policy framework and a joint risk assessment in the field of gas supply. The electricity sector appears to have taken a backseat again, which is unsurprising given the continuing tensions between Russia and Ukraine reaching its height around this period. Initiatives include energy cooperation with Ukraine by establishing reverse gas flow capacities.

The 2015-2016 Czech Presidency moved energy slightly down the agenda by listing it as a second priority, their proposals centred around implementation of the Energy Union project, establishing an internal gas market and cooperating with third countries. Cooperating with third countries is in line with the Czech diversification efforts in the search of alternative oil and gas suppliers. Cyber security is once again carefully coined as a 'prospective topic for the Visegrád cooperation', embedded within security and defence cooperation. Much like the previous Presidency, it suggests the Central European Cyber Security Platform (CECSP) as a useful platform to operationalise V4 cyber security cooperation. The report, however, does not discuss cybersecurity activities or initiatives. This can be considered relatively odd, considering growing concerns about hybrid warfare and the (successful) cyberattack on the Ukrainian electricity grid. In terms of energy, there was more substantial V4 activity, as the V4 published

a non-paper on energy security, stressing the relevance of Ukraine as a gas transit route. Interestingly, the report states that 'on some issues the V4 were unable to find a common position, […] trend towards fragmentation of V4 energy cooperation.' Here the Czech Republic acknowledges the difficulties of pushing for a common agenda with diverging national positions.

The 2016-2017 Polish Presidency stood largely in the light of the migration crisis and, as it coincided with the Slovak presidency of the EU Council, consolidating V4 interests to bring them to the EU level more effectively. Within the topics proposed, energy policy has distinctly taken second place behind migration. Regarding energy security, the focus is again largely on natural gas supply routes and integration of the Polish LNG terminal into the internal market. Nuclear energy is also awarded a large section of the presidency program, with the support of all of the V4 countries. Cyber security is mentioned as an area of cooperation, next to the Digital Single Market Strategy, and is placed within the security and defence section. In the final report, the digital agenda is discussed, but cybersecurity is reduced to being mentioned only once in a declaration by the prime ministers. Energy issues were represented more substantially. The Polish Presidency saw the presentation of a shared vision of energy independence for the V4, based on gas market integration and LNG imports through Swinoujscie – a tangible outcome in line with the Polish profile. The vision also included solidarity mechanisms regarding natural gas supply, a shared V4 interest.

The following 2017-2018 Hungarian Presidency placed a strong priority on both energy and digital interests. In terms of energy policy, there was a larger focus on infrastructure interconnectivity than energy security or independence per se. Especially the North-South Gas corridor is emphasized, but there is also attention for LNG development, cross-border loop flows and renewable energy. In the field of cybersecurity, there is an emphasis on critical infrastructure, information-sharing and the formulation of joint V4 positions towards the EU agenda. The report of this presidency allows for a fairly limited evaluation of these intentions as it takes the form of a 6-page infographic. It does mention the achievement of a joint V4 position towards EU energy policy and the launch of an energy think tank platform. The section on the digital agenda does not mention cybersecurity specifically.

Studying the development of the V4 agendas and activities, the development of cooperation on energy issues can clearly be observed. It started out as a minor element of presidency programmes, but has taken up an increasingly large share of V4 activities and has steadily risen through the ranks of V4 priorities. The common interests in diversification of supply routes,

interconnecting infrastructure and developing nuclear energy potential can also strongly be recognized throughout the years. During the Russia-Ukraine gas crises, energy security gained attention as a true security issue and gained more urgency on the agenda. Another interesting observation is its integration into different agendas. Gradually, energy issues were discussed in agriculture meetings, environment meetings, economy meetings and meetings by foreign ministers. So not only did energy move up the agenda 'vertically', it also spread throughout V4 policy 'horizontally'. Throughout the different Presidencies, subtle national distinctions could be noted. The Polish presidencies paid more attention towards the integration of LNG in the internal gas market, the Czechs and Hungarians strongly stated their concerns for the competitiveness of renewable energy sources and the Slovaks dedicated more time to environmental initiatives. The activities also reflected wider regional or even global developments. Security of supply in the gas sector became a prominent issue during the Russia-Ukraine gas disputes and during the height of the financial crisis, affordability took precedence over sustainability.

Other developments, on the other hand, seem less represented. Cybersecurity only appeared on the Slovak Presidency agenda of 2010-2011, almost three years after the cyberattack on Estonia. It gains little traction over the years. Most of its (limited) discussion takes place within the security and defence agenda. Later on, the 'Digital Agenda' does start taking up a larger share of V4 cooperation, but does not specify on cybersecurity per se. It centres around topics of digitalisation and work force developments. Not even the attack on the Ukrainian electricity grid in 2015, the Petya or Wannacry ransomware attacks or growing concerns about information warfare seem to really be able to firmly place cybersecurity on the V4 agenda. In the light of the cyber-transition, as outlined earlier in this research, and considering the high placement of energy security on the V4 agenda, it would have been likely that concerns about the cybersecurity of the electricity grid would have found their way into V4 governance. The opposite appears to be true. Cybersecurity does not gain much traction on the international agenda and if it does, it remains firmly positioned in the security and defence sections. It is not integrated into other topics, as is the case with energy policy to a certain extent.

The discussion of energy security on the international level appears to remain within the traditional fossil fuel framework and concerns are limited to security of supply and affordability, with sustainability only playing an intermittent but largely secondary role. There is some integration of energy concerns into other agendas, which indicates its increasing urgency. Yet, despite the frequent use of the term energy security, it is never directly placed on

the security and defence agenda. Its discussion is mainly located within the Ministries of Industry or Ministry of Economy. Sporadically, it finds its way to the heads of state, but these instances are still rare.

Cybersecurity is almost strictly placed under security and defence categories with very limited integration into other agendas, least of all the one of energy security. Cyber security is casually discussed within the 'digital agenda', but mainly in terms of job opportunities. A truly integrated agenda concerning both energy and cyber security, properly addressing the risk profile of the cyber dimension of the electricity grid, can only be found in industry and academic discussions and publications. Political discourse and governance publications seem to adhere to a stricter divide and show very distinct influences of national preferences.

In retrospect, the preferred national energy identities proved incredibly insightful in analysing V4 energy cooperation. They allowed for a detailed analysis of the timeline of V4 cooperation, distinguishing between the influence of national interests, shared interests and global events. The technical reality as developed earlier in this study on the other hand, merely proved to this analysis what it was missing. Despite cybersecurity being one of the main concerns of our information societies, despite the Visegrád countries sharing infrastructural vulnerabilities and despite the growing scale and impact of cyberattacks, cooperation in the field has not significantly materialized on the Visegrád platform. For some reason – perhaps time, perhaps perceived urgency, an interesting topic for future research – cybersecurity did not evolve in the same pattern as energy security on the V4 agenda. It did not move horizontally or vertically. The two agendas did not integrate.

Ultimately, looking back on the original research question, it has to be concluded that the cyber-transition in the electricity sector barely affected V4 energy governance. By analysing Visegrád Group cooperation regarding the energy sector between 2004 and 2018 from the socio-technical perspective, this analysis managed to point out that national energy preferences, mainly defined within the tradition fossil fuel framework, almost completely overshadow concerns introduced by the cyber-transition on the international agenda. The digitalisation of the electricity sector and the broadening risk profile that accompanies it, are mainly discussed within industry and academic circles but the political implications remain out of sight. Cybersecurity does reach the international agenda, but only marginally and it does not enter the energy agenda. Why this is the case, is an interesting question but unfortunately outside the scope of this research. Perhaps future research can shed a light on this question.

8. Conclusions

The energy sector, despite being considered by many to be a natural monopoly, turned out not to be immune to European decoupling efforts. The Energy Union is the institutional embodiment of the European wish to integrate and innovate – even in a sector as technological and complex as the energy sector. Yet innovation means change and change brings new challenges. The increasing digitalisation of the grid, its innovative control systems and tendency towards decentralization bring new complications to the security landscape. This research set out to discern the effects of these changes – referred to as the cyber-transition – on international energy governance in the V4. By adopting a socio-technical approach, the study attempted to establish a balance between technological considerations and social identities in order to see how both affected final international cooperation. In a time where technology and its infrastructure are so influential over the design of our wider societies, such an approach offered the appropriate amount of emphasis to both technological and political perspectives, or imaginaries.

To do this, first, a technical reality was constructed by conducting a content analysis of industry reports. This section developed an aggregate account on the cyber-transition of the electricity grid from a technical perspective and offered an insightful analysis of the technical consensus regarding the cybersecurity of the electric grid. Secondly, preferred national energy identities were constructed by analysing national political discourse along the lines of a discourse analysis from the individual V4 countries. These individual national energy identities allowed insights into the norms and values at the centre of national policies – allowing for a sharper and deeper analysis of national interests at the international level. In the final step, following the logic of the socio-technical approach, these two elements were used as an analytical framework through which to study the effects of the cyber transition in the electricity sector on V4 cooperation in the energy sector.

While using this socio-technical approach to analyse V4 international cooperation in the energy sector, it quickly became clear that elements of the preferred national energy identities could strongly be recognized in final governance activities. The V4 countries could be seen to cooperate on shared interests, but also on interests that were more specific to only one or two members. Energy, as an issue, spread throughout the international agenda both horizontally and vertically. It reached top level agendas and integrated with agricultural, economic, environmental and industry agendas. Specific preferences in certain sub-sectors, such as nuclear

energy or LNG, or regarding certain values, such as competitiveness and solidarity mechanisms, could also clearly be distinguished.

Cybersecurity, however, was very slow to develop in V4 governance. It remained in its security and defence silo and did not integrate with other agendas – if it was discussed at all. Whereas the consequences of the Ukraine-Russian gas disputes, the financial crisis and the migration crisis could clearly be recognized in V4 cooperation, the largest cyberattacks did not have the same effect. The attack on Estonia, the Petya and Wannacry attacks, the hack of the Ukrainian electricity grid or even the more recent data privacy scandals did not manage to give cybersecurity a firm position within V4 security considerations and did not allow cyber-related concerns to penetrate the energy security debate. The energy security debate still largely centres around oil and gas supply of security, the more traditional view of energy security. In the ongoing process of the cyber-transition in the electricity sector, academia and the industry have recognized the broadened risk profile in the cyber-dimension of the energy sector. They have broadened their gaze from pipeline politics to also include grid governance. The V4 international political debate, however, has not.

The socio-technical imaginaries approach, with its interesting combination between content analysis and a discourse historical approach, emphasises the far-reaching consequences that our imagination can have on our actions. They shape and limit the range of possibilities that we see for the future, defining our politics and policies. Here, the approach allowed for an insight into the technical perspective on the cyber-transition of the electricity grid, a deeper understanding of the values and preferences that shape individual national energy identities and, most importantly, a unique insight into the forces that shape international governance in a sector as technical and precarious as the energy sector. It clearly displayed that, where the cybersecurity of the Central European energy sectors are concerned, traditional politics strongly take precedence over the abstract concerns coming from the cyber-dimension. Whereas the future may see an increased emphasis on the security of our electric grids, fossil fuels currently still dominate the international agenda.

9. Bibliography

Beaulieu, A., de Wilde, J., & Scherpen, J. M. A., eds. (2016). *Smart Grids from a Global Perspective: Bringing Old and New Energy Systems.* Springer: Switzerland.

Bolton, R., Lagendijk, V., & Silvast, A. (2018). Grand visions and pragmatic integration: Exploring the evolution of Europe's electricity regime. *Environmental Innovation and Societal Transitions*, no.15, 1-14.

Campbell, R.J., (2015). *Cybersecurity Issues for the Bulk Power System*. Washington: Congressional Research Service.

CBS News (2017, June 23). Was Russian Hacking of Ukraine's power grid a test run for U.S. attack? *CBS News*. Accessed 19 February 2019. Retrieved from: https://www.cbsnews.com/news/russian-hacking-of-ukraines-power-grid-test-run-for-us-attack/.

Central European Energy Partners (2019, January 25). EU invests almost EUR 800 million on energy infrastructure in Central Europe. *Central Europe Energy Partners*. Accessed 19 February 2019. Retrieved from: https://www.ceep.be/eu-invests-almost-eur-800-million-on-energy-infrastructure-in-central-europe/

CEZ Group (2017). *EY: Firms' ability to predict cyber-attacks has increased*. Accessed March 25 2019. Retrieved from: https://www.cez.cz/en/cez-group/media/macroeconomic-news/5019.html.

Cherp, A. and Jewell, J., (2014). The concept of energy security: Beyond the four As. *Energy Policy,* no. *75*, 415-421.

Council of European Energy Regulators (2018). *CEER Cybersecurity Report on Europe's Electricity and Gas Sectors*. Council of European Energy Regulators asbl: Brussels.

Cox, J. (2016a, January 4). Malware Found Inside Downed Ukrainian Grid Management Points to Cyberattack. *Vice Motherboard*. Accessed 19 February 2019. Retrieved from https://motherboard.vice.com/en_us/article/z43vdx/malware-found-inside-downed-ukrainian-power-plant-points-to-cyberattack.

Cox, J. (2016b, January 26). The Malware That Led to the Ukrainian Blackout. *Vice Motherbooard*. Accessed 19 February 2019. Retrieved from https://motherboard.vice.com/en_us/article/wnx5yz/the-malware-that-led-to-the-ukrainian-blackout.

Dearden L. (2017), Hackers target Irish energy networks amid fears of further cyberattacks on UK's crucial infrastructure, [online] http://www.independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irishenergy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html

Denkova, A. (2017, May 26). *Sobotka and Fico: Czechs and Slovaks committed to nuclear energy*. Euractiv. Accessed March 25 2019. Retrieved from: https://www.euractiv.com/section/energy-environment/news/sobotka-and-fico-czechs-and-slovaks-committed-to-nuclear-energy/.

Denkova, A., (2016, November 22). *Czech support for renewable energy in uncertain situation*. Euractiv. Accessed march 25 2019. Retrieved from: https://www.euractiv.com/section/energy/news/czech-support-for-renewable-energy-in-uncertain-situation/

Denkova, A., (2017, February 2). *Czechs against capacity mechanisms, regional centres in Winter Package*. Euractiv. Accessed March 25 2019. Retrieved from: https://www.euractiv.com/section/energy/news/czechs-against-capacity-mechanisms-regional-centres-in-winter-package/.

Denkova, A., Zgut, E., Kokoszczy, K., and Szalai, P. (2017, March 16). *V4 energy security: the land of nuclear and coal*. Euractiv. Accessed March 25 2019. Retrieved from: https://www.euractiv.com/section/electricity/news/v4-energy-security-the-land-of-nuclear-and-coal/.

Dostál, V., and Végh, Z. (2017). *Trends of Visegrad European Policy*. Prague: Association for International Affairs.

Ducheine, P. (2016). Cyber warfare is taking place! *Clingendael Internationale Spectator*. Accessed 19 February 2019. Retrieved from https://spectator.clingendael.org/pub/2016/6/cyber_warfare_is_taking_place/.

Duyvesteyn, I. (2016). Cyberaanvallen: organisatie, besluitvorming en strategie. *Clingendael Internationale Spectator*. Accessed 19 February 2019. Retrieved from https://spectator.clingendael.org/pub/2016/6/weerbaarheid_tegen_cyberaanvallen/.

Estonian Information System Authority (2018). *Annual Cyber Security Assessment 2018*. Tallinn: Information System Authority of the Republic of Estonia.

EU28 Survey (2018). EU Coalition Survey: Results of the EU28 Survey 2018 on coalition building in the European Union. London: European Council on Foreign Relations.

European Commission (2014). Communication from the Commission to the European Parliament and the Council: European Energy Security Strategy. 28 May 2014. Brussels.

European Commission (2016). *Cybersecurity*. Accessed 19 February 2019. Retrieved from: https://ec.europa.eu/jrc/en/research-topic/cybersecurity.

European Commission (2017). *EU Cybersecurity Initiatives Factsheet.* Accessed 03 March 2019. Retrieved from: https://ec.europa.eu/digital-single-market/en/cyber-security.

European Commission (2018). *EU Energy in figures: Statistical Pocketbook*. Luxembourg: European Union.

European Technology & Innovation Platforms (2018). *Digitalization of the Energy System and Customer Participation: Description and recommendations of Technologies, Use Cases and Cybersecurity*. ETIP-SNET WG4 TF3.

Franceschi-Bicchierai, L. (2016, August 4). How Drones Could Help Hackers Shut Down Power Plants. *Vice Motherboard*. Accessed 19 February 2019. Retrieved from https://motherboard.vice.com/en_us/article/yp3qqb/how-drones-could-help-hackers-shut-down-power-plants.

Ghavam, Z. M. (2016). *NATO's Preparedness for Cyberwar*. Monterey: Naval Postgraduate School.

Ghica, L. (2008). Rhetorical strategies, institutional dilemmas: The Visegrád group and the Baltic cooperation facing the EU and NATO accession process. *Analele Universităţii Din Bucureşti. Seria Ştiinţe Politice, X*(10), 75-86.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *Organizational Research Methods, 16*(1), 15-31.

GLOBSEC (2017). *Future War NATO? From Hybrid War to Hyper War via Cyber War*. GLOBSEC NATO Adaptation Initiative. Accessed 19 February 2019. Retrieved from https://www.globsec.org/wp-content/uploads/2017/10/GNAI-Future-War-NATO-JLF-et-al.pdf.

Glynos, J., Howarth, D., Norval, A., and Speed, E. (2009). Discourse Analysis: Varieties and Methods. *ESRC National Centre for Research Methods Review Paper*, August 2009.

Greenberg, A. (2017, June 28). Researchers found they could hack entire wind farms. *Wired.* Accessed 23 February 2019. Retrieved from: https://www.wired.com/story/wind-turbine-hack/.

Gurzu, A. (2018, 31 August). Romania's Black Sea gas sparks political crisis. *Politico.* Accessed 19 February 2019. Retrieved from: https://www.politico.eu/article/romania-black-sea-gas-political-crisis-liviu-dragnea/.

Hetter Tidwell, J., and Tidwell, A.S.D. (2018). Energy ideals, visions, narratives, and rhetoric: Examining sociotechnical imaginaries theory and methodology in energy research. *Energy Research & Social Science*, 39, 103-107.

Imeson, M. (2017, November 8). Electricity industry on alert for 'cyber sabotage'. *Financial Times*. Accessed 19 February 2019. Retrieved from https://www.ft.com/content/1fc89bd8-996c-11e7-8c5c-c8d8fa6961bb.

Institute for Foreign Affairs and Trade (2018). *New Security Challenges from a Visegrad 4 Perspective*. IFAT: Budapest.

International Energy Agency (2019). *Statistics.* IEA.org. Accessed 19 February 2019. Retrieved from:

https://www.iea.org/statistics/?country=WORLD&year=2016&category=Energy%20supply&indicator=NatGasProd&mode=chart&dataTable=GAS.

Jarmakiewicz, J., Maslanka, K., & Parobczak K., (2015). Evaluation of the Cyber Security Provision System for Critical Infrastructure. *Journal of Telecommunications and Information Technology*, no. 75, 22-29.

Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2017). Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection, 18*, 20-33.

Jasanoff, S. (2015). Serviceable Truths: Science for Action in Law and Policy. *Texas Law Review* 93(7), 1723-1751.

Jasanoff, S., & Kim, S. (2009). Containing the atom: Sociotechnical imaginaries and nuclear power in the united states and south korea. *Minerva, 47*(2), 119-146.

Jasanoff, S., & Kim, S. (2013). Sociotechnical imaginaries and national energy policies. *Science as Culture, 22*(2), 189-196.

Jay, J. (2017, December 8). Cyber-attacks on critical national infrastructure firms may double by 2020. *TEISS*. Accessed 19 February 2019. Retrieved from https://www.teiss.co.uk/news/cyber-attacks-critical-national-infrastructure-firms/.

Jewkes S., Vukmanovic O., Suspected Russia-backed hackers target Baltic energy networks, [online] http:// www.reuters.com/article/us-baltics-cyber-insight-idUSKBN1871W5 http://www.reuters.com/article/ us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5

Kapersky Lab (2017). *Cybersecurity for Electric Power Infrastructure*. ICS Cybersecurity report.

Kuchler, M., & Bridge, G. (2018). Down the black hole: Sustaining national socio-technical imaginaries of coal in poland. *Energy Research & Social Science, 41*, 136-147.

Lagendijk, V. (2008). [proefschrift] Electrifying Europe: the power of Europe in the construction of electricity networks. *Technology and European History series*: Eindhoven.

Lagendijk, V. (2012). To Consolidate Peace? The international electro-technical community and the grid for the United States of Europe. *Journal of Contemporary History, 47*(2), 402-426.

Lagendijk, V. (2018). Ideas, individuals and institutions: Notion and practices of a European electricity system. *Contemporary European History, 27*(2), 202-220.

Levenda, A. M., Richter, J., Miller, T., & Fisher, E. (2018). Regional sociotechnical imaginaries and the governance of energy innovations. *Futures*.

Lin, A. (2014). Critical discourse analysis in applied linguistics: A methodological review. *Annual Review of Applied Linguistics*, 34, 213-232.

Maglaras, L. A., Maglaras, A., Kim, K., Janicke, H., Ferrag, M. A., Rallis, S., Cruz, T. J. (2018). Cyber security of critical infrastructures. *ICT Express, 4*(1), 42-45.

Marsh & McLennan Companies (2014). *Advanced Cyber Attacks on Global Energy Facilities.* Marsh LLC.

Minarik, M. (2014). Energy Cooperation in Central Europe: Interconnecting the Visegrad Region. *Occasional Paper of the Energy Charter Secretariat Knowledge Centre*, 23 October 2014.

Ministry of Defence of Estonia (2008). *Cyber Security Strategy*. Tallinn: Ministry of Defence.

Ministry of Industry and Trade (Czech Republic) (2017). *National Action Plan for the Development of the Nuclear Energy in the Czech Republic.* Accessed March 25 2019. Retrieved from: https://www.mpo.cz/en/energy/strategic-and-conceptual-documents/national-action-plan-for-the-development-of-the-nuclear-energy-in-the-czech-republic--232864/.

Ministry of Industry and Trade (Czech Republic) (2018). *State Energy Policy of the Czech Republic*. Accessed March 25 2019. Retrieved from https://www.mpo.cz/assets/en/energy/state-energy-policy/2017/11/State-Energy-Policy-_2015__EN.pdf.

Ministry of Industry and Trade (Czech Republic) (2019). *Executive Summary of the Draft of Integrated National Energy and Climate Plan of the Czech Republic*. Accessed March 25 2019. Retrieved from https://www.mpo.cz/en/energy/strategic-and-conceptual-documents/the-draft-of-integrated-national-energy-and-climate-plan-of-the-czech-republic--243403/.

Mischke, J. (2018, January 26). Slovak PM: Visegrad group 'not black sheep' of EU. *Politico*. Accessed 19 February 2019. Retrieved from https://www.politico.eu/article/slovak-pm-visegrad-group-not-black-sheep-of-eu-robert-fico/.

National Cybersecurity and Communications Integration Center (2016, February 25). Alert Cyber-Attack Against Ukrainian Critical Infrastructure. *Official website of the Department of Homeland Security*. Accessed 19 February 2019. Retrieved from: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

NATO (2015). Energy as a Tool of Hybrid Warfare. *NATO Research Division Research Paper*, no. 113.

NATO (2017a). Energy Security: Operational Highlights. *NATO Energy Security Centre of Excellence*, no. 7.

NATO (2017b). Hybrid Threats: Overcoming Ambiguity, Building Resilience. *NATO Energy Security Centre of Excellence,* no. 11.

Nič, M. 2016, "The Visegrád Group in the Eu: 2016 as a Turning-point?", *European View,* vol. 15, no. 2, pp. 281-290.

Ostrowski, W., and Butler, E., eds. (2018). *Understanding Energy Security in Central and Eastern Europe: Russia, Transition and National Interest*. Routledge: New York.

Priday, R. (2018, March 10). The science that explains why a spat between Serbia and Kosovo made your oven clock run slow. *Wired*. Accessed 19 February 2019. Retrieved from https://www.wired.co.uk/article/clock-slow-europe-electricity-power-serbia-kosovo.

Proedrou, F. (2018). Revisiting pipeline politics and diplomacy: From energy security to domestic politics explanations. *Problems of Post-Communism, 65*(6), 409-418.

Prontera, A. (2017a). Forms of state and european energy security: Diplomacy and pipelines in southeastern europe. *European Security, 26*(2), 273-298.

Prontera, A. (2017b). *The new politics of energy security in the European Union and beyond: States, Markets, Institutions*. London: Routledge.

Puka, L., & Szulecki, K. (2014). The politics and economics of cross-border electricity infrastructure: A framework for analysis. *Energy Research & Social Science, 4*, 124-134.

Ratsiborynska, V. (2018). Russia's hybrid warfare in the form of its energy manoeuvres against Europe: how the EU and NATO can respond together? *NATO Research Division Research Paper*, no. 147.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics, 22*(3), 283-300.

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An Introduction to Cyber Peacekeeping. *Journal of Network and Computer Applications*, no. 114, 70-87.

Roggenkamp, M. M., Redgwell, C., Rønne, A., and del Guayo, I. (2016). *Energy Law in Europe : National, EU and International Regulation*. Oxford: Oxford University Press.

Silvast, A. (2017). Energy, economics, and performativity: Reviewing theoretical advances in social studies of markets and energy. *Energy Research & Social Science, 34*, 4-12.

Skokowski, D. (eds.) (2017). *Cyberseucirty of the Polish Industry: the Energy Sector*. Krakow: the Kosciuszko Institute.

Stegen, K. S. (2011). Deconstructing the "energy weapon": Russia's threat to europe as case study. *Energy Policy, 39*(10), 6505-6513.

Střeleček, F., Lososová, J., & Zdeněk, R. (2009). Comparison of subsidies in the visegrad group after the EU accession. *Agricultural Economics (Zemědělská Ekonomika), 55*(No. 9), 415-423.

Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber Security of a Power Grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, no. 99, 45-56.

Szalai, P. (2017, March 8). *Energy analyst: New nuclear reactors will heavily increase Hungary's debt.* Euractiv. Accessed March 25 2019. Retrieved from: https://www.euractiv.com/section/electricity/interview/energy-analyst-new-nuclear-reactors-will-heavily-increase-hungarys-debt/.

Szőke, D. (2018). Energy and Climate Security. In: *New Security Challenges from a Visegrad 4 Perspective*. Budapest: Institute for Foreign Affairs and Trade.

Szulecki, K. (2018). Conceptualizing energy democracy. *Environmental Politics, 27*(1), 21-41.

Szulecki, K., eds. (2017). *Energy Security in Europe: Divergent Perceptions and Policy Challenges*. Palgrave Macmillan: Cham.

Talus, K (2013). *EU Energy Law and Policy : A Critical Account*. Oxford, United Kingdom: Oxford University Press.

The Kosciuszko Institute (2018). *Polish National Cybersecurity System – Infographic*. Accessed 19 February 2019. Retrieved from https://ik.org.pl/en/polish-national-cybersecurity-system-infographic/.

The Kosciuszko Institute, Swiatkowska, J. eds. (2016). *NATO Road to Cybersecurity*. Krakow: the Kosciuszko Institute.

Toritti, J. (2010). "Impact Assessment and the Liberalization of the EU Energy Markets: Evidence-Based Policy-Making or Policy-Based Evidence-Making?" *JCMS: Journal of Common Market Studies* 48.4: 1065-1081.

Töró C., Butler E., and Grúber K., 2014, "Visegrád: The Evolving Pattern of Coordination and Partnership After EU Enlargement", *Europe-Asia Studies*, vol. 66, no. 3, pp. 364-393.

Ugrosdy, M. (2019). *Hungarian Foreign Policy Goals* workshop at the Institute for Foreign Affairs and Trade, Budapest, Hungary. 8 February 2019.

Van der Vleuten, E., and Lagendijk, V. (2010a). Interpreting Transnational Infrastructure Vulnerability: European Blackout and the Historical Dynamics of Transnational Electricity Governance. *Energy Policy*, no. 38, 2053-2062.

Van der Vleuten, E., and Lagendijk, V. (2010b). Transnational Infrastructure Vulnerability: The Historical Shaping of the 2006 European "Blackout". *Energy Policy*, no. 36, 2042-2052.

Van Dijk, T. A. (1993). Principles of critical discourse analysis. *Discourse & Society* , 4(2); 249-283.

Van Dijk, T. A. (1995). What is Political discourse analysis. *Key-note address Congress Political Linguistics.* Antwerp, 7-9 -December 1995. In Jan Blommaert & Chris Bulcaen (Eds.), *Political linguistics.(pp. 11-52).* Amsterdam: Benjamins.

Verloo, M.M.T. 2006, "Multiple inequalities, intersectionality and the European Union", *The European Journal of Women's Studies,* vol. 13, no. 3, pp. 211-228.

Visegrad Group. (2019). International Visegrad Fund. Accessed 19 February 2019. Retrieved from: http://www.visegradgroup.eu/.

Wen, X., Wei, Y., & Huang, D. (2012). Measuring contagion between energy market and stock market during financial crisis: A copula approach. *Energy Economics, 34*(5), 1435-1446.

Xiang, Y., Wang, L., & Liu, N. (2017). Coordinated Attacks on Electric Power Systems in a Cyber-Physical Environment. *Electric Power Systems Research*, no. 149, 156-168.

Xiang, Y., Wang, L., & Zhang, Y. (2018). Adequacy Evaluation of Electric Power Grids Considering Substation Cyber Vulnerabilities. *International Journal of Electrical Power & Energy Systems*, no. 96, 368-379.

Xie, J., Stefanov, A., & Liu, C. C. (2016). Physical and Cyber Security in a Smart Grid Environment. *WIREs Energy Environ*, no. 5, 519-542.

Yergin, D. (1988). *Energy security in the 1990s*. New York: Council on Foreign Relations.

Zachova, A., Zgut, E., Zbytniewska, K., and Yar, L. (2018, May 07). Is Visegrad Group Ready for cyber-attacks? *Visegradinfo*. Accessed 02 March 2019. Retrieved from http://visegradinfo.eu/index.php/80-articles/560-is-visegrad-group-ready-for-cyberattack.

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*. Accessed 19 February 2019. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zetter, K. (2017, January 10). The Ukrainian Power Grid Was Hacked Again. *Vice Motherboard*. Accessed 19 February 2019. Retrieved from https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report.

Appendix A

Publisher →			WEC (2016)	EECSP Report (2017)	Kapersky (2017)	Kosciuszki Inst. (2017)	CEER (2018)	ETIP (2018)	HCSS (2019)
Publication →		Total	World Energy Perspective	Cyber Sec in the Energy Sector	ICS cyber-security	Cybersecurity of the Energy Sector	Cybersecurity Report on EU Electricity	Digitalization	Geopolitics of the Energy Transformation
Structural Changes	Increased digitisation of grid management	7	X	X	X	X	X	X	X
	Increasingly integrated and interoperable systems	7	X	X	X	X	X	X	X
	Decentralized (remote) supply chain	6	X	X		X	X	X	X
	Diversification in equipment and tech	6	X	X	X	X	X	X	
	Increase in communication	6	X	X	X		X	X	X
	Automated demand response programs	4		X		X		X	X
Changes in risk profile	Customer data privacy breaches	7	X	X	X	X	X	X	X
	Economic espionage	6	X	X	X	X	X		X
	Data corruption	6		X	X	X	X	X	X
	Loss of control and understanding[2]	6	X	X	X	X	X	X	
	Loss of control of key equipment	5	X	X	X	X			X
	Software corruption	5	X	X	X	X		X	

[2] Due to increased specialization and outsourcing, elements of software or hardware can have been developed outside of the company that uses or applies the final system. Sometimes authorization settings have not been adapted to grant the operational engineers access to edit or update software. This decreases the level of control and the level of understanding of the engineers over the final system and ultimately increases the level of risk.

	Increase in entry points for breaches	4	X	X		X			X
			WEC (2016)	EECSP Report (2017)	Kapersky (2017)	Kosciuszki Inst. (2017)	CEER (2018)	ETIP (2018)	HCSS (2019)
			World Energy Perspective	Cyber Sec in the Energy Sector	ICS cyber-security	Cybersecurity of the Energy Sector	Cybersecurity Report on EU Electricity	Digitalization	Geopolitics of the Energy Transformation
	Physical damage	3	X			X			X
	Weakest link problem	2		X		X			
	(threat of) extortion	1	X						
	Monoculture risk	1	X						
Required Response	Stimulate risk awareness culture	7	X	X	X	X	X	X	X
	Standards and regulations	6	X	X	X	X	X	X	
	International cooperation	5	X	X		X	X		X
	Knowledge and skill building	5	X	X	X		X	X	
	Information sharing	5	X	X		X	X	X	
	Set up a response framework	4		X		X	X	X	
	Value chain security coordination	3	X	X			X		
	Promote market consolidation of cybersec products	1				X			
	Coordinated impact assessments	1					X		