gases

MDPI

Article

Transnational Cyber Governance for Risk Management in the Gas Sector: Exploring the Potential of G7 Cooperation

Megghi Pengili [1,*] and Slawomir Raszewski [2]

[1] School of Politics and International Studies, University of Leeds, Leeds LS9 2JT, UK
[2] The Royal Docks School of Business and Law (RDSBL), University of East London, London E16 2RD, UK; s.raszewski@uel.ac.uk
* Correspondence: m.pengili@leeds.ac.uk

Abstract: At the Group of Seven (G7) summit held on 13–15 June in 2024, the Group's leaders committed to establishing a collective cyber security framework and reinforcing the work of the cyber security working group to manage the risks targeting energy systems. Likewise, oil and electricity, and natural gas rely on complex and interdependent technologies and communication networks from production to consumption. The preparedness to handle cyber security threats in the energy infrastructures among decision makers, planners, and the industry in a concerted manner signifies that cyber security is becoming more appreciated. Therefore, considering the ambition and achievement of the G7 countries towards energy and cyber sovereignty, this paper's focus and research question aims to explore the potential existence of the cyber governance alliance in the gas subsector within the G7. The objective of this paper is twofold. First, it explores the potential of the G7, the world's seven largest advanced economies, to lead on a nascent cyber governance for risk management in the gas sector. The qualitative analysis conducted through the institutional analysis and design method examines up-to-date data involving mainly state actors. Second, by drawing on LNG, one of the world's fastest growing energy types in the coming decades, the paper points out the need for further research on the transnational governance operating through public–private engagement to address the cyber risks to gas systems. While the paper makes an empirical contribution to the field of security governance and a practical contribution to security consulting, its limitations rely on the necessity to also conduct a quantitative enquiry, which would necessitate, among others, a review of the literature in the G7 countries, and a group of researchers from academia and practitioners to obtain a sense of the cyberspace in the energy reality.

Keywords: cyber risk management; gas sector; G7; transnational cyber governance

Citation: Pengili, M.; Raszewski, S. Transnational Cyber Governance for Risk Management in the Gas Sector: Exploring the Potential of G7 Cooperation. *Gases* **2024**, *4*, 327–350. https://doi.org/10.3390/gases4040019

Academic Editor: Ben J. Anthony

Received: 30 July 2024
Revised: 18 September 2024
Accepted: 18 October 2024
Published: 23 October 2024

1. Introduction

Government agencies, retailers, banks, and airlines called an emergency on 19 July 2024 due to the CrowdStrike outage. Flights were grounded, payment systems were interrupted, and media networks were unable to operate normally due to the computer shutdown. U.S. cyber security firm CrowdStrike explained that a faulty system update caused the outage [1]. Though there is no specific report on the energy system, energy infrastructures are still interconnected to transport and data, and, supposedly, the energy sectors might have been impacted to a degree.

Today's societies are highly dependent on digital technologies. Cyber/ICT security and resilience are and will remain critical to societies' economic and social well-being, and national and international security. Governments do not have the means to understand and respond to risks from a breach of the vital infrastructures. Therefore, governments increasingly rely on cooperation and collaboration with the private sector beyond their borders. In 2023, Europe accounted for 32% of cyber incidents, North America represented 26%, and Asia–Pacific saw 23% [2]. Like other governments around the globe, G7 countries

too have advanced public–private partnerships (PPPs) for the cyber security of the energy sector beyond their borders.

Cyber security has risen to a position of great significance in the new energy–economic–political domain. Protecting energy systems from cyber attacks and the need for cyber governance to manage what is one of the fastest growing energy types has been at the forefront of the energy policy of the world's largest energy economies, the G7. The establishment of a cyber security working group within the G7 featured among the core issues on its policy agenda for two reasons [3]. First, there is a growing realisation of the need to effectively respond to challenges that the energy sector has become exposed to, be it in a form of deliberate and malign (planned), or accidental (unplanned) cyber threats. Second, the need for transnational cyber security governance frameworks and multilateral norms is crucial, as these underscore the importance of global cooperation in tackling threats that require a beyond-state response [4] (p. 407). For instance, digitalisation in the gas industry is premised on technological improvements (developing processes and changing workflows to improve manual systems) and enhancement of existing business models (provision of new revenue and value-producing opportunities). This digitalisation, however, is accompanied by a surging tide of cyber threats and attacks. With the ever-increasing volume of trade in LNG, the quest to safeguard critical energy infrastructures has never been more pressing, resulting in the need to invest in cyber security risk management as an organisational strategy and governance capacity (or the capacity to coordinate decision making) [5,6] (pp. 98–100). The need for investment in management, strategy, and capacity (MSC) is further necessitated by a highly volatile international system where geopolitical risks and uncertainties continue to impact business [7].

Russia's invasion of Ukraine, and related cyberattacks, continue to affect the energy sector. In parallel, the ongoing situation in Gaza is considered "to have a negative impact on the EastMed gas pipeline project, further disrupting the European energy market" [8]. Hacker activists, whose attacks of computer systems are driven by political reasons, are exploiting geopolitical uncertainties to advance their causes [9]. One of the widely publicised examples in this matter was the ransomware attack on the Colonial Pipeline in the United States (U.S.), which affected energy companies in Europe. In response to the hacktivist events or, indeed, other similar instances of computer-based forms of civil disobedience, there is a growing recognition of governments around the world prompting regulations to enforce law and sanction such activities [3]. With the attacks on Operational Technology (OT) against the energy sector having materialised soon after the start of the Russian invasion of Ukraine [10], 79% of oil and gas companies have become more aware of the potential OT vulnerabilities, thereby intensifying their investments and growing capabilities to focus on cyber security [10].

In this geostrategic scenario, the G7 countries: United States, United Kingdom, Canada, France, Germany, Italy, and Japan, have shared geo-economic interests, a level of trust, and also a good record of working together in the area of cyber governance. Cyber governance can be defined as the operation of decision-making processes aimed at risk control by means of increased participation, transparency, and accountability. In the international context, the participation of the G7 countries in the cyber governance domain positions the Group as a global player in establishing the energy digital agenda, helping it "to generate consensus within the U.S.-led Western camp on the conditions for coordinating with geopolitical foes such as China and Russia and reaching out to the Global South" [11]. The gas domain is of particular interest here since most of the G7 members are in various stages of either planning or constructing new gas power plants. For instance, Italy is seeking to increase its gas-to-power infrastructure by 12%, the U.K. by 23.5%, and Germany by 28% [12]. On the supply side, in the upstream and midstream of the gas value chain, the U.S. continues to play a pivotal role ranking among the top exporters at USD 63.9B [13,14] while operating the fourth largest natural gas pipeline in the world [12]. On the demand side, the largest economies of the G7 rank among the top importers of gas including Japan (USD 54.7B), France (USD 24B), and the U.K. (USD 21.2B) [13,14]. Additionally, Germany acts as a

major gas transit hub, including new additions to its gas infrastructure, most notably the recently commissioned LNG regasification capacity. In 2021, 46.1% of gross German gas imports were exported to neighbouring countries [15]. Rachel Waldholz et al. [16] predict a consolidated autonomy of Germany in the gas sector, presumably due to Germany's recent diversification away from piped gas to LNG. Lastly, Italy is becoming an important playmaker in the gas sector as it is considering its involvement with the East Med Pipeline (EMP) connecting the gas fields in the Eastern Mediterranean via Cyprus to Greece [17]. The EMP is not just an energy project but is also considered a major geopolitical endeavour with far-reaching implications. If constructed, the pipeline will help connect to new sources of supply while diversifying Europe's external imports, with the project's capacity estimated to cover about 10% of Europe's gas supply needs [18].

Regarding the cyber capabilities potential of the G7, digital competitiveness is among the top nine priorities of the G7 summits from 2018–2023 [19], which explains the national efforts of each of the countries to achieve cyber sovereignty. Save Japan and Canada, the G7 countries are bound by memberships of the North Atlantic Treaty Organization (NATO) and the European Union (EU). These memberships explain the adherence to joint cyber arrangements, and their engagements in projects such as the Italian Leonardo Industries in the NATO Global Security Operation Centre, which conducts operations and draft solutions to cyber threats [20,21]. G7 members are among the top 20 countries with the highest level of cyber capabilities as per the National Cyber Power Index in 2022 [22]. Based on the rankings of cyber military capabilities, the U.S., Australia, and Japan are among the top ten leaders [23]. The U.S. followed by the U.K. and Canada make up the Five Eyes Alliance (FVEY), an intelligence cooperative arrangement for sharing signal intelligence [24].

At the same time, France and Japan are two close FVEY cyber allies. Additionally, Germany seems to have succeeded in deploying a cyber branch as part of its military to combat increasing cyber aggression from Russia towards NATO members [25]. Of all the G7 countries, the Italian approach to cyber diplomacy favours international and multilateral forums. These include, for instance, the activities within the Organization for Security and Cooperation in Europe (OSCE), and those within the Ise-Shima Cyber Group of the G7, which concerns the declaration of the rules of responsible behaviour of states in cyberspace [26,27].

Considering the relationship between the G7 countries, and the strategic importance of the gas sector to the G7 economies, the resilience by design (the ability to anticipate and plan for potential problems) of its systems and infrastructures becomes imminent as a coordinated response to cyberattacks. Therefore, through the case of the G7, this paper explores the potential of transnational engagement in the governance of cyber risk management for the gas sector. While existing research captures the geopolitical tensions related to energy sources and cyber security dynamics, there has been little attempt to capture the dynamics around the transnational governance of cyber management in the gas sector.

For this purpose, this article is structured as follows. After this introduction, Section 2 is a literature review of the interplay between security dynamics, cyberthreats, and energy–cyber power balances in the gas sector. Section 3 then develops the methodology, which is framed around the institutional analysis and design (IAD) approach to the effectiveness of transnational governance for cyber risk management. Section 4 analyses the information gathered by navigating the national cyber capabilities of each country and the rise of public–private partnerships as a proactive and active response to cyber attacks. The discussion continues in Section 5, utilising the extracted data we obtained from the national level of analysis in order to reflect on risk management of shared critical energy infrastructures through transnational engagement, such as those initiated between Germany and Italy [28] or the US and Japan [29]. The Conclusion brings up the key findings pointing out the performance of transnational governance in enhancing resilience to cyberthreats in the gas sector, through public–private partnership engagement in cyber security, by making a

contribution to the application of the transnational cyber governance concept to the case study of critical gas infrastructures.

2. Ghost in the Pipeline: Natural Gas Security Dynamics, Energy-Cyber Power Balances, and Cyberthreats

This section introduces the background literature that drives the underlying question of this paper: does a cyber governance alliance in the energy sector exist within the G7? We start by reviewing the strategic context in which cyber governance operates by looking at the security dynamics in the gas sector and the quest of G7 nations to be energy sovereign. Additionally, by recognising that disruptive technological innovations open attackers' pathways, and the dependence of energy security on these technologies, we then observe the issue of energy–cyber power balances and cyberthreats.

The approach to energy supply security has been conventionally premised on two objectives. First, the EU policy has sought to project and export the EU rules and regulations (acquis communautaire) to its immediate neighbourhood by means of legal and institutional frameworks. Second, the EU policy has encouraged diversification of energy supplies, by source and route, by means of institutional support for infrastructural projects [30] (see p. 2). The EU's strategy on energy has been underscored by the complexities associated with other energy resources such as coal, oil, and nuclear sources, either due to market or policy concerns. Consequently, natural gas has been a dominant policy tool for the EU member states to meet the policy targets set at the EU level, thereby enhancing energy security [31].

At the time of writing, there is an ongoing development of new approaches to address the climate policy on decarbonisation as exemplified by France's gas system operator, GRTgaz, in cooperation with Norway's state-owned Equinor, aimed at the development of infrastructure for CO_2 transportation [32]. In Germany, a major shift away from the new Ostpolitik strategy premised in its economic rationale on reliance on cheap Russian gas supplies, in the post-2022 Nord Stream context, has dramatically made way for 'Zeitenwende', or the end of an (energy security) era, in which greater sovereignty over security of supplies is being addressed [33].

The 2022 invasion of Ukraine by Russia triggered a significant energy crisis in the EU 27 and the U.K., leading to profound changes in their natural gas supply, transmission, and consumption dynamics. Russian gas supplies to the EU and the UK experienced a dramatic decline by 87.8%, while LNG imports into the EU expanded exponentially, becoming the largest gas supply source with an increase from 20.7% to 37.5% of the total gas supply [34]. In these critical circumstances, the EU has been compelled to address its energy security through alternative supplies, including more flows of LNG and options to boost domestic production and use its regassification structure [35–37]. The natural gas supply disruption experienced following the sabotage of the Nord Stream 1 and 2 pipelines [38] affected the EU as the world's top importer of piped natural gas in many ways. Equally, the sheer extent of the disruption has impacted the international LNG market, leading to growth and greater infrastructural expansion. Almost overnight, the energy supply security has transformed: gas supply dependence on Russia was curtailed in nominal terms, while the partnership with the U.S. in LNG has suddenly become an important part of Europe's pursuit for energy security. With the launch of US LNG export projects, gas businesses in Europe have embraced the idea of having the U.S. supplies as a potential partner, before the dramatic disruption of Russian gas supplies, in an attempt to diversify sources and routes of supply [39] (see p. 53). In the post Nord Stream supply world, infrastructure development decisions in the U.S. are likely to have an impact on EU energy security. For instance, should the US interrupt the construction of new LNG terminals, as announced earlier in 2024, the EU market would face disruptions and would turn to coal as the main energy source [40] (see p. 52).

The energy crisis regarding gas supplies from the Russian Federation has exposed underlying differences in the national energy strategies of key EU member states, such as

France and Germany. These differences have made it harder to achieve a unified climate policy as set out by ambitious EU targets [33].

Similarly to other G7 members, Italy's renewed energy security approach is one that seeks to seize new opportunities in its geographical proximity. Thanks to its Mediterranean location, Italy's renewed approach aims to turn it into an energy bridge between Europe and Africa. Their renewed energy policy seeks to contribute to achieving the EU's economic and energy policy-related objectives. However, Italy will also need to take into consideration future gas demands in the EU and coordinate accordingly with Germany [41].

Energy security is also framed by energy interdependence dynamics distilled from the relationship between the importer and the exporter. It is of common knowledge that natural gas can be transported only through pipelines or in liquefied form, in the presence of liquification and regasification capacities, transported in special LNG carriers. Natural gas pipelines require a direct connection between the exporter and importer of this energy commodity. As a consequence, the relationship between the two actors involved in the natural gas trade is often described as energy interdependence, i.e., the importing country needs the energy commodity, while the exporting country needs a safe market where it can sell its energy commodity. Energy interdependence in the natural gas sector is a key issue, as this phenomenon influences the foreign policy of the countries involved in the commercial relationship and, in particular, their energy security policies. While the era of energy interdependence between the EU and Russia is ending, the EU's new energy era arises "where security, sovereignty, and solidarity shape a revised geopolitical energy landscape" [42] (p. 2).

Sovereignty applies to the cyberspace as well, according to Eric Jensen [43]. In international relations, there is a widespread consensus that cyber power could influence the balance between the U.S. and its allies, and China and Russia. Cyberspace challenges the principle of state sovereignty [44] as it questions where to draw the line for the harm caused. Qualifying a cyberattack as an act of war could trigger the victim state's right of self-defence to attack [45,46]. States "could see cyberattacks as acts of war, while academics appear to agree that a cyberattack on critical national infrastructure that causes damage and can be attributed to a state constitutes a violation of the Law of Armed Conflict" [47] (p. 11).

The link between energy sovereignty and cyber sovereignty is expressed through the United Nations (UN) principles on cyber sovereignty and the protection of information-critical infrastructures (ICT)[1]. For a country to achieve energy sovereignty, that country should also have cyber sovereignty. To achieve both goals, investment must be made in the security and resilience of energy infrastructures. These infrastructures are critical to modern economies, yet, at the same time, the very same infrastructures appeal to cybercriminals with their malign activities, as well as to unfriendly state actors. The new energy–cyber nexus provides a context which requires states to maintain sovereignty in the cyberspace, considering that energy systems rely on digital technologies and "these technologies can impact directly on state sovereignty" [47] (p. 9). As the war in Ukraine continues, the energy infrastructure around the world is increasingly at risk, especially at a time when the power and utility of artificial intelligence (AI) technologies are growing and, thus, blurring the traditional divide between IT infrastructure and Operational Technology (OT), thereby making the risk a reality [48,49]. A case in point is the attack on the Colonial Pipeline and the oil-refining hub of Amsterdam–Rotterdam–Antwerp (ARA) [50,51].

The energy infrastructures of all countries are at risk, according to Dragos' report released in 2019 [52]. Cyberattacks are tools for power in the energy domain. Traditional oil, natural gas, electric, and others can no longer be viewed as separate; a threat to one entity is a threat to all energy infrastructures. Among the most dangerous threat activities targeting gas and oil companies are XENOTIME and DYMALLOY [53,54]. Both can achieve long-term and persistent access to IT and OT for intelligence collection and possible future disruption events [52]. Cyberattacks are becoming more sophisticated in identifying vulnerabilities and causing disruptions [55]. Moreover, land-based LNG facilities could

be physically attacked. Since LNG is used as a fuel destined to power plants, heating, military bases, and other uses, disruption of LNG shipping or storage poses additional downstream risks, especially in more LNG-dependent regions [56]. Figure 1 introduces a cyber attack on an oil and gas system, while Table 1 describes the main cyber risks and their characteristics. Figure 2 displays the most important tools that can directly target the infrastructure domain.

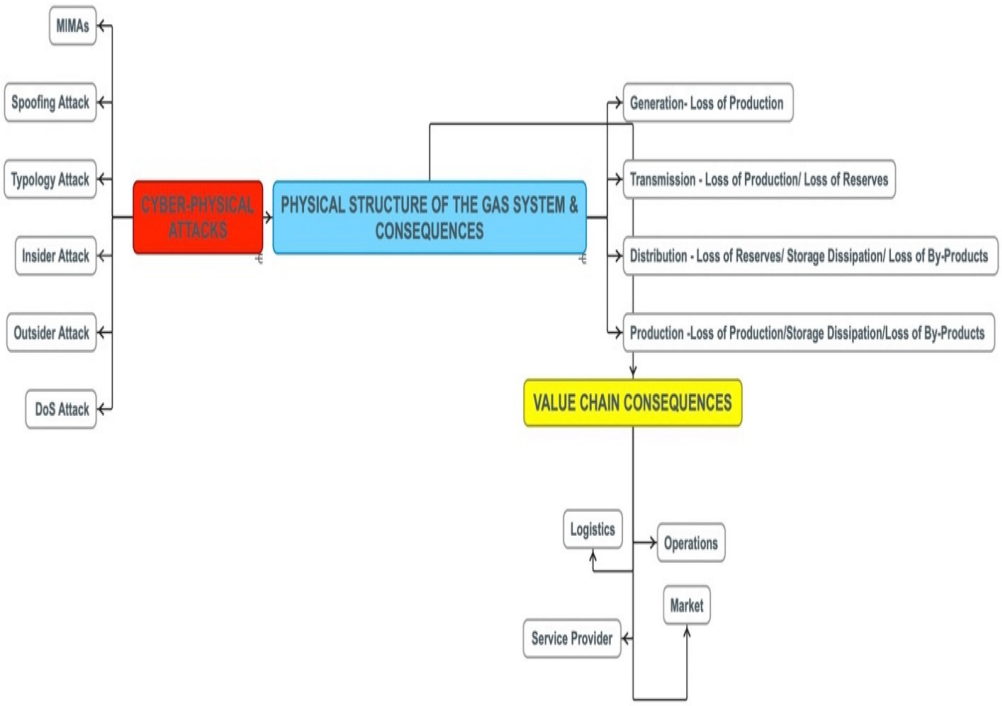

Figure 1. Attack graph on gas cyber physical system and consequences for value chains. **Source:** adopted by the authors, 2024, from [57,58].

Table 1. Cyber risks and their characteristics. **Source:** authors 2024.

Risks	Characteristics	Examples
Communication [59]	Relates to the risk message Risk source Message receiver	Difficulty in understanding and transmitting the message Inaccurate information that affects decision making Media have also been shown to cause problems through a lack of care in interpreting and reporting
Escalation phases [60]	Targeting (decision making) Destabilisation (multiple operations) Coercion (hybrid warfare)	Creating and exploiting infrastructure dependency: cyber espionage, exploiting legal rules and institutions Infiltrations, water space violation Paramilitary organisations attack
Cyberweapons [60,61]	Computer; worm; trojan back-door; modular virus, modular malware; remote attacks;	Industrial system damage; cyber espionage in the energy sector; covert intelligence monitoring
Cyber attacks that propagate from cyber to the gas pipeline physical domain [57]	Before SCADA responds Preventing SCADA response	A failure of a cyber node controlling power grid functionality propagates from cyber to power to gas pipeline systems
Others	Theft of core intellectual property; disruption or destruction of a physical plant; biased communications by leadership	

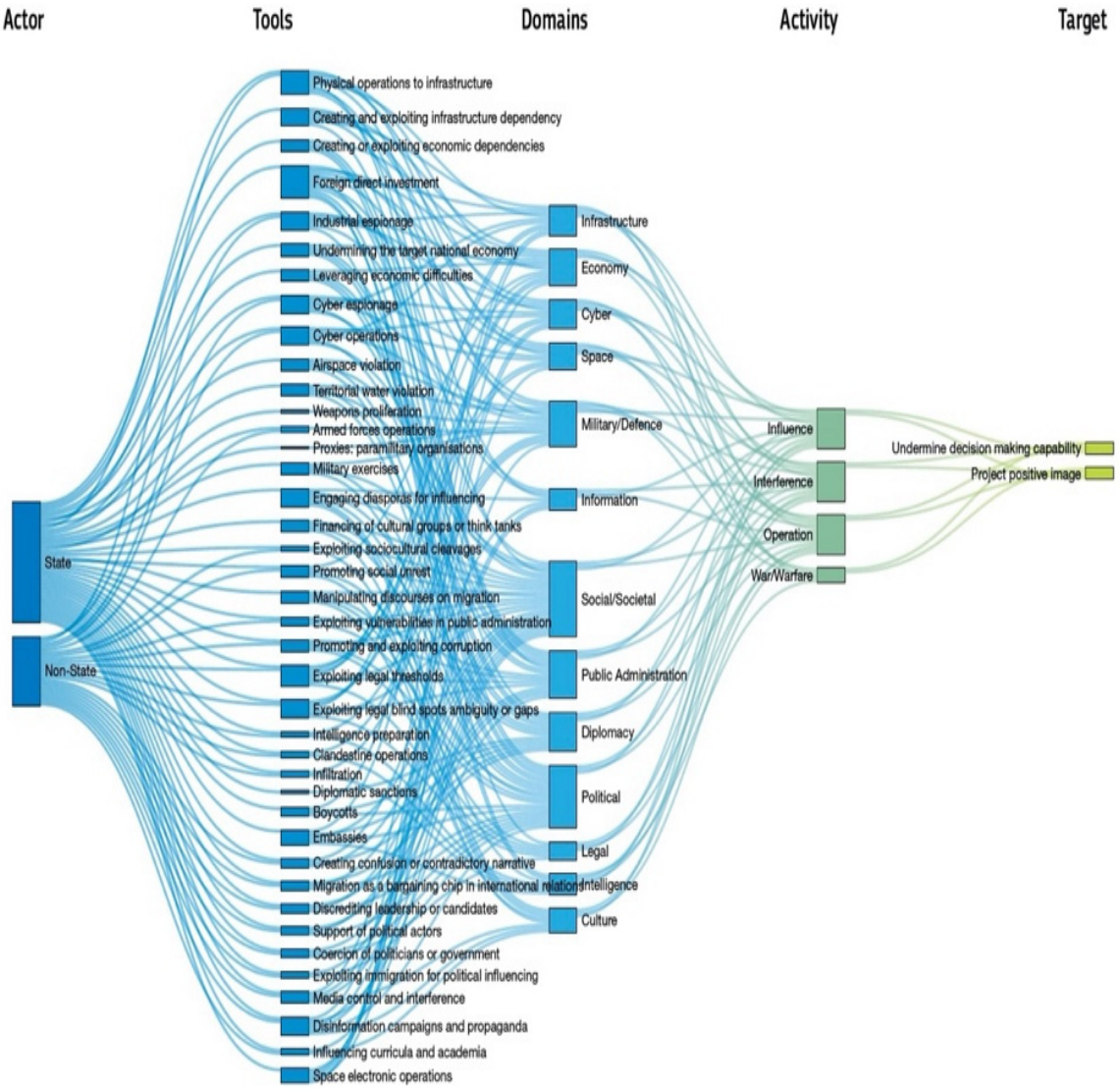

Figure 2. Actors and tools that can directly target the infrastructure domain. **Source**: adopted from [58].

Reflecting on the considerations above, the cyber risks are multiple, hybrid, and complex. Ian Kilovaty suggests that these attacks breach three cyber security principles: confidentiality, integrity, and availability [62]. These principles guide the risk management platforms and strategies to protect the assets. Confidentiality ensures that assets are only viewed by authorised parties. Integrity signifies that an asset is modified only by authorised parties, while the system's availability refers to uninterrupted access to assets by authorised users [59]. Interruption of access may compromise the entire system and, thus, infringement on any of the above principles represents a cyberthreat, the nature of which falls under five main groups: communication, escalation phases, cyberweapons, structure vulnerabilities, and others as summarised in Table 1. The upcoming section outlines the methodology employed to investigate our research question: is transnational cyber governance of the energy sector a reality within the G7?

3. The Path to Transnational Governance: An Institutional Analysis Design Approach

Our case study is characterised by the complexity of strategic contexts of the G7 members, their political and economic national objectives, energy and cyber power balances, and the rapid technological progress, where nations are increasingly reliant on digital systems and networks to power their economies and safeguard their national security [63].

The principles of cyber security governance within the G7 were laid out initially in 2016 in the non-binding document which addressed cyber risks in the financial sector. They serve as the building blocks upon which an entity can design and implement its cyber security strategy and operating frameworks, informed by its approach to risk management and culture [64]. The document conceptualises a cyber governance committed to continuous learning by updating and reviewing strategies and methodologies for cyber risk management and cyber training for personnel. This commitment to learning and improvement is fundamental for the effectiveness of risk management policy in critical energy infrastructures. Therefore, the establishment of a clear governance framework specifying the decision-making roles of the public and private sectors, trust, and a common "level of understanding of what is strategic, operational, and technical" [65] (p. 35) is crucial.

Based on these considerations, and with reference to the information generated from the previous two sections, the discussion moves to a brief introduction of the IAD approach and the data that inform the next two sections.

3.1. Institutional Analysis Design

This section applies the Institutional Analysis Design (IAD) framework to examine the potential of G7 cyber governance on risk management in the gas sector. Developed by Margaret M. Polski and Elinor Ostrom in 1999 [66], the method here is constructed within a single-case study design, the Group of Seven. At the same time, IAD integrates the process tracing technique to capture the evolution of cyber governance within the G7, i.e., process tracing helps us to explore and explain how, and to what extent, cyber governance in the energy sector can exist or become a reality. In essence, the method applied focuses on tracing the process that identifies institutional change, which we carry out in this paper, and the actors that design policy interventions to generate institutional outcomes, such as policy effectiveness and innovations in the governance [63,67].

IAD is a method of analysis that is based on schematic organisation of the policy activities to design new policy interventions, to evaluate policy effectiveness, and initiate policy changes [63]. Institutional thinking has been, for a long time, concerned with seeking to clarify the conditions, processes, and variability in change over time. Change is a process that has implications for both the institutions and their final target(s) [68], which for this paper is a nascent form of transnational cyber governance. The concept of transnational cyber governance, which refers to the coordination and regulation of cyber activities across national borders, builds on a complex geostrategic and institutional setting, in the confluence of cyber's and energy's virtual and physical domains. Because it involves knowledge from multiple actors, levels of decision making, and complex policy and social situations, the IAD framework provides a common basis for integrating all these elements to explain institutional change [66], an expression of which is new forms of governance [69]. Additionally, IAD allows us to navigate the potentiality of transnational cyber governance pioneered by the G7, since like-minded political actors with similar expertise backgrounds will approach problems in much the same way and, therefore, socialisation reinforces this governance's effectiveness [70]. Walter Powell and Paul DiMaggio argue that institutional actors "define power and choices; while they are certainly a result of human activity, they are also a result of historical and cultural circumstances" [71] (p. 19).

The application of IAD expands on six aspects of the policy problem: "physical and material conditions, community attributes (culture), rules-in-use, action arena, patterns of interaction, and outcomes" [66] (pp. 16–17). This comprehensive approach, with its ability to logically connect each aspect to the other, provides a robust understanding of the policy problem. The IAD framework's analytical power instils confidence and a sense of security, as it can effectively dissect and analyse the complexities of the policy problem.

The physical and material conditions reflect those events and circumstances that influence transnational engagement in cyber risk management and determine institutional arrangements in important ways. The community attributes refer to the characteristics of the G7 community, such as the degree of common understanding, political communication,

economic and political features, shared interests, and "the extent to which potential participants' values, beliefs, and preferences about policy oriented strategies and outcomes are homogeneous or heterogenous" [66] (p. 22). Rules-in-use include the source of rules, formal and informal norms, regulations, and the laws in place which justify a policy action, such as cyber security frameworks, cyber management strategies, and cybercrime laws. The operational activity of all policy actors is observed in the action arena, which explores their decision-making capabilities that decide on the patterns of interaction, such as the structural characteristics of a policy action, and the behaviour of actors in that structure. Flowing from the patterns of interaction, we can determine the policy performance or effectiveness to reduce uncertainties in the outcomes.

3.2. Data

To answer the research question on the potential for transnational cyber governance for risk management in the gas sector, our institutional analysis design consulted around 120 sources. These sources fall into five categories per topic: G7 dynamics, cyber security, public–private partnerships in cyber, and the cyber protection of critical energy infrastructures. Each category expands on reports, journal articles, books and book chapters, government publications, institutional research papers, newspapers, and blogs. The data collection and analysis are organised in four blocks, as illustrated in Figure 3. The first block surveys the cyber risk management process for critical infrastructures and how it is organised nationally. The second block explores available data about national capabilities for cyber management in the United States, United Kingdom, Canada, France, Germany, Italy, and Japan. We selected information that is narrowly focused on cyber governance at the national level, regulatory frameworks, cyberspatialities and decision making, and international engagements of these countries at NATO, the EU, OSCE, and G7 levels. The third block screens information about the public–private partnership cyber governance at the national level of each country in the cyber protection of critical energy/gas infrastructures. The last data set reflects on the partnership/cyber governance structure within the G7 grouping of nations, which is increasingly about energy and its interdependent infrastructures.

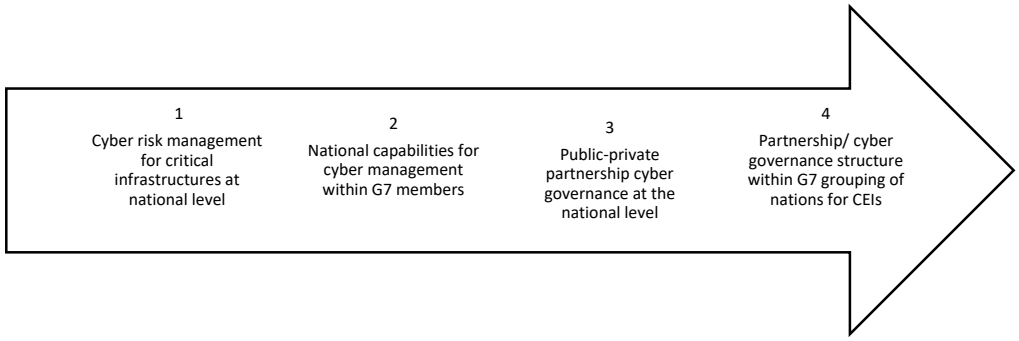

Figure 3. Data description. **Source:** authors 2024.

4. Assessing National Capabilities for Cyber Risk Management

While the previous sections portrayed the nexus of energy–cyber security within the G7 context by navigating the gas security dynamics and defining the threats that target the cyber security framework of the gas sector, this section provides a technical and analytical overview of the cyber risk management framework by navigating the national cyber capabilities of each country and the rise of public–private partnership as a proactive and active response to cyber attacks. The analysis starts with risk management frameworks, explores the national cyber governance capabilities, and concludes with the performance of public–private partnerships (PPPs) in cyber security.

4.1. Cyber Risk Management

Risk management is a comprehensive technical–analytical process that helps an organisation to map the full range of risks it faces by examining the relationship between the motivation of the attack, types of information targeted, stakeholders involved, and potential damages. The risk management process is instrumental in helping organisations, institutions, or industries produce a more accurate risk map, which takes into account the attacker's vision. Table 2, a common example adopted in most national cyber security strategies, serves as a tool to support decision making in the process of drafting counter-risk strategies. Starting from left to right, the management process defines the typology of the attackers listed under Players. The next columns identify the motivation and goal of the attack. The last column determines the consequences and effects of this attack.

Table 2. Risk assessment table. **Source**: adapted by the authors from [54].

Source of Threat	Motivation	Goals	Consequences	Risk Impact—TBD
Government/Proxies	Espionage/Military	Reputation Damage	Human Lives	Insignificant
Criminal Actors	Espionage	IP Theft/Corruption	IP Theft	Minor
Non-state Actors	Pre-mission Intelligence	Money Extortion	Destruction of Critical	Major
Illiterate users	Sabotage	Leak of sensitive	Energy Infrastructure	Critical
Business competitors	Economic Profit	information	Sanctions	Catastrophic
	Revenge	Services Disruption	Disinvestment	

Each entity should consider its goals and priorities and adjust how it may apply guidance accordingly [72] in five phases: identify, protect, detect, respond, and recover. These five steps of formulating a response are orientated towards principles pertinent to the infrastructure's operational activity, human behaviour, organisational awareness, practical regulatory framework, and resilience [72] (p. 13).

Comparing the national cyber security strategies of the United States, United Kingdom, Canada, France, Germany, Italy, Japan, NATO's cyber strategy, and the EU's cyber strategy, it is possible to conclude that the lifecycle of risk management to cyber security infrastructure is to counter "the full spectrum of cyber threats at all times". To mitigate the asymmetrical threat of cyberattacks, risk management guidelines emphasise that organisations remain technologically advanced and agile, and invest in joint civil–military capabilities [73–76]. The process can be summarised in these guidelines:

- Develop cyber security processes: the organisation should develop cyber capabilities to identify, protect, detect, respond, and recover;
- Education and training staff for cyber security for risk analysis and risk evaluation;
- Upgrade and maintain a system to mitigate cyber risk;
- Create a cyber security culture to raise awareness and encourage proactive behaviour;
- Draft resilience by design through sectoral methodologies and system approaches for interconnected critical energy infrastructures [77].

While these principles guide the response to threats, the concept of resilience by design underscores the need for organisations to invest in cyber governance resources. Such an investment is crucial to ensure robustness, autonomy, responsiveness, and preparedness. Robustness is about resistance to shocks, autonomy refers to the stand-alone operational mode, and the last three principles consist of efficient and proactive strategies to mitigate future risks [77].

4.2. National Cyber Governance Capabilities[2]

The German Cyber Security Strategy 2021 is written in a considerably different way than the other strategies considered here. It identifies a large number of cyber security topics to be addressed. One particular aim also addresses cyber governance directly. The unique structure of the German strategy, which shifts from mere statements to a complete framework of activities, underscores its strong focus on governance [78]. Germany is ranked

13th in the Global Cybersecurity Index 2020 [79], and 5th among the top 20 countries with the highest budget in digital defence with a budget of USD 7.9 billion [80]. According to the International Institute for Strategic Studies (IISS) report on Cyber Capabilities and National Power [81], France's president holds the highest authority in cyber decisions with support from the Defence and National Security Council (CDSN), ComCyber, and the Cyber Defence Executive Committee.

Cyber intelligence in France is mainly produced by the General Directorate for External Security (DGSE), and all French intelligence agencies have cyber capabilities and specific cyber responsibilities [81]. Although France's cyber-intelligence capabilities are strong in certain regions such as North Africa, they could benefit from a more global reach as is the case in the US and the UK. Unlike the FVEY countries, French intelligence services support extensive industrial espionage by French industry [81,82]. Additionally, the government has entered a three-year agreement with eight manufacturing companies to enhance cyber security [83] and is engaged in enhancing public–private cooperation on cyber security through a "national cyber-security campus" [84]. In the 2020 Global Cybersecurity Index, compiled by the International Telecommunication Union, France ranked ninth out of 175 countries [79], and sixth among the top 20 countries with the highest budget in digital defence with a budget of USD 5.5 billion [80].

In Italy, cyber security governance is outlined in the Quadro Strategico Nazionale (QSN), National Cybersecurity Strategy 2022–2026 [85], and Italy's Cloud Strategy. Decision-making powers remain with the prime minister, the Interministerial Committee for the Security of the Republic, the National Cybersecurity Agency, the Technical CISR (CISR Tecnico, CISR-T), and the Cyber Security Unit (Nucleo Sicurezza Cibernetico, NSC) [86]. Italian cyber and energy companies supply information services to operators of critical infrastructures and are required to report network violations to the Cyber Security Unit, while the national Computer Emergency Response Team (CERT Nazionale or IT-CERT) was established in 2015 to comply with the 2013 EU strategy for "An Open, Safe and Secure Cyberspace" [86]. In the 2020 Global Cybersecurity Index compiled by the International Telecommunication Union, Italy was ranked 20th out of 175 countries [79], and 12th among the top 20 countries with the highest budget in digital defence with a budget of USD 2.6 billion [80].

As per the INSS report [81], in 2014, Japan began restructuring its civilian command-and-control structure to resemble those of allied states like the US and the UK. However, coordination between the public and private sectors in Japan is not an element of resilience. The Cyber Security Strategic Headquarters (CSSH) and the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) are key organisations in Japan's cyber security efforts [81]. The country was ranked seventh in the 2020 Global Cybersecurity Index out of 175 countries [79], and fourth among the top 20 countries with the highest budget in digital defence with a budget of USD 10.1 billion [80].

In Canada, the prime minister has ultimate command over cyber organisations. The country follows a multi-stakeholder approach to cyber security policy. A cyber force was established in 2019 for offensive cyber warfare preparation [81]. Canada has the procedures and capability to protect its critical infrastructure from cyber threats. Public–private collaboration is another element of Canadian resilience, with the National Cross-Sector Forum[3]. In all of these critical infrastructure areas, there is significant interdependence between Canada and the US [4]. In the 2020 Global Cybersecurity Index, the country was ranked third out of 175 countries [79], and ninth among the top 20 countries with the highest budget in digital defence with a budget of USD 3.68 billion [80].

The United Kingdom's cyber capability direction is set out by the prime minister and cabinet members, implemented through the National Cyber Security Service (NCSS), National Cyber Security Centre (NCSC), and National Cyber Force (NCF) [81]. Unlike the US, the UK lacks a centralised military cyber command. The Government Communication Headquarters' cyber intelligence is bolstered by its partnership with the US and membership in the FVEY. The UK's armed forces benefit from these capabilities and have their

own cyber-intelligence assets, including interception activities, intelligence assessment, and rapid integration of cyber information with other military assets [81,87]. The efficacy of that ecosystem was reflected in the UK being ranked second out of 175 countries in the 2020 Global Cybersecurity Index [79], and third among the top 20 countries with the highest budget in digital defence with a budget of USD 10.6 billion [80].

The United States is a global leader in promoting multi-stakeholder governance of cyberspace security, influenced by its liberal political culture and institutions [88]. The federal political system fosters a pluralistic approach to cyber governance [81]. Various executive channels, including the National Security Council, guide cyber policy. Collaboration between intelligence agencies, the private sector, and universities is integral to cyber defence. Despite significant efforts, the US recognises the ongoing challenges and vulnerabilities in safeguarding its critical information infrastructure in cyberspace [81]. The US is ranked first among the top 175 countries in the 2020 Global Cybersecurity Index [79], and first among the top 20 countries with the highest budget in digital defence with a budget of USD 78.3 billion [80]. Table 3 summarises the cyber governance capabilities for the countries of the Group of Seven.

Table 3. National cyber governance capabilities of the G7 countries. **Source**: authors, 2024.

Country	Important Governance Structures	Strategic Documents	Budget 2024 (USD Billion)	Global Cybersecurity Index Ranking (2020)	Membership
United States	National Security Council Department of Defence Intelligence agencies Private Sector Universities US Cyber Army Command Cyber industry	National Cybersecurity Strategy 2023 DoD Cyber Strategy 2023 International Cyberspace and Digital Policy Strategy, 2024	78.3	1	NATO FVEY
United Kingdom	National Cyber Security Service National Cyber Security Centre National Cyber Force CERT Cyber industry	National Cyber Strategy 2022 Government Cyber Security Strategy 2022 to 2030	10.6	2	NATO FVEY
Canada	Communications Security Establishment Canadian Armed Forces Canadian Security Intelligence Service Joint Force Cyber Command Canadian Centre for Cyber Security National CERT Cyber industry	Enterprise Cyber Security Strategy 2024 National Cyber Security Action Plan 2019–2024	3.68	3	NATO FVEY
Japan	Cyber Security Strategic Headquarters National Center of Incident Readiness& Strategy for Cybersecurity Defence Intelligence Headquarters Directorate for Signals Intelligence National CERT Military C4 Systems Command Japan Self-Defence Forces	Cybersecurity Strategy 2018 National Security Strategy 2022 National Defence Strategy 2022 Individual Partnership and Cooperation Programme in 2020	10.1	7	FVEY ally
France	Defence and National Security Council, ComCyber, Cyber Defence Executive Committee General Directorate for External Security National cyber-security Campus Private Sector National CERT	National Security Strategy 2022 Strategic Review of Cyber Defence	5.5	9	NATO EU FVEY ally

Table 3. *Cont.*

Country	Important Governance Structures	Strategic Documents	Budget 2024 (USD Billion)	Global Cybersecurity Index Ranking (2020)	Membership
Germany	Federal Min Interior Centre for Digitization & Capability Development Federal Office for Information Security Citizen-CERT Implementation Plan for Critical Infrastructure Military Cyber Branch Private Sector Cyber industry	White Paper 2016 National Cyber Security Strategy 2021	7.9	13	NATO EU
Italy	Interministerial Committee for the Security of Republic National Cybersecurity Agency Technical CISR, Cyber Security Unit Leonardo Cybersecurity Academy NATO-Leonardo Security Operation Centre IT-CERT National Cybersecurity Authority Public-private collaboration Cyber industry	Quadro Strategico Nazionale National Cybersecurity Strategy 2022–2026 Italy's Cloud Strategy	2.6	20	NATO EU

4.3. The Partnership Approach to Risk Management

Cyber security risks are not easily managed due to the complexity of information and communication technology (ICT). Cyber attacks may come from anywhere and at any time, entailing challenges to the management of cyber security risks. However, they also present an opportunity for innovations in the governance system [69]. PPPs are often seen as a form of potential cyber security governance or as an expression of institutional change that can significantly enhance flexibility and robustness by including a broader range of civil and private actors [89].

In all G7 countries, there is a positive government approach to engaging in a system of knowledge management with the private sector to learn how to build cyber resilience. The arrangements taken in all countries reflect that PPPs are in an agreement built on trust. Interestingly, the evidence here, also supported by studies of business relationships, shows that the PPPs' communication does not always have to be through formal dialogues; informal communication styles could also be employed to build trusted relationships [90] (see p. 90). The first level of the model regards building a sense of trust among the parties. The case of France and the cyber ecosystem of the United Kingdom show that PPPs "can be formed in two ways: collaborative (non-legally binding) or contractual (legally binding) agreements" [90] (p. 92).

Madeline Carr notes that "the public–private partnership in national cyber security is multifaceted" [91] (p. 45). Governments have diverse relations with industry and other non-state actors. However, within the cyber security discourse and defence generally, the public–private partnership is often referred to as a procurement method, ignoring its role in cyber governance. This happens even though "the core focus in the strategies is on the relationship between the government and the owners/operators of critical infrastructure, the protection of which is unequivocally and intrinsically linked to national security" [91] (p. 45).

The Cybersecurity Strategy of the European Union [76] points out that cyber resilience is achieved through practical cooperation between public authorities and the private sector. "Information and communications technology has become the backbone of our economic growth and is a critical resource on which all economic sectors rely. It now underpins the complex systems that keep our economies running in key sectors such as finance, health, energy, and transport. At the same time, many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information

systems" [37] (p. 2). Most of these systems are under the private sector's control, so the government's cooperation with industry is important [65,92].

Although PPPs are stimulating security cooperation through innovative governance tools, there are potential pitfalls from such partnerships as well [93]. For instance, the government can expand its presence and influence via PPPs in homeland security. This carries legal implications in terms of decision-making responsibility or accountability [91]. In other words, the fundamental uncertainty associated with cyber security seems to have opened up the space for contestation over "what to counter, and thus what counts as cyber-security knowledge" [94] (p. 1436). Moreover, there are situations in which national strategic interests do not match individual economic interests [91]. In this case, choosing between economic interests and the protection of critical energy infrastructure might be a problem.

By increasing our knowledge of cyber threats, we can effectively enhance cyber security overall. The PPP is a knowledge-management system that helps to exchange and share best practices, thereby fostering a common understanding among all stakeholders [26]. PPPs are responsible for important changes involving cyber governance and its institutions. These changes concern cyber capabilities, the structure of the cyber ecosystem, the support to educational infrastructures, and the assimilation of the Fourth Industrial Revolution (4IR) technologies to organisational aspects—altogether contributing to the resilience by design.

5. A Cyber Governance Alliance? Navigating CEI Interdependence and G7 Cyber Governance

The evidence built on the previous section on the national cyber governance capabilities, and the G7 members' approach to the PPP framework to cyber governance, allows us to export the analysis to an upper level: the transnational setting and the case of interdependent infrastructure.

As gas use for power generation increases, the interdependency between the gas and electricity sectors can create regional reliability challenges. Coordination between the two sectors remains an issue that requires further attention, and adding electric transmission capacity can assure the reliability and resilience of natural gas delivery and the electricity system [95] (see Figure 4). In line with this, the interdependence between infrastructures requires good knowledge from both sides engaged in the conflict to consider the existing connections between the infrastructures in order to avoid damage to other infrastructures, which may count as a war crime [96].

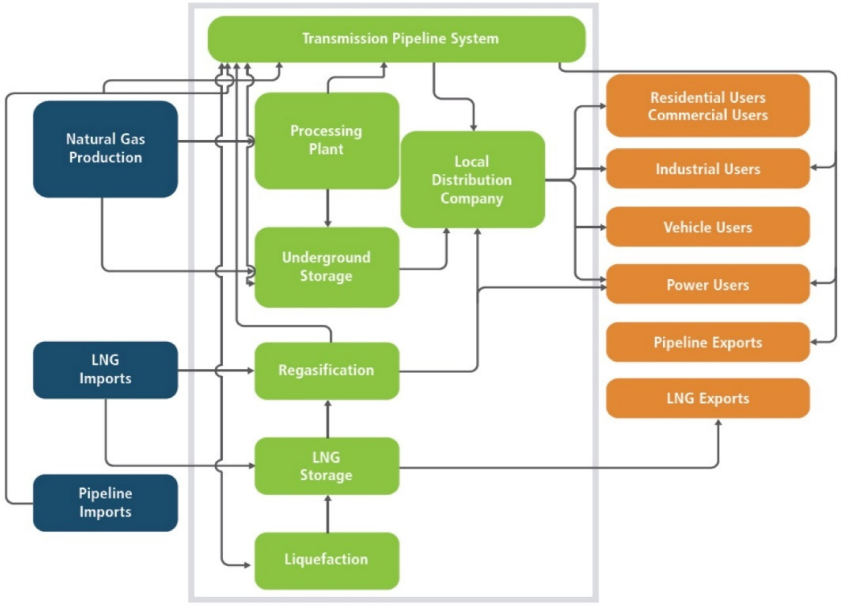

Figure 4. Scheme illustrating interdependency between gas and power systems. **Source**: adopted from [95].

Besides infrastructures shared between countries or interdependent between countries, there is also mutual interdependence between infrastructures within the same country [96]. An attack on one infrastructure impacts the functioning of other infrastructures. For example, electricity systems depend on resources supplied through gas or oil infrastructure. An attack on the oil or gas infrastructure will affect the electrical infrastructure. The research addressing infrastructure interdependencies started more than 15 years ago with the work of Steven M. Rinaldi et al. [97], yet technological evolutions have made it harder to notice the interdependencies between energy infrastructures. Too often, as identified during Superstorm Sandy, interdependencies are discovered only after the fact by the direct experience of cascading failures [98,99].

Infrastructure interdependencies can be physical, geographical, cyber, and logical. Infrastructures are physically dependent when each depends on a physical product of the other, whereas if a local environmental event can cause a change in their state, this is geographical interdependence. In the case of cyber interdependency, the state of an infrastructure is conditioned upon data, information, and technology. Lastly, logical dependence is created through decision-making processes made by the human factor [100] (see pp. 62–63). All typologies of interdependent infrastructures face failures, which can be classified as common cause, escalating, or cascading failures. Common cause failures happen when infrastructures are simultaneously affected by a common cause. For example, electric power disruptions instantaneously spread to disruptions in telecommunication components. Escalating failure is the domino cause and effect, while cascading failure refers to the disruption in one infrastructure which will cause disruption in several other infrastructures [96]. For example, an interruption in the supply of electricity will cause problems in the production of natural gas. Further along the cascading chain, enterprises that need natural gas for their operation will be affected.

These scenarios are common in a cyber warfare campaign. Cyber weapons are relatively inexpensive, and training in how to use them is not required. These low costs enable terrorist groups and countries with limited means to take part in cyber warfare. The fighting takes place on critical infrastructures and information systems that, in most cases, are also used by the civilian population [96]. The absence of regulatory legislation and an international convention on cyber warfare make it harder to determine what is permitted and what is forbidden in such a conflict. Though cyber attacks are becoming the new normal, "the response cannot be business as usual" [101]. In an area where many states are already actively involved, a treaty could complement existing rules and contribute to raising the global level of cyber security.

To address the cyber risk management of shared and interdependent infrastructures, scholarship offers modelling and simulation approaches to draft comprehensive transgovernmental strategies [102,103]. At the level of the EU, the Directive on Measures for a High Common Level of Cybersecurity across the Union urges member states to adopt the Network Information Security (NIS) strategies, designate CSIRTs ("Computer Security Incident Response Teams"), and create cooperation groups to facilitate the establishment of a CSIRTs network [92]. This demand is supported by the European Network and Information Security Agency (ENISA), which described the process of setting up such public–private expertise.

Growing cyber security concerns, arising from the deeply entangled geopolitical risks and uncertainties, have created an increased demand for risk management initiatives with the "potential to accelerate and promote international cooperation on the development of critical technologies, and to harness civilian innovation to solve critical security-related issues" [104] (p. 2). The knowledge that determines the potential of these initiatives affects the kind of partnerships between institutions and defence industries that steer those initiatives [69]. Through the vehicle of expertise, PPPs invest and allocate resources in an effort to create an effective comprehensive framework to identify and mitigate risks. This framework has the potential to provide resources for efficient coordination, directives

and regulation, standards for information sharing, identification of a set of protocols, and interoperable management tools [102].

Besides the contributions of scholarship and international bodies, the G7 countries are at the forefront of improving international collaboration on cyberspace issues. The United States, for instance, pioneered, in 2003, the adoption of several principles for protecting critical information infrastructures [105]. One of those principles concerned the coordination of investigations into attacks on countries' infrastructure in accordance with their domestic laws [105]. In 2016, the US further demonstrated its commitment to international collaboration by signing an agreement with the UK to advance its collaborative development of cyber capabilities [81].

The United Kingdom, in turn, has led cyber security initiatives in the United Nations, the European Union, and the Commonwealth [81]. For example, it has implemented international programmes under the UK-developed, Cybersecurity Capacity Maturity Model for Nations [106]. Additionally, the UK has long-standing international alliances with its FVEY partners, EU, and NATO members. These alliances provide a sense of reassurance and security in the face of cyber threats.

Canada seeks to shape the international cyber debate. Its 2019 National Cyber Security Action Plan outlined the roadmap to pursue national security interests through collaboration in the cyber security and cybercrime issues among stakeholders. This approach has seen the country participate in cyber security discussions, such as advancing discussions at the UN level on the adoption of international norms related to the safety of information and telecommunication infrastructures [107].

Italy's cyber diplomacy, as already mentioned in the introduction, is centred on the OSCE geo-space. One of the activities that has paved the way for the political and diplomatic actions in cyberspace was launched by the OSCE with the specific mandate to find confidence building measures (CBMs) suitable for cyberspace. CBM 1 and CBM 7 encourage OSCE-participating states to share information on their national structures, strategies, policies, and programmes responsible for cyber/ICT security, as well as their national views on various aspects of national and transnational threats to, and the use of, ICTs [108]. Luigi Martino [109] suggests that OSCE's framework for cyber diplomacy allows, ultimately, participating states to avoid the risk of misperception and mistrust in cyberspace.

In conclusion, cyber security threats are inherently cross-border and can only be effectively addressed through global cooperation aimed at reducing risks and fostering trust. Multilateral collaboration should prioritise the adoption of policy frameworks that promote international alignment and consistent cyber security measures. The G7 countries have a unique opportunity to drive this cooperation globally by advocating for the development and application of consensus-driven frameworks, standards, and best practices for risk-based cyber management. Embracing these internationally acknowledged approaches and frameworks for managing cyber risks can bolster economic security and fortify cyber resilience across the board. The G7 Cyber Expert Group (G7 CEG) established in 2015 [110], and the Institutional Arrangement for Partnership (IAP) endorsed in 2023, represents some steps towards a transnational cyber governance. Ultimately, trying to devise a new transnational governance would take time. The current geostrategic circumstances require a reconfiguration of existing institutions to meet the challenges of global governance.

Table 4 applies the key findings generated in Sections 4 and 5 to an IAD framework with the purpose of evaluating the potential for G7 cyber governance as a reality in the energy sector and, consequently, its effectiveness in reducing uncertainty and managing cyber threa.

Table 4. IAD Analysis of transnational cyber governance for risk management in the gas sector within G7. **Source:** authors, 2024, elaborating upon the IAD elements in [66].

IAD Domain	G7
Policy Analysis Objective & Analytic Approach	Analysis Objective: Transnational Cybergovernance in Energy Analytic Approach: Cybergovernance capabilities of each G7 member Multistakeholder approach to cybergovernance at national level Exploring international engagements in Cybergovernance of G7 members Energy & Cyber power balances Energy security domain of interest for G7 members
Physical World	Most industrialised economies Strength of cyber capabilities: Tier 1 (US, UK, Canada, France). Tier 2 (Japan), and Tier 3 (Italy, Germany) Cyber risk management national frameworks between innovation and technology Cyber culture of the state Approach to safeguard national critical energy infrastructures Energy sovereignty depends on cyber sovereignty Top gas exporters: US, Canada Top gas importers: UK, Japan, France EU gas transit hub: Italy and Germany Defence innovativeness
Community	Security Community-amalgamated and integrated characterised by political communications Members are bound by their allianceships Shared strategic and economic interests
Rules-in-use	National regulatory frameworks State-level agencies Methodologies for cyber risk management in the public and private sectors Offensive and defensive operations in France are clearly divided so the rules of engagements Decision-making is with state-level institutions, national cyber agencies and high-level leadership Some G7 countries have a military cyber command, others not.
Action arena	Integration of cyber units within government entities Public-private engagement is a preferred actor in the cyber governance. Industry forums
Patterns of interaction	Some countries have national cyber forums or campuses where private and public engage NATO structures EU structures OSCE Five Eyes Alliance Bilateral agreements Regional initiatives Informal and formal networks of cyber security communities Partnerships between state-level institutions and industry at NATO/EU level
Outcomes	The trust might be an issue amongst G7 governments for greater control over critical energy infrastructures Optimisation of cyber resources Greater expertise in cyber issues Governments agree on objectives and norms of cooperation Use transnational public-private partnerships to compensate the gap in cybergovernance Increase of clusters of transnational epistemic networks on cyber governance

6. Conclusions

The evidence that this paper consulted to address the research question on the G7 approach to a collective cyber governance to manage risks in the gas sector allows us to conclude that a transnational governance run through the public–private format is a strategic framework with the potential to become a reality. The main findings support our view to consider three patterns which address the research question of this paper: can the G7 pioneer a transnational cyber governance for the gas sector? These three patterns are

(a) the path dependence of the G7 countries since the end of WWII, which contributed to its establishment in 1976; (b) energy security being an essential policy domain for most, if not all, or for at least 50 years; and (c) the 'community of practice' approach to innovation and technology.

Currently, the G7 engagements and fields of priority this paper looked at reveal (a) the attempt of the Group to institutionalise modes of collective action for managing transnational issues by involving state and non-state actors, which is justified by (b) their cyber governance capabilities. Generally, most transnational governance initiatives under the PPP framework are carried out through indirect governance, such as delegation and orchestration [111], as exemplified by the G7 countries' activity. The governance of transnational cyber risk management in the gas sector will become increasingly relevant, and discussions in the area must continue. Cybercrime knows no borders; therefore, strategies, means, tools, and human capital are required, along with interdisciplinary expertise and a variety of strategic cultures that understand uncertainty and know how to mitigate its consequences. Considering that energy infrastructures and systems are the playground of shared interests and shared gains, only a coordinated response to defend those infrastructures has the potential to succeed.

In connection with our findings above, we will advance the following recommendations. First, while the findings reveal that the G7 has been the forum to coordinate policy actions for more than 50 years, this homogeneity can be transferred to the design of new frameworks and approaches that promote raising a new generation of professionals. These professionals can play a role in developing transnational cyber risk management policies. Second, considering their national and collective experiences in the cyber security policy, the G7 should refocus on cyber security as the 'new' fabric of energy security. The Group members can lead the way in aligning cyber security strategies among themselves and with like-minded nations. This entails establishing standards, sharing best practices, and coordinating responses to cyber threats. Lastly, the G7 has the resources to champion a more inclusive approach to strengthen the resilience of critical energy infrastructures and systems by improving the formal and informal networks/communities of practice. A more inclusive approach involving critical stakeholders beyond national borders, including influential industry players in cyber security initiatives, will ensure resilience through cooperation. Cyberattacks on essential energy infrastructures will continue to mainly impact the economy sector; hence, the G7 should consider transnational cyber governance as a litmus test for its capacity to act as an essential global actor in addressing cyber security concerns impacting the energy systems.

While this work is an introduction to further research in cyber governance for the energy sector, we think that more work needs to be conducted by both academics and practitioners, with a quantitative approach as well, to address two major challenges. The first is to bridge cyber security with the energy–commercial divide between the G7 countries. The second challenge is to build cyber expertise for foreign policy practitioners engaged in the energy sector. A competent cyber expertise would address, among other things, the issue of trust between the civil and military cyber forces engaged in the protection of the critical energy infrastructures. Both issues could be part of a simulation game which observes how cyber governance affords the reality of the cyberspace in the energy sector.

In conclusion, this work makes two contributions: empirical and practical. Empirically, this work challenges the literature on security governance on (a) the explanatory power of network theory and (b) on the concept of authority. The context of cyber governance does not find explanation only through the network governance approach, which views PPPs as collaboration practices. In the context of cyber governance, partnerships combine logics and governance structures from both the institutions and private sectors in response to competing institutional demands [112]. Currently, partnership structures in security and defence (cyber included) operate as stakeholder arrangements, legal regimes, and norms.

That said, for an effective response to complex questions, state and non-state actors cooperate as public–private institutions where policymaking and power are coordinated

among parties [79], challenging, therefore, the concept of a state's absolute authority on defence matters. This power coordination allows us to bring back in James Rosenau's concept of 'spheres of authority' (SOA) according to which governance extends beyond the jurisdiction of states [113,114]. The paper suggests two illustrations to this observation: the authority within the PPP platform, which is expressed through national cyber capabilities, and the authority of the national cyber ecosystem. Both cases are an expression of the participatory arrangements, which do not provide spaces for authoritative control from either side.

The second contribution is to security consulting. By analysing the national capabilities and assessing afterwards, on that basis, the potential of a transnational cyber governance, the paper offers an embryonic platform for auditing cyber governance in the energy sector. Recognising the importance of cyber governance for the organisation's strategies and objectives, security consultancy is often challenged with resolving issues, which require transnational cooperation and expertise to meet the high security demands of energy facilities.

Author Contributions: Conceptualization, M.P. and S.R.; methodology, S.R. and M.P.; analysis M.P. and S.R.; resources, M.P. ans S.R.; writing—original draft preparation, M.P. and S.R.; writing—review and editing, S.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created.

Acknowledgments: The authors wish to thank Nikitha Aithal, of Victoria University of Wellington, for her assistance in improving the written text of this and an earlier version of the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

Notes

[1] For the principles of UN Charter and Cyber Operations see UNGA (2013), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, UN Doc A/68/98, paras 19–20; UNGA (2015), Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, para 28(b). The 2015 UN GGE also agreed 11 voluntary and non-binding norms, rules, and principles of responsible state behaviour in the ICT environment. UN Doc A/68/98, paras 19–20; UNGA (2015), Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, para 28(b). The 2015 UN GGE also agreed 11 voluntary and non-binding norms, rules and principles of responsible state behaviour in the ICT environment.

[2] For study purposes, the overview of national cyber capabilities in this section is based on the Cyber Capabilities and National Power: Net Assessment [76].

[3] For more on the Canadian strategy to protect Critical Infrastructures. URL: https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240614/19-en.aspx (accessed on 28 June 2024).

References

1. Williams, P.; Molnar, N.; Springer, G. Northeast Ohio Impact of Global Tech Outage Extends to Utilities, Hospitals, Government. 2024. Available online: https://eu.beaconjournal.com/story/news/local/2024/07/19/crowdstrike-outage-imacts-some-akron-services/74467780007/ (accessed on 21 July 2024).
2. IBM. *X-Force Threat Intelligence Index 2024*; IBM: Armonk, NY, USA, 2024.
3. Greig, J. G7 Countries Vow to Establish Collective Cybersecurity Framework for Operational Tech. 2024. Available online: https://therecord.media/countries-vow-to-establish-cyber-collective (accessed on 8 July 2024).
4. Rosenzweig, P. International Governance Framework for Cybersecurity. *Can.-United States Law J.* **2012**, *37*, 405–432.
5. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. *Busines Horiz.* **2021**, *64*, 659–671. [CrossRef]
6. Mizrak, F. Integrating Cybersecurity Risk Management into Strategic Management: A Comprehensive Literature Review. *Res. J. Bus. Manag.* **2023**, *10*, 98–108. [CrossRef]
7. KPMG. Top Risks 2023: The Bottom Line for Business. 2023. Available online: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/02/top-risks-thought-leadership.pdf (accessed on 25 July 2024).

8. Alcamo, I. The Energy Security Dynamics Around the Israel-Hamas War and Their Implications for the Future of the Gaza Marine Gas Field. 2024. Available online: https://iari.site/2024/06/11/the-energy-security-dynamics-around-the-israel-hamas-war-and-their-implications-for-the-future-of-the-gaza-marine-gas-field/ (accessed on 18 June 2024).
9. Sabin, S. Hackers Make Their Mark in Israel-Hamas Conflict. 2023. Available online: https://www.axios.com/2023/10/10/hackers-ddos-israel-hamas-conflict (accessed on 4 June 2024).
10. Bouhdada, J. Digital Transformation: Building Cyber Resilience in the Oil and Gas Industry. 2023. Available online: https://www.worldoil.com/magazine/2023/december-2023/features/digital-transformation-building-cyber-resilience-in-the-oil-and-gas-industry/ (accessed on 8 July 2024).
11. Council on Foreign Relations. What Does the G7 Do? 2024. Available online: https://www.cfr.org/backgrounder/what-does-g7-do#chapter-title-0-6 (accessed on 18 July 2024).
12. Pastukhova, M. Over-Reliance on Gas Delays G7 Transition to Net-Zero Power. 2024. Available online: https://www.politico.eu/sponsored-content/over-reliance-on-gas-delays-g7-transition-to-net-zero-power/ (accessed on 8 July 2024).
13. Observatory of Economic Complexity. Natural Gas Liquified-Latest Trends. 2023. Available online: https://oec.world/en/profile/bilateral-product/natural-gas-liquefied/reporter/are/ (accessed on 8 July 2024).
14. U.S. Energy Information Administration. Japan's Energy Overview. 2023. Available online: https://www.eia.gov/international/content/analysis/countries_long/Japan/#:~:text=Because%20it%20has%20no%20international,crude%20oil%20to%20meet%20demand.&text=Japan%20was%20the%20world%E2%80%99s%20fifth-highest%20energy%20consumer%20in%202021 (accessed on 8 July 2024).
15. Wolff, G.; Gritz, A. Gas and energy security in Germany and central and Eastern Europe. 2023. Available online: https://dgap.org/en/research/publications/gas-and-energy-security-germany-and-central-and-eastern-europe-0 (accessed on 9 July 2024).
16. Waldholz, R.; Wehrmann, B.; Wettengel, J. Ukraine War Pushes Germany to Build LNG Terminals. 2023. Available online: https://www.cleanenergywire.org/factsheets/liquefied-gas-does-lng-have-place-germanys-energy-future (accessed on 9 July 2024).
17. Onyango, D. EastMed Pipeline Remains on EU's New List of Common Interest Projects. 2023. Available online: https://www.pipeline-journal.net/news/eastmed-pipeline-remains-eus-new-list-common-interest-projects (accessed on 2 July 2024).
18. Mikkelsen, D. Oil and Gas-How the EastMed Pipeline Strengthens European Energy Security. 2023. Available online: https://www.oilandgasmiddleeast.com/business/insights/how-the-eastmed-pipeline-strengthens-european-energy-security (accessed on 1 July 2024).
19. Hamre, J.J.; Cha, V.; Benson, E.; Bergmann, M.; Murphy, E.L.; Welsh, C. "Bending the Architecture"—Reimagining the G7. 2024. Available online: https://www.csis.org/analysis/bending-architecture-reimagining-g7 (accessed on 2 July 2024).
20. Corriere della Sera. Missione Sicurezza. 2019. Available online: https://specialistudio.corriere.it/leonardo-si1/cyber-security-chieti/ (accessed on 3 December 2022).
21. Leonardo. Training. 2022. Available online: https://www.leonardo.com/en/news-and-stories-detail/-/detail/leonardo-ecosystem-sole24ore (accessed on 9 November 2022).
22. Voo, J.; Hemani, I.; Cassidy, D. *National Cyber Power Index 2022*; Belfer Center: Cambridge, MA, USA, 2022.
23. Lowy Institute. Asia Power Index 2023-Cybercapabilities. 2023. Available online: https://power.lowyinstitute.org/data/military-capability/signature-capabilities/cyber-capabilities/ (accessed on 8 July 2024).
24. Haan, K.; Aditham, K. What Is The Five Eyes Alliance? Forbes, 4 June 2024. Available online: https://www.forbes.com/advisor/business/what-is-five-eyes/ (accessed on 25 July 2024).
25. Antoniuk, D. Germany to Launch Cyber Military Branch to Combat Russian Threats. 2024. Available online: https://therecord.media/germany-to-launch-cyber-military-unit-russia (accessed on 8 July 2024).
26. Zan, T.D.; Giacomello, G.; Martino, L. Italy's Cybersecurity Architecture and Critical Infrastructure. In *Routledge Companion to Global Cyber-Security Strategy*; Manjikian, M., Ed.; Routledge: London, UK, 2021; pp. 121–131.
27. DeCode39. First G7 Cyber Group Agrees on Info-Sharing to Defend Democracies. 2024. Available online: https://decode39.com/9058/first-g7-cyber-group-agrees-on-info-sharing-to-defend-democracies/ (accessed on 1 July 2024).
28. Feld, S.D.L. Germany, Austria, Italy to Develop the Southern Hydrogen Corridor. Simson: "Key project for decarbonization". 2024. Available online: https://www.eunews.it/en/2024/05/30/germany-austria-italy-to-develop-the-southern-hydrogen-corridor-simson-key-project-for-decarbonization/ (accessed on 12 June 2024).
29. Weatherby, C. EastWestCenter-Next Steps for US-Japan Collaboration on Energy Infrastructure. 2020. Available online: https://www.eastwestcenter.org/sites/default/files/private/ewc_api-n145_final.pdf (accessed on 12 June 2024).
30. Raszewski, S. When One Door Closes, Another Opens: How the Failure of the Turkey—Austria Natural Gas Pipeline Project Has Led to Recovery, Resilience and Scalability of Successor Projects. *Energy Policy* **2022**, *167*, 112978. [CrossRef]
31. Aalto, P.; Temel, D.K. European Energy Security: Natural Gas and the Integration Process. *J. Common Mark. Stud.* **2014**, *52*, 758–774. [CrossRef]
32. Sassi, F. LinkedIN-Francesco Sassi's Post. 2024. Available online: https://www.linkedin.com/posts/sassi-francesco_norway-france-are-planning-a-major-activity-7217120596197842945-I2I5?utm_source=share&utm_medium=member_ios (accessed on 14 July 2024).

33. Lafrance, C.; Wehrmann, B. EnergyPost.Eu-Russia's War Has Exposed France and Germany's Energy Policy Differences. Can It Also Bring Them Together? 2023. Available online: https://energypost.eu/russias-war-has-exposed-france-and-germanys-energy-policy-differences-can-it-also-bring-them-together/ (accessed on 10 June 2024).
34. Zhou, C.; Zhu, B.; Halff, A.; Davis, S.J.; Liu, Z.; Bowring, S.; Arous, S.B.; Ciais, P. Europe's Adaptation to the Energy Crisis: Reshaped Gas Supply; Transmission-Consumption Structures and Driving Factors from 2022 to 2024. 2024. Available online: https://essd.copernicus.org/preprints/essd-2024-173/essd-2024-173.pdf (accessed on 16 July 2024).
35. International Energy Agency. World Energy Investment 2024. 2024. Available online: https://iea.blob.core.windows.net/assets/60fcd1dd-d112-469b-87de-20d39227df3d/WorldEnergyInvestment2024.pdf (accessed on 9 July 2024).
36. Energy Security Sentinel. An Interactive Study of Geopolitical Risk and Energy Prices. 2024. Available online: https://storymaps.arcgis.com/stories/6e44901bfd7e421ca06cacc7c6e9ea1d (accessed on 4 June 2024).
37. European Commission. Eighth Report on the State of the Energy Union. 2024. Available online: https://energy.ec.europa.eu/topics/energy-strategy/energy-union/eighth-report-state-energy-union_en# (accessed on 4 June 2024).
38. Bowden, M. The Atlantic 'The Most Consequential Act of Sabotage in Modern Times: The Destruction of the Nord Stream Pipeline Curtailed Europe's Reliance on Russian Gas. But Who Was Responsible? 2023. Available online: https://www.theatlantic.com/international/archive/2023/12/nord-stream-pipeline-attack-theories-suspects-investigation/676320/ (accessed on 25 July 2024).
39. Hecking, H.; Schulte, S.; Vatansever, A.; Raszewski, S. *Options for Gas Supply Diversification for the EU and Germany in the Next Two Decades, Cologne*; EWI-EUCRS: London, UK, 2016.
40. Sassi, F. Stop ai Nuovi Terminal di Gnl Negli Usa: Quali Implicazioni per la Sicurezza Energetica Europea, Rome: Il Senato. 2024. Available online: https://www.researchgate.net/publication/382762146_Stop_ai_nuovi_terminal_di_gnl_negli_Usa_quali_implicazioni_per_la_sicurezza_energetica_europea (accessed on 24 July 2024).
41. Münchmeyer, M.; Raimondi, P.P. Between Security and Transition: Prospects for German-Italian Energy Cooperation. *IAI Comment.* **2023**, *23–66*, 1–7.
42. LaBelle, M.C. Breaking the era of energy interdependence in Europe: A multidimensional reframing of energy security, sovereignty, and solidarity. *Energy Strategy Rev.* **2024**, *52*, 101314. [CrossRef]
43. Jensen, E.T. Cyber Attacks: Proportionality and Precautions in Attack. *Int. Law Stud.* **2013**, *89*, 198–2017. [CrossRef]
44. Franzese, P.W. Sovereignty in Cyberspace: Can It Exist? 2009. Available online: https://go.gale.com/ps/i.do?id=GALE%7CA212035708&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00948381&p=AONE&sw=w&userGroupName=anon~d5434b46&aty=open-web-entry (accessed on 18 June 2024).
45. Nyman, M. Cyber Attacks as Armed Attacks? The Right of Self-Defence When a Cyber Attack Occurs. 2022. Available online: https://www.diva-portal.org/smash/get/diva2:1751329/FULLTEXT01.pdf (accessed on 18 June 2024).
46. Oorspronga, F.; Ducheine, P.; Pijpers, P. Cyber-attacks and the right of self-defense: A case study of the Netherlands. *Policy Des. Pract.* **2023**, *6*, 217–239. [CrossRef]
47. Baezner, M.; Robin, P. *Cyber Sovereignty*; ETHZürich: Zürich, Switzerland, 2018.
48. Davis, D. 5 Big Cyberattacks in Oil and Gas. 2022. Available online: https://www.oilandgasiq.com/digital-transformation/articles/5-big-cyber-security-attacks-in-oil-and-gas (accessed on 2 July 2024).
49. Caversan, F. Mind the Gap: Bridging the Gap Between Information Technology and Operational Technology. 2024. Available online: https://www.forbes.com/sites/forbestechcouncil/2024/02/23/mind-the-gap-bridging-the-gap-between-information-technology-and-operational-technology/ (accessed on 5 June 2024).
50. CISA. The Attack on Colonial Pipeline: What We've Learned and What We've Done over the Past Two Years. 2023. Available online: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (accessed on 5 June 2024).
51. Klimburg, A.; Beato, F.; Kolaczkowski, M. Why the Energy Sector's Latest Cyberattack in Europe Matters. 2022. Available online: https://www.weforum.org/agenda/2022/02/cyberattack-amsterdam-rotterdam-antwerp-energy-sector/ (accessed on 5 June 2024).
52. Dragos. Global Oil and Gas Cyber Threat Perspective. 2019. Available online: https://www.dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf (accessed on 5 June 2024).
53. Industrial Cyber. Dragos Detects Escalation in Adversarial Capabilities, As Pipedream Threat Group Widens Attack Competence. 2023. Available online: https://industrialcyber.co/news/dragos-detects-escalation-in-adversarial-capabilities-as-pipedream-threat-group-widens-attack-competence/ (accessed on 26 July 2024).
54. Israel National Cyber Directorate. *Cyber Defense Doctrine Managing the Risk: Full Applied Guide to Organizational Cyber Defense*; ICND: Tel Aviv, Israel, 2021.
55. Smith, D.C. Cybersecurity in the energy sector: Are we really prepared? *J. Energy Nat. Resour. Law* **2021**, *39*, 265–270. [CrossRef]
56. Parfomak, P.W. Liquefied Natural Gas (LNG)Infrastructure Security: Issues for Congress. In *Liquefied Natural Gas: Security and Hazards*; Keller, B.W., Ed.; Nova Science Publishers, Inc.: New York, UK, 2009; pp. 49–85.
57. Wadhawan, Y.; Neuman, C. Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, Vienna, Austria, 28 October 2016.

58. Wang, Z.; Zhao, B.; Blum, R.S. An Overview of Cybersecurity for Natural Gas Networks: Attacks, Attack Assessment, and Attack Detection. In *Security in Cyber-Physical Systems Foundations and Applications*; Fink, G.A., Song, H., Jeschke, S., Eds.; Springer: London, UK, 2021; pp. 256–268.
59. Nurse, J.R.C.; Creese, S.; Goldsmith, M.; Lamberts, K. Trustworthy and Effective Communication of Cybersecurity Risks: A Review. The 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST 2011). In Proceedings of the The 5th International Conference on Network and System Security (NSS 2011), Milan, Italy, 8 September 2011.
60. Giannopoulos, G.; Jungwirth, R.; Hadjisavvas, C. *Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats*; EDA: Brussels, Belgium, 2023.
61. Hadjistassou, C.; Bratskas, R.; Koutras, N.; Kyriakides, A.; Charalambous, E.; Hadjiantonis, A.M. Safeguarding critical infrastructures from cyber attacks: A case study for offshore natural gas assets. *J. Pol. Saf. Reliab. Assoc. Summer Saf. Reliab. Semin.* **2015**, *6*, 115–124.
62. Kilovaty, I. Cybersecuring the Pipeline. *House Law Rev.* **2023**, *60*, 605.
63. Greco, E.; Marconi, F. Technological Innovation and Cybersecurity: The Role of the G7. *IAI Comment.* **2024**, *24*, 1–6.
64. European Central Bank. G7 Fundamental Elements of Cybersecurity for the Financial Sector. 2016. Available online: https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf (accessed on 27 July 2024).
65. ENISA. *Public Private Partnerships (PPP) Cooperative Models*; ENISA: Brussels, Belgium, 2017.
66. Polski, M.M.; Ostrom, E. An Institutional Framework for Policy Analysis and Design. 1999. Available online: https://ostromworkshop.indiana.edu/pdf/teaching/iad-for-policy-applications.pdf (accessed on 24 July 2024).
67. Skarbek, D. Qualitative research methods for institutional analysis. *J. Institutional Econ.* **2020**, *16*, 409–422. [CrossRef]
68. Vanhoonacker, S. The Institutional Framework. In *International Relations and the European Union*; Hill, C., Smith, M., Eds.; Oxford University Press: Oxford, UK, 2011; pp. 76–100.
69. Andonova, L. *Governance Entrepreneurs*; Cambridge University Press: Cambridge, MA, USA, 2017.
70. DiMaggio, P.J.; Walter, P. The iron cage revisited" institutional isomorphism and collective rationality in organizational fields. *Am. Sociol. Rev.* **1983**, *48*, 147–160. [CrossRef]
71. Powell, W.I.; Maggio, P.D. Introduction. In *The New Institutionalism in Organizational Analysis*; Powell, W.W., DiMaggio, P.J., Eds.; The University of Chicago Press: Chicago, IL, USA, 1991; pp. 7–61.
72. Newhouse, W.; Long, J.; Weitzel David Warren, J.; Thompson, M.; Yates, C.; Tran, H.; Mink, A.; Herriott, A.; Cottle, T. *Cybersecurity Framework Profile for Liquefied Natural Gas*; US National Institute of Standards and Technology: Washington, DC, USA, 2023.
73. Luiijf, E.; Besseling, K. Nineteen national cyber security strategies. *Int. J. Crit. Infrastruct.* **2013**, *9*, 3–31. [CrossRef]
74. NATO CCDCOE. NATO CCD COE National Cyber Security Strategy Guidelines. 2013. Available online: https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf (accessed on 4 June 2024).
75. Park, C.; Shi, W.; Zhang, W.; Kontovas, C.; Chang, C.H. Cybersecurity in the maritime industry: A literature review. In Proceedings of the International Association of Maritime Universities (IAMU) Conference, the 20th Commemorative Annual General Assembly, Tokyo, Japan, 30 October–1 November 2019.
76. European Commission and HR FASP. Joint Communication To The European Parliament And The EU's Cybersecurity Strategy for the Digital Decade. 2020. Available online: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (accessed on 4 June 2024).
77. European Defence Agency. Protection of Critical Energy Infrastructure (PCEI) Conceptual Paper. 2017. Available online: https://eda.europa.eu/docs/default-source/events/eden/phase-i/information-sheets/cf-sedss---protection-of-critical-energy-infrastructure-conceptual-paper.pdf (accessed on 3 July 2024).
78. Bundesministerium des Innern für Bau und Heimat. Cybersicherheitsstrategie für Deutschland 2021. 2021. Available online: https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-sicherheit-und-netze/it-sicherheit/cybersicherheitsstrategie-fuer-deutschland/cybersicherheitsstrategie-fuer-deutschland2021.pdf;jsessionid=3A70E0CBE8BA58D4304BB64CCD5EC4C0.live881?__blob=public (accessed on 10 June 2024).
79. International Telecommunication Union. *Global Cybersecurity Index 2020*; International Telecommunication Union: Geneva, Switzerland, 2020.
80. Raath, S. Cybersecurity Spending: How Much Are Countries Investing in Their Digital Defenses? 2024. Available online: https://www.expressvpn.com/blog/cybersecurity-spending/#20 (accessed on 6 June 2024).
81. IISS. *Cyber Capabilities and National Power: Net Assessment*; INSS: London, UK, 2020; Volume 1.
82. Blooshi, B.A.; Eksteen, A. Cyber Governance in the EU. In *European Cybersecurity in!Context A Policy-Oriented Comparative Analysis, Technoseries Paper 3*; Martino, L., Gamal, N., Eds.; European Liberal Forum: Brussels, Belgium, 2022; pp. 19–27.
83. G20 Research Group. *2019 G20 Osaka Summit Interim Compliance Report*; University of Toronto: Toronto, ON, Canada, 2019.
84. Pollet, M. France Launches "Cyber Campus" to Boost Cybersecurity Strategy. 2022. Available online: https://www.euractiv.com/section/cybersecurity/news/france-launches-new-cyber-campus-to-boost-cybersecurity-strategy/ (accessed on 1 July 2024).
85. Agenzia Cybersicurezza Nazionale. National Cybersecurity Strategy 2022–2026. 2022. Available online: https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza (accessed on 11 July 2024).

86. Hathaway, M.; Spidalieri, F. *Italy Cyber Readiness at a Glance*; Potomac Institute for Policy Studies: Arlington, VA, USA, 2016.
87. HM Government. National Cyber Strategy 2022 Pioneering a Cyber Future with the Whole of the UK. 2022. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf (accessed on 10 June 2024).
88. The Whitehouse. US National Cybersecurity Strategy. 2023. Available online: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed on 4 June 2024).
89. Andonova, L. Globalization, Agency, and Institutional Innovation: The Rise of Public-Private Partnerships in Global Governance. *Colby-Work. Pap. Econ.* **2006**, *3*, 1–62.
90. Manley, M. Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership. *J. Strateg. Secur.* **2015**, *8*, 85–98. [CrossRef]
91. Carr, M. Public–Private Partnerships in National Cyber-Security Strategies. 2016. Available online: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf (accessed on 14 January 2022).
92. The European Parliament and the Council. Directive 2022/2555 of The European Parliament and of The Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *Off. J. Eur. Union* **2022**, *L333*, 80–152.
93. Busch, N.E.; Givens, A.D. Public-Private Partnerships in Homeland Security: Opportunities and Challenges. *Homel. Secur. Aff.* **2012**, *8*, 1–24.
94. Christensen, K.K.; Petersen, K.L. Public–private partnerships on cyber security: A practice of loyalty. *Int. Aff.* **2017**, *93*, 1435–1452. [CrossRef]
95. US Department of Energy. Natural Gas. 2015. Available online: https://www.energy.gov/sites/prod/files/2015/06/f22/Appendix%20B-%20Natural%20Gas_1.pdf (accessed on 3 June 2024).
96. Menashri, H.; Baram, G. Critical Infrastructures and Their Interdependence in a Cyber Attack—The Case of the U.S. 2015. Available online: https://www.inss.org.il/wp-content/uploads/systemfiles/5_Menashri_Baram.pdf (accessed on 21 March 2023).
97. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, Understanding, and Analyzing Critical Infratsructures Interdependencies. *Control. Syst. Mag.* **2002**, *21*, 11–25. [CrossRef]
98. Portante, E.C.; Kavicky, J.A.; Craig, B.A.; Talaber, L.E.; Folga, S.M. Modeling Electric Power and Natural Gas System Interdependencies. *J. Infrastruct. Syst.* **2017**, *23*, 1–18. [CrossRef]
99. Bureau of Policy and Research. *Ten Years After Sandy Barriers to Resilience*; Bureau of Policy and Research: New York, NY, USA, 2022.
100. Hokstad, P.; Utne, I.B.; Vatn, J. (Eds.) Interdependency Modelling in Risk Analysis. In *Risks and Interdependencies in Critical Infrastructures*; Norwegian University of Science and Technology: Trodenheim, Norway, 2012; pp. 45–101.
101. Pawlak, P.; Géry, A. Why the World Needs a New Cyber Treaty for Critical Infrastructure. 2024. Available online: https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en&center=europe (accessed on 8 June 2024).
102. Settanni, G.; Skopik, F.; Shovgenya, Y.; Fiedler, R.; Carolan, M.; Conroy, D.; Boettinger, K.; Gall, M.; Brost, G.; Ponchel, C.; et al. A collaborative cyber incident management system for European interconnected critical infrastructures. *J. Inf. Secur. Appl.* **2017**, *34*, 166–182. [CrossRef]
103. Sonesson, T.R.; Johansson, J.; Cedergren, A. Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Saf. Sci.* **2021**, *142*, 105383. [CrossRef]
104. Fägersten, B.; Fiott, D.; Kleberg, C. *Navigating the Euro-Atlantic Defence Innovation Landscape*; Politea: Stockholm, Sweden, 2023.
105. Group of Eight. G8 Principles for Protecting Critical Information Infrastructures. 2003. Available online: http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf (accessed on 8 June 2024).
106. Global Cyber Security Capacity Centre. Cybersecurity Capacity Maturity Model for Nations (CMM). 2016. Available online: https://gcscc.web.ox.ac.uk/files/cmmrevisededition090220171pdf (accessed on 8 June 2024).
107. UNODA. Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security" (UNCLASSIFIED). 2021. Available online: https://documents.unoda.org/wp-content/uploads/2021/12/Canadian-position-paper-2021-25-OEWG-final-Dec-6_Annex-Gender-Considerations.pdf (accessed on 8 June 2024).
108. OSCE. 10 Years of OSCE Cyber/ICT Security Confidence-Building Measures. 2023. Available online: https://www.osce.org/files/f/documents/f/7/555999_1.pdf (accessed on 10 June 2024).
109. Martino, L. Give Diplomacy a Chance: OSCE's Red Lines in Cyberspace. 2018. Available online: https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2018_Martino_Luigi.pdf (accessed on 3 June 2024).
110. Home Treasury. About the G7 Cyber Expert Group (CEG). 2023. Available online: https://home.treasury.gov/policy-issues/international/g-7-and-g-20/g7-cyber-expert-group (accessed on 8 June 2024).
111. Abbott, K.W.; Genschel, P.; Snidal, D.; Zangl, B. Two Logics of Indirect Governance: Delegation and Orchestration. *Br. J. Political Sci.* **2016**, *46*, 719–729. [CrossRef]

112. Klijn, E.H. Public Private Partnerships: Deciphering meaning, message and phenomenon. In *International Handbook of PPP*; Hodge, G.A., Greve, C., Boardman, A.E., Eds.; Edgar Elgar: Cheltenham, UK, 2010; pp. 68–80.
113. Rosenau, J. Governance in the Twenty-first Century. *Glob. Gov.* **1995**, *1*, 13–43. [CrossRef]
114. Rosenau, J. Governing the ungovernable: The challenge of a global disaggregation of authority. *Regul. Gov.* **2007**, *1*, 88–97. [CrossRef]