УПРАВЛЕНИЕТО НА КРИТИЧНАТА ИНФРАСТРУКТУРА В ЕВРОПА: ПРЕДВИЖДАНЕ И СТРАТЕГИИ НА ПУБЛИЧНАТА АДМИНИСТРАЦИЯ ЗА ВЪЗНИКВАЩИ ЗАПЛАХИ ЗА СИГУРНОСТТА

Проф. д-р Рафаел Рьотингер, , raphael@roettinger.net
д-р Ойген Рьотингер

Резюме: В тази статия се разработва рамка за проактивно управление, насочена към защитата на критичната инфраструктура от нововъзникващи заплахи за сигурността. Чрез преглед на литературата и сравнителен анализ на казуси се идентифицират управленски практики, които укрепват публичната администрация посредством прогнозиране, координация, институционално учене и адаптивно управление на риска.

Ключови думи*:* критична инфраструктура, европейска сигурност, защита, управление

JEL: H83, H56, H54

DOI: https://doi.org/10.58861/tae.di.2026.3.01

THE GOVERNANCE OF CRITICAL INFRASTRUCTURE IN EUROPE: ANTICIPATION AND PUBLIC ADMINISTRATION STRATEGIES FOR EMERGING SECURITY THREATS

Prof. Raphael Röttinger, PhD, raphael@roettinger.net
Eugen Röttinger, PhD

Abstract: This article develops an anticipatory governance framework for protecting critical infrastructure from emerging security threats. A literature review and comparative case studies identify governance practices that strengthen public administration through foresight, coordination, institutional learning, and adaptive risk governance.

Key words*:* critical infrastructure, European security, protection, governance

JEL: H83, H56, H54

DOI: https://doi.org/10.58861/tae.di.2026.3.01

1. Introduction

1.1 Background

The Russo-Ukrainian war has shown the vulnerability of critical infrastructure with the sabotage of the Nord-Stream pipelines in September 2022 (McCabe & Flynn, 2024). Modern societies depend on interconnected infrastructure like cables and pipelines for energy use (Pursiainen & Kytömaa, 2023), water (Kapucu et al., 2023) or transport and communication in general (Sonesson, Johansson & Cedergren, 2021). As these

infrastructures are interwoven, disruptions to networks, cables and pipelines reveal the vulnerability of the foundations of modern life's core functions (McCabe & Flynn, 2024).

The term “critical” refers to functions that are essential for supporting economic and social activities and can therefore be regarded as basic societal functions (Thistlethwaite & Henstra, 2026). Chang (2016) defines critical infrastructure as the combination of systems that sustain businesses, public institutions, and governments and enable the functioning of modern welfare states. More recent definitions have increasingly emphasized the indispensability of such systems that are prone to technical failure that put societies at risk (Pursiainen & Kytömaa, 2023). Sonesson, Johansson and Cedergren (2021) have shifted attention to the interdependencies of such infrastructures. This puts cascading effects into the limelight of attention once such infrastructures are at risk (McCabe & Flynn, 2024; Chang, 2016).

Consequently, and due to recent geopolitical power shifts and conflicts, critical infrastructure has evolved from being merely a subject of governmental attention (Chang, 2016) to becoming a central concern of resilience and security governance. This shift is fundamental for the governance of critical infrastructure and reflects the continuously evolving understanding of the role of public administration in securing and monitoring critical infrastructure (Sonesson, Johansson, & Cedergren, 2021). Consequently, the governance of critical infrastructure has become an increasingly important topic in research on infrastructure security (Kapucu et al., 2023; McCabe & Flynn, 2024).

An emerging threat is the increasing number of cyberattacks targeting energy infrastructure, reflecting the advancement of digital warfare and the profound digitalization of critical infrastructure that makes it more vulnerable and prone to attacks (Ruohonen, 2024; Pursiainen & Kytömaa, 2023; Mikac, 2023, Martínez & Durán, 2021, Russell, 2021). One striking example has been the ransom-ware attack of the Colonial Pipeline in 2021, compromising nearly half of the fuel supply of the US East coast (Beerman et al., 2023). Other cyberattacks were directed at companies like SolarWinds in 2020 that compromised around 18,000 other organizations, among them public organizations using the software of this company (Centre for Cyber Security, 2021). Equally the Kaseya attack put organizations using the company's software at risk (Ghanbari, Koskinen & Wei, 2026). Among the targets of such attacks are hospitals and public organizations (Ewoh & Vartiainen, 2024; Wasserman & Wasserman, 2022). Another type of threat is represented by hybrid threats that comprise acts of strategic disinformation, sabotage, or terrorism (Pestana & Sofou, 2024). Also, climate change poses severe risks to critical infrastructure and by so doing to humankind (Lomba-Fernández et al., 2019) but it also directly threatens the functioning of governing bodies (Zhang & van Valkengoed, 2025; Huddleston et al., 2022). This became obvious during the Ahrtal floods in 2021 in Germany (Rhein & Kreibich, 2025) or the Valencia floods in Spain in 2024 (Fekete, Estrany, & Ramírez, 2025): both occasions ended in intense debates over public administration.

Clearly, threats to critical infrastructure endanger not only the infrastructure itself, but also governments and public administrations. These threats have therefore provoked policy responses and are part of new and emerging governance needs (Pestana & Sofou, 2024; Wolbach & Talukder, 2025). At the heart of efforts made in this regard are strategic planning and policy coordination for the development of national security strategies and the definition of new political priorities, enabling cooperation, for instance, between EU institutions and member states (Pursiainen & Kytömaa, 2023; Ruohonen, 2024). Regulatory inputs, the monitoring of critical infrastructure,

compliance with norms, sanctioning, and reporting are other efforts (Mikac, 2023). Risk and crisis management based on risk analysis and direct crisis response (Nolte & Lindenmeier, 2024; Leal Filho et al., 2024), as well as intergovernmental and cross-sector collaboration between bodies of administration, ministries, and public authorities (Knodt, Fraune, & Engel, 2022), also form part of it. This has led to policy initiatives like the NIS Directive (EU, 2016/1148), the NIS2 Directive (EU, 2022/2555) and the CER Directive (EU, 2022/2557). The fundamental change to ensure the functioning of digital infrastructure was broadened to more sectors and their operators and was harmonized more deeply into national law in European member states (Ruohonen, 2024; Pursiainen & Kytömaa, 2023). This is clearly a recognition of cascading effects emerging from attacks on critical infrastructure. Both EU Directive 2023/C20/01 and EU Directive 2022/2557 are therefore responses to the increased vulnerability of critical infrastructure to catastrophic events and sabotage, to name just two examples.

1.2 Objective

Initially, authors in critical infrastructure governance focused on the critical assets and vulnerabilities of infrastructure and its management during crises (Ansell & Gash, 2008; Boin & McConnell, 2007). Ansell and Gash (2008) underline that states and administrations cannot resolve risk issues alone and therefore heavily rely on collaboration and stakeholder cooperation. More recent works have focused on the adaptation and networking of governing bodies to strengthen the resilience of critical infrastructure, thereby helping this governance principle gain a foothold in the field of research (Rydén Sonesson et al., 2021; Pursiainen & Kytömaa, 2023; Monstadt & Schmidt, 2019). However, the increasing number of digital threats (Ruohonen, 2024; Pursiainen & Kytömaa, 2023; Mikac, 2023) has shifted the focus to the question of whether infrastructure can continue to function in the event of a malfunction. Pursiainen and Kytömaa (2023) highlight this shift clearly in the context of EU policymaking: Traditional critical infrastructure protection is increasingly giving way to the resilience of critical entities, as evidenced by the CER directive (EU 2022/2557) and the NIS2 directive (EU 2022/2555).

An important ingredient has therefore become the collaboration of knowledge-intensive governance that is part of critical infrastructure management and comprises the collaboration between public authorities, operators, utility companies, private companies and security organisations that enable resilience of critical infrastructure (Kapucu et al., 2023). This strand of literature underlines the importance of cooperation between specific levels and sectors and puts into consideration as for instance cross-sector governance (Sonesson, Johansson & Cedergren, 2021) or multi-level governance-practices such as expert-policy boards and real-time monitoring systems (Kapucu et al., 2023; Knodt, Fraune & Engel, 2022). The focal point here is coordinating different levels of administration to strengthen management and prevent threats to critical infrastructure.

While these approaches have been useful in determining modes of collaboration within governance systems, public-private partnerships have also become a subject of interest in the context of infrastructure resilience governance (Ansell & Gash, 2008; Emerson et al., 2012), as administrations rely on the information and knowledge of the groups and corporations that oversee critical infrastructure. This governance focus also encompasses commonly developed risk governance models (Sonesson, Johansson & Cedergren, 2021) and crisis management strategies (Knodt, Fraune & Engel, 2022).

These approaches are fundamental to critical infrastructure governance and demonstrate that public administration involvement is one of the cornerstones. The

emergence of new critical infrastructure highlights the importance of preparedness due to its high vulnerability. However, this makes current approaches seem rather reactive and neglects the importance of anticipation and preparedness. This article focuses on this issue by drawing on approaches stemming from literature on anticipatory governance (Fuerth & Faber, 2012). This strand of literature has emerged from questions over the development of emerging technologies that are characterized by unwanted side effects. This literature investigates strategic foresight, early risk detection, scenario development, adaptive policymaking, institutional learning and proactive governance to govern unprecedented risks (Guston, 2008, 2014). An important role in this mode of governance is given to ways of governance by public administration (Johnston, 2026).

Thus, anticipatory governance is a term that draws heavily on the concept of technology assessment that was developed in the 1970s to develop a framework that helps govern technological risks. According to technology assessment research, such risks arise from already existing technologies (Collingridge, 1980). Another approach is represented by strategic foresight or anticipatory governance that looks at unprecedented risks when developing innovative technologies (Guston, 2008). This is the case for most emerging technologies like for instance digitalization or artificial intelligence (Sakthivel, 2025) or biotechnology (Ely et al., 2011; Guston, 2008, 2014). Its perspective might be an interesting way of approaching unprecedented threats on critical infrastructure from a rather technological perspective. However, this article aims for a more explicit perspective of the role of public administrations in crisis governance that most governance literature seems to neglect.

However, a general focus on specific practices of public administration is still missing. Most anticipatory governance approaches fall short on the definition of a repertoire of public administration practices (Benighaus & Bleicher, 2019; Bleicher, 2016; Bleicher et al., 2019). Therefore, the article will also refer to literature from the field of Science and Technology Studies (STS) to enrich the framework by situating governance practices that aim to sustain critical infrastructure.

1.3 Method and organization of the article

This article aims to address the general question of how governing and management practices of public administration might help to address the problem of managing newly arising threats to critical infrastructures. This perspective asks for a concrete set of practices that might help a more anticipatory governance to govern critical infrastructure risks. This is mainly done with two approaches: a literature review on anticipatory governance literature toward conceptualizing the translation of anticipatory governance principles, and by analyzing case studies based on a framework derived from the reviewed literature. Here, Scopus, Web of Science, and Google Scholar were likewise used by drawing on the following Boolean operator:

(("anticipatory governance" OR " anticipatory governance" OR "anticipatory innovation governance" OR "future-oriented governance" OR "strategic foresight" OR foresight OR "anticipatory policy" OR "anticipatory public administration") AND (government OR "public sector" OR "public administration" OR agenc* OR authorit* OR ministr* OR municipal* OR bureaucr* OR regulator* OR "public organisation*" OR "public organization*" OR "government institution*" OR "government agenc*" OR "public institution*"))*

The search yielded a set of 21 articles that addressed aspects of the research question. This initial selection included articles that focused on public administration.

Among the literature was a second selection of articles that was more theoretically and conceptually focused.

The case studies were researched using an open search and snowball sampling. Also, policy documents were of relevance here.

A conceptual perspective is developed in the theoretical section of this article. By examining public administration practices to protect critical infrastructure, specific attention is paid to anticipatory governance literature. A rigorous scoping review identifies relevant literature in the field and helps develop an analytical framework. The framework is applied to analyze current threats to critical infrastructure in section three of this article.

This article follows a holistic multiple-case study design as outlined by Yin (2018). This enables a context-sensitive examination of complex phenomena across several real-world cases (Yin, 2018). Each case is regarded as a separate unit of analysis. The selection follows the logic of Yin (2018), who emphasizes that cases exhibiting key differences or similarities in relation to the research question are particularly suitable for analytical case studies.

The design allows for both a within-case analysis and a systematic cross-case analysis to identify similarities, differences, and contextual factors influencing the governance of new threats (Yin, 2018). Within-case studies are a thorough analysis of the context, process, and case characteristics. Insights from within-case analyses provide the basis for defining common analytical dimensions and comparison criteria across cases. This, in turn, helps to identify common patterns or differences across cases (Yin, 2018). The article looks at three cases that represent different security threats that provoked reactions on the governance side of confronting new and emerging threats to critical infrastructure. One is the Nord Stream attack, which can be characterized as a hybrid threat. The Nord Stream attack aimed at critical energy systems (Mikac, 2023; Pestana & Sofou, 2024). This is a serious economic threat for several countries, but specifically for the largest European economy, Germany (Pursiainen & Kytömaa, 2023). The case is representative for changing security landscapes and hybrid forms of warfare (Mikac, 2023). The second case is the Colonial Pipeline cyberattack (Ewoh & Vartiainen, 2024; Ghanbari et al., 2026; Wasserman & Wasserman, 2022). This case stands for threats against digitalized infrastructures that are eminent these days, such as those in the US. Critical digital infrastructure has, since its existence, been subject to attacks; the case is interesting because it shows how interdependent critical infrastructures have become on a global level (U.S. Department of Homeland Security, 2021). The third case is the impact of the flood in Valencia, Spain, which was partially rooted in human error. The case of Valencia is alarming since the southern coast of Spain has always been subject to severe weather extremes. Nevertheless, in October 2024, one of the most severe floods hit the Valencia valleys and caused high casualties (Leal Filho et al., 2024; Rhein & Kreibich, 2025).

In Section 4, these cases are discussed from the perspective of the framework as laid out in this article. The case selection aims to facilitate a comparative analysis of different institutional contexts (Yin, 2018). The framework does not only identify specific practices and governance aspects to anticipate and address newly emerging security threats to critical infrastructure. It also helps to develop new insights into specific governance taxonomies that help public administrations to cope with such systemic risks. Therefore, the case selection is regarded as being guided by theoretical considerations. Contrasts between specific reactions and controversies are of particular interest.

Section five concludes this article and makes transparent limitations and outlooks that emerge from this article.

2. Theory and framework

2.1 The foundations of anticipatory governance

The groundwork of anticipatory governance was laid out by David Guston (Guston, 2007, 2014) and Daniel Sarewitz (Guston & Sarewitz, 2020) in Science and Technology Studies (STS) and environmental studies. The work of Guston has allowed for further theoretical development that has found much appreciation in the scientific STS and governance communities. Basically, the term anticipatory governance describes the five terms foresight, engagement, integration, ensemble, and reflexivity (Guston, 2014).

Foresight is not a crystal ball for estimating futures. It is rather an outline of many possible scenarios that might be realized soon (Guston, 2014). This is where the approach becomes valuable for analyzing public administrative practices to govern critical infrastructure risks.

The second category is described as engagement, which characterizes the inclusion of different visions and positions of stakeholders (Guston, 2014). This is specifically important considering the multiple stakeholders of critical infrastructures. This means that different sorts of knowledge are necessary to govern critical infrastructures. Thus, engagement raises the question of who should participate in discourses and discussions on governance and who is supposed to decide on that (Guston, 2014; Guston & Sarewitz, 2020). By so doing, the focus is not merely on a democratic turn in governance, but rather on the constant question of who possesses useful knowledge to realize informed governance practices.

This leads to the category of integration, which can be regarded as the actual use of different perspectives when governing critical infrastructures. Guston and Sarewitz (2020) refer here to the integration of perspectives from the social sciences and natural sciences to jointly integrate the right perspectives. Again, it is important to note that the questions of why specific knowledge is to be integrated, how, and under which assumptions this is done are important (Guston, 2014). This also includes assumptions about what other ways and visions are possible (Guston & Sarewitz, 2020).

Thus, ensembleization is the crucial point of learning where foresight, engagement, and integration are carefully knitted together to develop a better understanding of possible futures (Guston, 2014; Guston & Sarewitz, 2020). By delivering different future scenarios, foresight allows for their discussion, and engagement can enhance such visions by adding different aspects, whereas integration then complements these visions with critical and technical perspectives (Guston & Sarewitz, 2020).

The framework then culminates in the category of reflexivity. This means that one's own role, assumptions, norms, interests, and responsibilities should be questioned (Guston, 2014). The crucial questions here are why specific perspectives on possible futures are considered important and which specific societal assumptions they are based on. This enables a more careful and stable consideration of possible futures. This includes a shift towards perspectives that actively ask: Why are we looking at this problem in this way? Which groups were not consulted when the problem was defined? Which institutional routines are influencing our decisions? What long-term consequences does our current approach have? After consolidating the perspective of the governance approach discussed here, a review of the anticipatory governance literature on public administration practices is presented to develop the foundation of the framework.

2.2 A review of anticipatory *governance literature on governance practices of public administration*

The review consisted of 21 high-quality articles in specific governance journals on anticipatory governance issues of public administrations to derive a framework for this article. The articles can be thematically clustered as follows: (1) development of the theoretical concept as a main goal for public administration use (Guston, 2014; Fuerth, 2009, 2011; Ramos, 2014; Heo & Seo, 2021), (2) the organization of foresight capacities in ministries and administrative bodies for strategic future planning (Miles, 2010; Calof & Smith, 2010; van der Steen & van Twist, 2013; Greenblott et al., 2019; Priebe et al., 2025; Heo & Seo, 2021; Kallo & Välimaa, 2025), (3) the integration of foresight in administrative practices in policy making, policy design, and the modernization of public administration (Kimbell & Vesnić-Alujević, 2020; Greenblott et al., 2019; Priebe et al., 2025; Heo & Seo, 2021), (4) the anticipation of climate risk, catastrophes, and the construction of resilient infrastructure (Boyd et al., 2015; Croxatto et al., 2020; Boyd & Wilson, 2021; Warren, 2025; Krishnan & Robele, 2024), (5) the socially responsible development and application of technologies (Guston, 2014; David et al., 2017; Nelson et al., 2023), and (6) the deliberate participation of publics (Bezold, 2018; Ramos, 2014; Kimbell & Vesnić-Alujević, 2020; Nelson et al., 2023).

The category of foresight received the most attention. Accounts argued from a rather conceptual perspective (Guston, 2014; Fuerth, 2009; Fuerth, 2011; Ramos, 2014; Heo & Seo, 2021). At the center of the argument is the development of an administrative capacity for scenario building, horizon scanning, weak signal monitoring, modelling, and simulation to help governments prepare for uncertainty. More explicitly, Miles (2010), Calof and Smith (2010), van der Steen and van Twist (2013), Greenblott et al. (2019), Heo and Seo (2021), Priebe et al. (2025), and Kallo and Välimaa (2025) argue for organizational units in administrative bodies that enable the steady realization of horizon-scanning processes, scenario development, trend analyses, roadmaps, and strategic future planning in order to support anticipatory administration. This includes delivering this kind of knowledge into the regular policy and regulatory cycle and therefore making it a condition of administrative practice (Kimbell & Vesnić-Alujević, 2020; Greenblott et al., 2019; Priebe et al., 2025; Heo & Seo, 2021).

This is specifically the case for scenarios, climate models, hydrological models, probabilistic risk analyses, worst-case analyses, red teaming, and the assessment of cascading risks in order to govern climate risks and catastrophes (Boyd et al., 2015; Croxatto et al., 2020; Boyd & Wilson, 2021; Warren, 2025; Krishnan & Robele, 2024). According to Guston (2014), David et al. (2017), and Nelson et al. (2023), this must include a responsible way to deal with innovative technologies, such as the development of alternative technology pathways or addressing ethical issues connected to the use of specific technologies. Furthermore, this goes hand in hand with realizing workshops, co-design processes, future workshops, and deliberative participation processes (Bezold, 2018; Ramos, 2014; Kimbell & Vesnić-Alujević, 2020; Nelson et al., 2023). The review therefore results in a consistent focus on foresight regarding administrative practices.

The articles have a rather heterogeneous understanding of engagement. It was therefore necessary to build different clusters. Fuerth (2009, 2011), van der Steen & van Twist (2013), Greenblott et al. (2019), and Priebe et al. (2025) highlight the cooperation of ministries, public administrative bodies, and political decision-makers, but do not explicitly rely on the participation of publics. Another common perspective is that different levels of government, administration, and governing organizations should engage in strong networking activities (Ramos, 2014; Boyd et al., 2015;

Croxatto et al., 2020; Krishnan & Robele, 2024). Whereas Miles (2010), Calof & Smith (2010), Heo & Seo (2021), Kallo & Välimaa (2025), and Croxatto et al. (2020) specifically emphasize the consultation of publics, scientists, and international organizations as fruitful. The authors argue that the quality of future analyses is enhanced and that a general knowledge transfer for foresight is enabled (Miles, 2010; Calof & Smith, 2010; Heo & Seo, 2021; Kallo & Välimaa, 2025; Croxatto et al., 2020). Also, Bezold (2018), Ramos (2014), Nelson et al. (2023), Guston (2014), and Kimbell & Vesnić-Alujević (2020) argue in this direction but base scenario building specifically on activities of citizens. David et al. (2017), Nelson et al. (2023), Guston (2014), Boyd & Wilson (2021), and Warren (2025) take a rather moderate perspective and speak of consultations that might be fruitful for enriching the perspective of public administrations. It becomes clear that the authors differ in their understanding of the purpose of engaging with specific publics, such as NGOs or citizens.

Also, the integration of perspectives followed the same cluster since the difference in how to engage with actors relates to the ways in which actors are engaged and how their perspectives are consequently considered. Fuerth (2009, 2011), Greenblott et al. (2019), Heo & Seo (2021), Priebe et al. (2025), and Kallo & Välimaa (2025) strongly advocate the integration of ministerial routines, strategic planning, and household processes, but also for the design of concrete processes for integrating different perspectives in public administration. By so doing, the authors rely strongly on the normative assumptions of the anticipatory governance framework. More dedicated to the policy cycle, Calof & Smith (2010), Greenblott et al. (2019), Kimbell & Vesnić-Alujević (2020), Priebe et al. (2025), and Warren (2025) assume that integration is employed in the concrete policy design process.

Others see this competence rather rooted in the ways in which technology design, development, and deployment are co-designed with different societal actors, such as public representatives, NGOs, or citizens, as, for instance, Guston (2014), David et al. (2017), Croxatto et al. (2020), and Nelson et al. (2023). This reveals that the focus of concern is shifted from a general practical and institutional level to concrete practices of technology deployment and use. As in the engagement category, others rely on networking between levels (Ramos, 2014; Boyd et al., 2015; Croxatto et al., 2020; Boyd & Wilson, 2021; Krishnan & Robele, 2024) or combining foresight methods (Miles, 2010; Ramos, 2014; Greenblott et al., 2019; Kimbell & Vesnić-Alujević, 2020; Krishnan & Robele, 2024) and therefore do little to distinguish between levels.

Guston (2014), Ramos (2014), Heo and Seo (2021), Kimbell and Vesnić-Alujević (2020), and Nelson et al. (2023) rely on the original perspective that strongly links to the original framework and that poses ensemblization as a recursive learning practice that reflects on the cooperation of actors. Other reviewed accounts see ensemblization as the combination of foresight and governance practices, as, for instance, the development of an anticipatory governance system (Fuerth, 2009; Fuerth, 2011; Guston, 2014). Others highlight long-term technology cooperation to strategically foster foresight (Miles, 2010; Kallo & Välimaa, 2025). Differently, Greenblott et al. (2019), Heo & Seo (2021), and Priebe et al. (2025) pledge for constituting organizational capacities to fulfil functions of anticipatory governance. This includes linking policy with anticipatory politics (Calof & Smith, 2010; van der Steen & van Twist, 2013). As laid out for the former categories, some accounts suggest developing future scenarios with stakeholders across society (Ramos, 2014; Bezold, 2018; Kimbell & Vesnić-Alujević, 2020; David et al., 2017; Nelson et al., 2023), and others see ensemblization in the installation of early warning systems (Boyd et al., 2015; Croxatto et al., 2020; Boyd & Wilson, 2021; Warren, 2025; Krishnan & Robele, 2024).

Reflexivity is thus seen as the means to continuously engage in reflection on societal values and the ethical and moral consequences of practices that include innovative technologies (Guston, 2014; David et al., 2017; Nelson et al., 2023). This somehow limits the focus to the deployment and use of technologies. Another important viewpoint is to root reflexivity in the development of risk scenarios and their impacts on society (Boyd et al., 2015; Croxatto et al., 2020; Boyd & Wilson, 2021; Warren, 2025; Krishnan & Robele, 2024). This shifts the focus to the perception of foresight practices. Other authors share a broader understanding that understands reflexivity as the means to reflect on the very core functions of public administration and its meaning for society (Fuerth, 2009, 2011; Greenblott et al., 2019; Heo & Seo, 2021; Priebe et al., 2025). Others understand the sheer integration of different societal actors already as an act of reflection (Bezold, 2018; Ramos, 2014; Kimbell & Vesnić-Alujević, 2020; Nelson et al., 2023).

From this perspective, anticipatory governance differs from traditional risk governance approaches in three specific ways. Firstly, one of the key features of this governance concept is the extensive involvement of the public, public administration, businesses and politicians (Guston, 2014). This integrative perspective can be viewed as an early governance strategy for intervention. Examples include the development of technologies such as nanotechnology (Guston, 2008) and geoengineering (Foley et al., 2015; Macnaghten & Owen, 2011). This allows for societal stabilization and discussion of risks that may arise when applying emerging technologies. This means that anticipatory governance encapsulates the notion of sharing visions, knowledge and information and broadens not only a general understanding but to actively generate knowledge that can then be useful to govern crises and conflict (Ely et al., 2011).

Another important pillar of anticipatory governance is its recognition of the possibility of failure. Anticipatory governance does not necessarily investigate and predict the future. Rather, it is an approach that makes significant efforts to deal with scenarios such as crises, failures and malfunctions as part of a governance objective (Guston & Sarewitz, 2020). The understanding of anticipatory governance can thus help to assess critical infrastructure risks arising from new and unprecedented threats. Emerging technologies diffuse into many areas of societal practice, and their potential downsides can cause significant harm (Rotolo et al., 2015). Insofar, they share a quality with critical infrastructures that are a critical backbone of the functioning of modern societies.

The third important denominator of anticipatory governance is its notion of governance "while such management is still possible" (Guston, 2008:vi) to deal with risk and to protect societies from harm. Here windows of opportunity such as policymaking or technological development come into play.

2.3 Anticipatory governance practices in public administration

Literature on public administration does not necessarily see it as an enforcement authority but rather understands it as a governance body itself. This perspective is specifically reflected in the work of Bleicher et al. (2019), Benighaus and Bleicher (2019), as well as Bleicher (2016). Public administration must be understood as a set of social practices that have a steering function in a variety of publicly relevant contexts (Bleicher et al., 2019). This is enabled through the organization of long-term development and cooperation for common developments such as technologies (Bleicher et al., 2019). From this perspective, it becomes clear that one important dimension of governance practices of public administration is the control and development of system-relevant knowledge.

Practices such as horizon scanning, scenario development, trend analyses, roadmaps, and strategic future planning are therefore characteristic of this knowledge dimension. Often, this includes the integration of heterogeneous knowledge (Benighaus & Bleicher, 2019) originating, for instance, from uncertain futures or newly emerging risks (Rotolo et al., 2015; Boyd et al., 2015; Boyd & Wilson, 2021; Croxatto et al., 2020; Krishnan & Robele, 2024; Warren, 2025). This concerns administrative and ministerial routines such as reporting, consulting, or strategic planning, as well as perspectives on policy design and co-creation (Calof & Smith, 2010; Fuerth, 2009, 2011; Greenblott et al., 2019; Guston, 2014; Heo & Seo, 2021; Kallo & Välimaa, 2025; Kimbell & Vesnić-Alujević, 2020; Miles, 2010; Priebe et al., 2025; Ramos, 2014; van der Steen & van Twist, 2013). This is relevant specifically for the governance of environmental risks that emerge from threats and applications alike (Benighaus & Bleicher, 2019, S. 50–51). Sets of practices therefore comprise the use of regulatory and consulting practices. This relates to a wide range of policy-making-relevant practices.

Another governance resource is coordination between actors such as politics, science, the economy, and the public (Bleicher et al., 2019). This brings together line ministries, public administrative bodies, networks between entities, and consulting science, as well as international and non-governmental organizations (Bezold, 2018; Boyd et al., 2015; Calof & Smith, 2010; Croxatto et al., 2020; Fuerth, 2009, 2011; Greenblott et al., 2019; Guston, 2014; Heo & Seo, 2021; Kallo & Välimaa, 2025; Krishnan & Robele, 2024; Miles, 2010; Nelson et al., 2023; Priebe et al., 2025; Ramos, 2014; van der Steen & van Twist, 2013).

There is also a perspective on public administration as the juridical power that makes public administrations strong actors in all kinds of policy-making processes and regulation (Benighaus and Bleicher, 2019). Therefore, foresight capacities are important for regulatory processes and modernizations of all kinds to connect anticipation with regular administrative actions (Calof & Smith, 2010; Greenblott et al., 2019; Heo & Seo, 2021; Kimbell & Vesnić-Alujević, 2020; Priebe et al., 2025; Warren, 2025).

Most authors agree, however, that reflexive modes of practice are necessary to govern risks (Bezold, 2018; Boyd et al., 2015; Boyd & Wilson, 2021; Croxatto et al., 2020; David et al., 2017; Fuerth, 2009, 2011; Greenblott et al., 2019; Guston, 2014; Heo & Seo, 2021; Kimbell & Vesnić-Alujević, 2020; Nelson et al., 2023; Priebe et al., 2025; Ramos, 2014; Warren, 2025). Reflexivity is the continuous re-working of all practices by revising processes and visions.

The following section displays the three exemplifying case studies that are to be discussed from the perspective of the framework.

3. Case Study Analysis

3.1 Foresight

This section displays the three cases according to the framework. According to literature, foresight practices are constructing knowledge capacities, horizon scanning, and strategic future planning to estimate possible risks (Miles, 2010; Calof & Smith, 2010; Greenblott et al., 2019; Priebe et al., 2025).

The jurisdiction of the Nord Stream pipeline has reached German courts since the pipeline ends in German territory (Reuters, 2026). After the explosions in September 2022 in the Baltic Sea on the Polish and the Danish coastline, German and Russian authorities stopped the flow of Russian gas via the Nord Stream pipelines (McCabe & Flynn, 2024; Mikac, 2023). In the scientific community, Kóczy et al. (2022) developed

a model of security of supply including the Nord Stream pipelines before the attack. The risk model pointed to a high vulnerability to sabotage and was therefore estimated to increase European supply security (Kóczy et al., 2022). The authors had their article accepted only days before the attack (Kóczy et al., 2022). The then German Ministry of Economic Affairs (BMWi) still concluded in 2021 that Nord Stream would boost supply security (BMWi, 2021). This prevailing economic vision of connecting the gas fields of Jamal with Germany (BMWi, 2021) contrasts with findings of the scientific service of the European Parliament. In 2016, it was found in a press release that the pipeline would rather increase European supply risk (European Parliament, 2016). This was repeated in 2021 in a study of the scientific service of the European Parliament, and an increasing interdependency on fossil fuels was recognized as endangering the New Green Deal in 2015 (European Parliament, 2021). After the attack on the pipeline, the discourse changed, and investments were made in other providers. The policy reaction at the European regulatory level is therefore not surprising. This has held true specifically for pipelines (McCabe & Flynn, 2024; Pursiainen & Kytömaa, 2023).

The Colonial Pipeline cyberattack in the USA in 2021 points to an equal pattern. Already in 2018, the U.S. Government Accountability Office (GAO, 2018) informed about gaps in the cybersecurity of the pipeline project. The GAO report states: “Pipeline operators reported using a range of guidelines and standards to address physical and cybersecurity risks, including the Department of Homeland Security's (DHS) Transportation Security Administration's (TSA) Pipeline Security Guidelines, initially issued in 2011.” (GAO, 2018). The US Department of Energy relied on a self-assessment-based security standard that was intended to provide a sufficient benchmark for investments (Department of Energy, 2022).

Caused by an extreme weather event, the flood event in Valencia, Spain, was of a different nature. Its impact was accelerated by human failure. Even before the 2024 flood, various practices for anticipating flood risks were already in place in the Valencia region. These included hazard mapping initiatives such as PATRICOVA and SNCZI, which were used to spatially identify areas potentially affected by flooding (Camarasa-Belmonte et al., 2025). PATRICOVA maps and manages flood risks at the regional level in the Valencian Community and incorporates these findings into spatial and urban planning, while the national SNCZI systematically maps flood hazards and potentially affected areas and provides this information for risk prevention, spatial planning, and disaster management (Generalitat Valenciana, 2015; Ministry for Ecological Transition and the Demographic Challenge). The importance of such mapping for assessing extreme events and associated risks has long been documented in research (Büchele et al., 2006), while climate change and the associated uncertainties regarding future flood events were also studied prior to 2024 (Benito et al., 2021). The fact that 85.9% of the area flooded in 2024 was already included in existing hazard maps shows that a significant portion of the spatial risk was known even before the event and that scientifically based information was available (Camarasa-Belmonte et al., 2025). However, the autonomous government made late use of merchant law; this was seen to be one of the main reasons why the death toll was so high.

This shows that the outset of all three cases was characterized not by a lack of foresight, but by the limited translation of already available risk knowledge into preventive administrative action. The cases have very different starting points that are displayed in the following chart.

Table 1. Foresight

Case	Knowledge before the event	Central problem
Nord Stream	Geopolitical and security-of-supply risks were known	Competing risk interpretations
Colonial Pipeline	Cyber risks and regulatory weaknesses were known	Implementation/regulatory gap
Valencia	Hazard maps, risk plans, and warning information were available	Translation/coordination gap between risk knowledge, warning, and action

Source: own compilation.

3.2 Engagement

Prior to the Nord Stream attack, German and European authorities, companies, and the scientific community assessed supply security, energy dependencies, Russia's role, Ukrainian transit, and wider geopolitical risks (BMWi, 2021; European Parliament, 2016, 2021; Kóczy et al., 2022; Deutscher Bundestag, 2016, 2018, 2021). This was because the German energy market influences the entire German region (European Parliament, 2016). The assessments of private and scientific actors differed from those of the German authorities about geopolitical dependencies and infrastructure risks (Bundesregierung, 2019; BMWi, 2021; Deutscher Bundestag, Wissenschaftliche Dienste, 2016; Deutscher Bundestag, 2020; European Parliament, 2016, 2021; Kóczy et al., 2022). This shows that the main problem was not stakeholder engagement, but rather the absence of a shared risk perspective (Guston, 2014).

Before the Colonial Pipeline attack, a broad public-private governance network existed that operated energy grids. This network consisted of operators, security agencies, and government bodies that were supported by guidelines, security reviews, and cybersecurity standards (GAO, 2018; U.S. Congress, 2021; Congressional Research Service, 2021). The network was characterized by voluntary participation, fragmented responsibilities, and underused governance means as well as limited collective preventive capacity. These measures were not enough to share information to put it into effect (Ramos, 2014; Boyd et al., 2015; Croxatto et al., 2020). This emphasizes that the mere existence of knowledge is not enough to anticipate threats.

A similar pattern of ignored knowledge followed the 2024-Valencia disaster. Valencia is an example of an existing multi-level network of scientific, technical, regional, local, and national actors and institutionalized flood-risk planning through PATRICOVA (Generalitat Valenciana, 2015; Camarasa-Belmonte et al., 2025). The entire system was in place but failed to translate into direct action for civil protection during the disaster. Literature blames fragmented responsibilities and a lack of a clear chain of command to cause harm by not turning to regional merchant law (Boyd et al., 2015; Croxatto et al., 2020; Camarasa-Belmonte et al., 2025). As the Colonial Pipeline case, the Valencia case shows that acknowledging different perspectives is not enough in order to build strong foresight.

Comparing the three cases shows that engagement is not about the number of stakeholders but about how they are integrated with their own visions and perspectives.

3.3 Integration

Prior to the Nord Stream attack, differing perspectives on supply security, economic dependencies, infrastructure risks, and geopolitical threats were prevailing in the general discourse on Germany's and Europe's energy security (BMWi, 2021; European Parliament, 2016, 2021; Kóczy et al., 2022). These perspectives were

integrated only to a very limited extent in closed joint meetings from the perspective of other European partners as was revealed. The main market for Russian natural gas is Germany, with a high share of natural gas in its energy mix and an overall high level of energy supply for other European countries (McCabe & Flynn, 2024; Mikac, 2023; Pursiainen & Kytömaa, 2023). One of the main drivers of the Nord Stream attack has been the motivation to cut energy supplies from Russia to weaken Russia's economy (Pestana & Sofou, 2024; Pursiainen & Kytömaa, 2023).[1] The high dependency from fossil fuels shows that industries and private households were targeted alike. However, the attack revealed a large lack of integration from a European perspective; supply risks were merely neglected by German administration.

As described prior to the case of Valencia, the responsibilities for acting and regulating security standards at the Colonial Pipeline were distributed widely. Effective pipeline governance depended on close interagency coordination across several agencies (GAO, 2019; Congressional Research Service, 2021). The cooperative framework was partly outdated as the 2006 TSA-PHMSA *MOU Annex* and the 2010 *Pipeline Security and Incident Recovery Protocol Plan* found out since it no longer fully reflected evolving responsibilities and cyber threats (GAO, 2019, 2021). Colonial therefore reflects a weakness in the quality rather than the extent of engagement, as existing actors, expertise, standards, and information channels did not translate into shared preventive capacity (GAO, 2018, 2019, 2021; Congressional Research Service, 2021; Guston, 2014; Ramos, 2014; Boyd et al., 2015; Croxatto et al., 2020; Greenblott et al., 2019; Heo & Seo, 2021; Kimbell & Vesnić-Alujević, 2020).

This pattern of diverging stakeholder perspectives was also present in the Valencia floods (Generalitat Valenciana, 2015; Camarasa-Belmonte et al., 2025). In fact, there was an extensive production of management- and governance-relevant knowledge built by AEMET or other local bodies like PATRICOVA. However, the event demonstrated that different bodies of knowledge are not automatically and effectively integrated into timely administrative decisions and warnings. In all three cases, the central challenge was thus less a lack of knowledge than the need to combine different bodies of knowledge and risk assessments into a shared understanding of risk and to translate this into coordinated preventive action.

3.4 Ensemblization

The Nord Stream project incorporated various elements of anticipatory governance, including risk analyses, stakeholder engagement, and European precautionary mechanisms. In 2020, 24% of Germany's natural gas demand was met by Russian natural gas (Eurostat, 2020). The interruption of the gas supply had several critical effects on macro- and microeconomic scales. This makes hybrid warfare an effective tool to stoke uncertainty and thereby undermine the legitimacy of political systems through artificially induced energy shortages (Pursiainen & Kytömaa, 2023). However, the integration of these elements remained limited, as energy policy, geopolitical, and infrastructure risks were not combined into a common precautionary approach—a fact also reflected in the European resilience policy, which was only strengthened after the attack (European Parliament, 2017, 2021; European Council, 2022).

[1] However, cross-border infrastructure such as the subsea Nord Stream pipelines supplies all kinds of industries with natural gas. Back in the year 2022, German industries still depended on Nord Stream imports for 55% of their natural gas supply (BPB, 2022). Back in 2020 natural gas made a 31% of German energy supply. A large portion of this energy use was by private households with about 41% back in 2019 (Statistisches Bundesamt, 2022).

In the Colonial Pipeline case, security guidelines, risk assessments, security reviews, and public-private cybersecurity cooperation were already in place, but these elements did not yet form a fully cohesive and adaptive preparedness system, as reflected in shortcomings in risk assessment, guideline updating, review follow-up, and incident-response protocols (Guston, 2014; Greenblott et al., 2019; Heo & Seo, 2021; Kimbell & Vesnić-Alujević, 2020; GAO, 2018, 2019, 2021; Congressional Research Service, 2021).

In Valencia, the mapping of seasonal well-known floods, meteorological monitoring, warning and disaster response structures were already in place prior to the event. Nevertheless, the integration of these elements remained limited, as they did not form a continuous chain of risk detection, warning, and timely response (AEMET, 2024a; MITECO, 2025a).

In all three cases, key governance elements were in place; however, their integration into a continuous and mutually reinforcing preparedness process remained limited (Tanguay et al., 2023).

3.5 Reflexivity

At Nord Stream, geopolitical risks and the growing dependence on Russian gas were already the subject of heated debate even before the attack (European Parliament, 2021). Nevertheless, the impact of this criticism remained limited, as it initially had only a limited effect on Germany's fundamental assessment of the project and its approach to the associated strategic risks. The secondary effect of this attack was increased costs for the European economy's largest export market. According to Rotolo et al. (2015), emerging technologies are characterized by their tendency to spread across all systems. A similar pattern can therefore be observed here in relation to this act of sabotage, as its impact is felt on multiple scales and continues to fundamentally transform the European economy (Mikac, 2023; Pursiainen & Kytömaa, 2023; Soldi et al., 2023). Nevertheless, the oil embargo and the sanctions on the Russian economy had already had a significant impact on the Russian economy (Mikac, 2023). A cut-off of this pipeline therefore promised to weaken the Russian economy as an act of hybrid warfare (McCabe & Flynn, 2024). It also had side effects on the policy side. The sabotage of Nord Stream was perceived and interpreted differently among European public administrations. Energy policymakers across Europe saw the cut-off rather as an economic threat that increased energy prices, affected supply security, political systems, and the security of maritime infrastructure on a general level (Wolbach & Talukder, 2025; McCabe & Flynn, 2024). One of the responses in the field of energy economy and energy management was the REPower plan that was launched by the EU (European Parliament & Council of the European Union, 2022). This plan aims to mitigate gas shortages by requiring Member States of the European Union to fill up gas storage up to 90% each November (EU directive 2022/1032). Furthermore, REPower redistributes resources to diversify energy sources (European Parliament & Council of the European Union, 2022, European Commission). The aim of the plan is therefore to reduce dependence on Russian fossil fuels. This shows that European energy policy interpreted the sabotage of Nord Stream pipelines as a systemic risk that needs systemic answers.

Another yet developing policy field was critical infrastructure protection, which aims to protect and monitor cross-border infrastructure and support its resilience (European Parliament & Council of the European Union, 2022). This includes maritime security, as presented by the Council of the European Union (2023) with the EUMSS Action Plan. Yet another newly emerging policy field that was reinforced by the Nord

Stream attack is cybersecurity (European Parliament & Council of the European Union, 2022), which led to the NIS2 Directive that repealed the NIS1 Directive based on new standards for cross-border infrastructure security reporting and risk management. Furthermore, European defence policy was rethought based on the idea of a common strategic response to cross-border threats (Council of the European Union, 2022). This was also the policy basis for Russian economic sanctions. Defence also includes supporting European civil protection mechanisms (European Parliament & Council of the European Union, 2021).

The TSA regulation—which was largely voluntary and based on the Pipeline Security Guidelines and operator cooperation—was made mandatory for the first time for certain critical pipeline operators following the Colonial Pipeline attack through Security Directive 1 of May 27, 2021, which required the appointment of a cybersecurity coordinator, the reporting of cyber incidents to CISA, and a Cybersecurity Vulnerability Assessment—including the identification of non-conformities, corrective actions, and implementation deadlines—(Jaikaran & Parfomak, 2021, 2022; TSA, 2021). Security Directive 1 initially established a mandatory 12-hour deadline for reporting relevant cyber incidents to CISA, while Security Directive 2 of July 20, 2021, significantly expanded the regulations to include mandatory protective measures against ransomware and other IT/OT threats, as well as the requirement for a Cybersecurity Contingency and Recovery Plan and a Cybersecurity Architecture Design Review (Jaikaran & Parfomak, 2021, 2022). Following the attack, the TSA shifted its regulatory focus more toward the interaction between IT and operational technology systems (OT) and made the requirements enforceable through trained TSA inspectors; however, the initially highly prescriptive nature of the second directive was reevaluated shortly after its introduction in light of more than 380 requests for alternative measures as well as criticism from industry and Congress (Jaikaran & Parfomak, 2021). In 2022, the TSA revised its post-colonial rules toward a more flexible, performance-based approach with mandatory IT/OT security, monitoring, incident response, and regular assessments, ultimately developing toward a permanent Cyber Risk Management Program (Jaikaran & Parfomak, 2022; TSA, 2022, 2024). Valencia had established flood forecasting and warning systems, but their limitations became apparent during the extreme event.

In all three cases, there was reflection on risks; however, prior to the respective event, this led only to a limited extent to a fundamental review and adjustment of existing assumptions and procedures. Following the DANA disaster, the existing flood risk model was immediately adjusted based on lessons learned from the event by mandating the revision of PATRICOVA to account for the actual observed flooding, supplementary DANA-2024 mapping and its integration into planning procedures, as well as additional risk analyses, while at the same time linking the reconstruction efforts to existing flood resilience requirements (Generalitat Valenciana, 2015). Immediately after the disaster, Decreto-ley 20/2024 initially suspended certain urban planning procedures in flood-prone areas, based on PATRICOVA, SNCZI, and the new DANA mapping, so that not only the existing risk management but also the regulations introduced immediately after the event were reevaluated and adjusted (Generalitat Valenciana, 2015).

4. Discussion

The three case studies show that anticipatory governance does not primarily fail due to a lack of risk knowledge, as significant hazards were already known prior to the respective events (BMWi, 2021; GAO, 2018; Camarasa-Belmonte et al., 2025). While

in the Nord Stream case, differing political and administrative risk assessments competed with one another, the Colonial Pipeline case tends to illustrate an inadequate institutional response to already known cyber risks (European Parliament, 2021; GAO, 2018). In the case of Valencia, large portions of the spatial flood risk had already been mapped, which places particular emphasis on translating existing knowledge into timely administrative action (Generalitat Valenciana, 2015; Camarasa-Belmonte et al., 2025). These cases thus confirm that foresight alone is not sufficient; rather, it must be linked to administrative decision-making processes through integration, engagement, and institutional embedding (Fuerth, 2009, pp. 101–109; Guston, 2014; Greenblott et al., 2019, pp. 6, 11–16). Reflexivity is particularly relevant here because public administrations must continuously review and adapt existing assumptions and routines in light of new information (Fuerth, 2009, pp. 105–113; Boyd & Wilson, 2021, pp. 20–29).

The actual deficiency is where risk-relevant knowledge needs to be translated into administrative action.

Engagement in the context of the public administration assumes a coordinating role among these various stakeholders (Bleicher et al., 2019; Greenblott et al., 2019). The three cases have in common that all mechanisms aimed at managing critical infrastructure risks failed to translate into what could be an actionable understanding of risk (Guston, 2014; Guston & Sarewitz, 2020; Fuerth, 2009, 2011; Ramos, 2014; Boyd et al., 2015; Croxatto et al., 2020; Greenblott et al., 2019; Kimbell & Vesnić-Alujević, 2020; Heo & Seo, 2021; Priebe et al., 2025). The manifestations differ widely across the cases: Geopolitical risk interpretations in Nord Stream (European Parliament, 2016, 2021; BMWi, 2021; Kóczy et al., 2022), incomplete institutionalization of cybersecurity knowledge in Colonial Pipeline (GAO, 2018, 2019, 2021; Congressional Research Service, 2021), as well es difficulties integrating distributed technical and scientific knowledge under pressure in Valencia (Generalitat Valenciana, 2015; AEMET, 2024b; Camarasa-Belmonte et al., 2025, 2026; Camarasa-Belmonte & Soriano-García, 2026). This shows that the cases were embedded in an environment that produced these discrepancies.

One of the crucial questions is therefore whether actors with knowledge that is crucial for risk assessment are involved in the transfer of actionable knowledge. Consequently, this would need a careful reassessment of information from administrations. The sole existence of networks, this is one of the findings of this analysis, is not enough.

The cases reflect that there was no coherent integration of concrete governance capacities in the form of controls and resources that could be mutually integrated to boost foresight capacities (Guston, 2014; Fuerth, 2009, 2011; Ramos, 2014; Greenblott et al., 2019; Kimbell & Vesnić-Alujević, 2020; Heo & Seo, 2021; Tanguay et al., 2023; Priebe et al., 2025). This is also shown by the weak level of ensemblization between geopolitical, economic, and infrastructure-security governance in Nord Stream (European Parliament, 2016, 2021; BMWi, 2021; Kóczy et al., 2022), risk assessment, regulatory oversight, cybersecurity expertise, and operator implementation in Colonial Pipeline (GAO, 2018, 2019, 2021; Congressional Research Service, 2021), and forecasting, monitoring, emergency coordination, warning, and protective action in Valencia (Generalitat Valenciana, 2015; AEMET, 2024a,b; Camarasa-Belmonte et al., 2025; MITECO, 2025b). As a higher-order governance aspect, ensemblization enacts foresight, engagement, and integration which are then reassessed in a continuous loop (Fuerth, 2009, 2011; Guston, 2014; Ramos, 2014; Boyd et al., 2015; Greenblott et al., 2019; Croxatto et al., 2020; Kimbell & Vesnić-Alujević, 2020; Boyd & Wilson, 2021;

Heo & Seo, 2021; Nelson et al., 2023; Tanguay et al., 2023; Krishnan & Robele, 2024; Priebe et al., 2025; Warren, 2025).

5. Conclusion

The case comparison shows that the cases fail at different stages of this mechanism. Nord Stream makes it transparent that combining different risk-perspectives was challenging, the Colonial Pipeline attack is more about coordinating regulation, risk-relevant knowledge and monitoring to safeguard data systems. Valencia shows that making indicative knowledge from real-time assessments actionable was difficult. Failure results therefore from different sources and translates into governance failure.

All cases point to recursive regulatory learning through repeated post-crisis adjustments (Jaikaran & Parfomak, 2021, 2022; TSA, 2022, 2024; Generalitat Valenciana, 2015; Greenblott et al., 2019; Heo & Seo, 2021), suggesting that reflexivity becomes an effective anticipatory governance capacity only when administrations institutionalize continuous mechanisms for challenging assumptions, incorporating lessons, revising risk models, and adapting policies before disruptive events expose governance failures (Fuerth, 2009, 2011; Guston, 2014; Ramos, 2014; Greenblott et al., 2019; Kimbell & Vesnić-Alujević, 2020; Heo & Seo, 2021; Boyd & Wilson, 2021; Tanguay et al., 2023; Priebe et al., 2025; Warren, 2025).

One of the vital learnings of this case comparison is that learning took place, but only at the end of the process. This is the difference between anticipatory governance and reactive approaches. Anticipatory governance therefore needs room for action prior to crisis.

Public administration does not address risks automatically with better foresight. Much more important is its interplay with engagement and integration. Thus, ensemblization ensures that these capabilities do not remain isolated. Reflexivity ensures that the resulting governance system can be adapted continuously. It is not newly produced knowledge but rather the interplay of actions to unify broad visions for potential risks.

Public administration can address risks of critical infrastructures best by incorporating various routines of knowledge integration and engagement. This requires existing routines to be questioned more critically and to directly involve holders of relevant knowledge directly. It is the embedding of foresight, engagement, integration and ensemblization that makes up for good governance decisions. Public administration therefore acts not only as a regulator or crisis manager, but also as a coordinating actor that translates risk knowledge into administrative decisions. At the same time, the cases suggest that the anticipatory governance framework can also be applied beyond its original technology-related context to hybrid, cyber, and climate-related threats to critical infrastructure.

This analysis has several limitations. Only three cases were compared. Also, the cases differ considerably in type. Moreover, differences in threat type, institutional context, governance level, and timing limit conclusions about whether the identified governance practices are equally effective across different contexts. A document-based analysis is always limited in displaying the decision-making. In addition, the ex-post analysis may create hindsight bias, as earlier decisions are assessed with knowledge about risks and consequences that became clearer only after the respective events. Future research should examine additional cases, particularly those in which crises were successfully prevented or mitigated and use interviews to better understand internal administrative decision-making. It should also investigate which institutional mechanisms effectively translate foresight into action and whether different

combinations of governance capacities are required for cyber, climate-related, and hybrid threats.

References

AEMET - Agencia Estatal de Meteorología. (2024a). *Estudio preliminar de las precipitaciones torrenciales del 29 de octubre de 2024 en la provincia de Valencia*. Gobierno de España.

AEMET – Agencia Estatal de Meteorología. (2024b). *Estudio del episodio de lluvias torrenciales del 28 de octubre al 4 de noviembre de 2024*. Ministerio para la Transición Ecológica y el Reto Demográfico.

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of public administration research and theory*, *18*(4), 543-571.

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023, May). A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd international symposium on cluster, cloud and internet computing workshops (CCGridW)* (pp. 8-15). IEEE.

Benighaus, C., & Bleicher, A. (2019). Neither risky technology nor renewable electricity: Contested frames in the development of geothermal energy in Germany. *Energy Research & Social Science, 47*, 46–55. https://doi.org/10.1016/j.erss.2018.08.022

Benito, G., Beneyto, C., Aranda, J. A., Machado, M. J., Francés, F., & Sánchez-Moya, Y. (2021). Inundaciones y cambio climático: Certezas e incertidumbres en el camino a la adaptación. *Cuadernos de Geografía, 107*, 191–216.

Bezold, C. (2018). *The history and future of anticipatory democracy and foresight. World Futures Review, 10*(4), 221–227.

Bleicher, A. (2016). Technological change in revitalization: Phytoremediation and the role of nonknowledge. *Journal of Environmental Management, 184*, 261–267. https://doi.org/10.1016/j.jenvman.2016.07.046

Bleicher, A., David, M., & Rutjes, H. (2019). When environmental legacy becomes a resource: On the making of secondary resources. *Geoforum, 101*, 18–27. https://doi.org/10.1016/j.geoforum.2019.02.018

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of contingencies and crisis management*, *15*(1), 50-59.

Boyd, E., Nykvist, B., Borgström, S., & Stacewicz, I. A. (2015). *Anticipatory governance for social-ecological resilience. Ambio, 44*(Suppl. 1), S149–S161.

Boyd, M., & Wilson, N. (2021). *Anticipatory governance for preventing and mitigating catastrophic and existential risks. Policy Quarterly, 17*(4), 20–31.

BPB – Bundeszentrale für politische Bildung. (2022). *Deutschlands Abhängigkeit von russischem Gas*. Online: https://www.bpb.de/kurz-knapp/hintergrund-aktuell/507243/deutschlands-abhaengigkeit-von-russischem-gas/

Büchele, B., Kreibich, H., Kron, A., Thieken, A., Ihringer, J., Oberle, P., Merz, B., & Nestmann, F. (2006). Flood-risk mapping: Contributions towards an enhanced assessment of extreme events and associated risks. *Natural Hazards and Earth System Sciences, 6*(4), 485–503.

Bundesministerium für Wirtschaft und Energie. (2021). *Versorgungssicherheitsprüfung gem. § 4b Abs. 2 und Abs. 3 EnWG vom 26.10.2021 im Rahmen des Zertifizierungsverfahrens der Nord Stream 2 AG*.

Bundesregierung. (2019). *Rede des Bundesministers für Wirtschaft und Energie, Peter Altmaier*.

Bundesregierung. (2021). *Gemeinsame Erklärung der USA und Deutschlands zur Unterstützung der Ukraine, der europäischen Energiesicherheit und unserer Klimaziele*.

Calof, J., & Smith, J. E. (2010). *Critical success factors for government-led foresight. Science and Public Policy, 37*(1), 31–40.

Camarasa-Belmonte, A. M., & Soriano-García, J. (2026). Turning warnings into territorial competence: Data-driven flood communication and risk education after the 2024 Valencia (Spain) cut-off low. *Geosciences, 16*(7), 29.

Camarasa-Belmonte, A. M., Zornoza-Gallego, C., Sanchis-Ibor, C., & Serrano-Lara, J. J. (2025). How effective is flood hazard mapping for emergency management? Evaluation based on the Valencia floods map of October 2024. *Ingeniería del Agua, 29*(4), 229–244.

Centre for Cyber Security (2021). State-sponsored global software supply chain attack. Danish Defence Intelligence Service. https://samsik.dk/wp-content/uploads/2026/01/20211105_CFCS-solarwinds-report-EN.pdf

Chang, Stephanie E, 'Socioeconomic Impacts of Infrastructure Disruptions' (26 Oct. 2016), in Djillali Benouar (ed.), Oxford Research Encyclopedia of Natural Hazard Science (New York, NY, online edn, Oxford Academic, 1 May 2015)

Collingridge, D. 1980. The Social Control of Technology. London: Pinter.

Congressional Research Service. (2021). *Pipeline cybersecurity: Federal programs* (R46903). https://www.congress.gov/crs_external_products/R/PDF/R46903/R46903.1.pdf

Council of the European Union. (2022). *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*

Council of the European Union. (2023). *European Union Maritime Security Strategy (EUMSS) and its Action Plan (Revised 2023).*

Croxatto, L. S., Hogendoorn, D., & Petersen, A. C. (2020). *How networked organisations build capacity for anticipatory governance in South East Asian deltas. Futures, 116*, 102512.

David, M., Wallkamm, M., & Bleicher, A. (2017). *Resource extraction technologies: Is a more responsible path of development possible? Perspectives on Global Development and Technology, 16*(4–5), 367–391.

Department of Energy. (2022). *Cybersecurity capability maturity model (C2M2), version 2.1*. Office of Cybersecurity, Energy Security, and Emergency Response.

Deutscher Bundestag, Wissenschaftliche Dienste. (2016). *Rechtliche Rahmenbedingungen der geplanten weiteren Ostseepipeline Nord Stream 2* (WD 5-3000-012/16).

Deutscher Bundestag. (2016). *Das Erdgasprojekt Nord Stream 2*.

Deutscher Bundestag. (2018). *Politischer Rahmen für Nord Stream 2*.

Deutscher Bundestag. (2020). *Antwort der Bundesregierung auf die Kleine Anfrage: Nord Stream 2* (Drucksache 19/18835).

Deutscher Bundestag. (2021). *Antwort der Bundesregierung auf die Kleine Anfrage: Gemeinsame Erklärung der Vereinigten Staaten von Amerika und Deutschlands zur Unterstützung der Ukraine, der europäischen Energiesicherheit und unserer Klimaziele* (Drucksache 19/32570).

Ely, A., Van Zwanenberg, P., & Stirling, A. (2011). New models of technology assessment for development.

Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of public administration research and theory*, *22*(1), 1-29.

European Commission. (2022). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: REPower EU Plan (COM (2022) 230 final).

European Council. (2022, October 21). *European Council conclusions, 20–21 October 2022*. Council of the European Union.

European Parliament & Council of the European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, L 194, 1–30.

European Parliament & Council of the European Union. (2021). *Decision (EU) 2021/836 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism*

European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333, 164–198.

European Parliament & Council of the European Union. (2022). EU Directive 2022/2555 on measures for a high common level of cybersecurity across the Union

European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/1032 amending Regulations (EU) 2017/1938 and (EC) No 715/2009 as regards gas storage.

European Parliament. (2016, May 10). *MEPs voice grave concerns about Nord Stream 2 project*. European Parliament.

European Parliament. (2017). *New rules on security of gas supply*. European Parliamentary Research Service.

European Parliament. (2021). *Implementation of the common foreign and security policy – annual report 2021*. European Parliament.

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. *Journal of medical internet research*, *26*, e46904.

Fekete, A., Estrany, J., & Ramírez, M. Á. A. (2025). Cascading impact chains and recovery challenges of the 2024 Valencia catastrophic floods. *Discover Sustainability*, *6*(1), 586.

Foley, R., Guston, D., & Sarewitz, D. (2015). Toward the anticipatory governance of geoengineering (working paper). Geoengineering our climate. Working paper and opinion article series. http://wp. me/p2zsRk-c8.

Fuerth, L. S. (2009). *Foresight and anticipatory governance. Foresight, 11*(4), 14–32.

Fuerth, L. S. (2011). *Anticipatory governance. PRISM, 2*(4), 19–44.

Fuerth, L. S., & Faber, E. M. (2012). Anticipatory governance practical upgrades: equipping the executive branch to cope with increasing speed and complexity of major challenges. Online: https://apps.dtic.mil/sti/tr/pdf/ADA585519.pdf

Generalitat Valenciana. (2015). *Decreto 201/2015, de 29 de octubre, del Consell, por el que se aprueba el Plan de Acción Territorial sobre Prevención del Riesgo*

de Inundación en la Comunitat Valenciana (PATRICOVA). Diari Oficial de la Comunitat Valenciana, 7649.

Ghanbari, H., Koskinen, K., & Wei, Y. (2026). From SolarWinds to Kaseya: The rise of supply chain attacks in a digital world. *Journal of Information Technology Teaching Cases*, *16*(1), 198-205.

Greenblott, J. M., O'Farrell, T., Olson, R., & Burchard, B. (2019). *Strategic foresight in the federal government: A survey of methods, resources and institutional arrangements. World Futures Review, 11*(3), 245–266.

Guston, D. H. (2007). The Center for Nanotechnology in Society at Arizona State University and the prospects for anticipatory governance. In N. Cameron & M. E. Mitchell (Eds.), *Nanoscale: Issues and perspectives for the nano century* (pp. 377–392). John Wiley & Sons. https://doi.org/10.1002/9780470165874.ch21

Guston, D. H. (2014). *Understanding anticipatory governance. Social Studies of Science, 44*(2), 218–242.

Guston, D. H. (Ed.). (2008). *Yearbook of nanotechnology in society*. Heidelberg: Springer.

Guston, D. H., & Sarewitz, D. (2020). Real-time technology assessment. In Emerging technologies (pp. 231-247). Routledge.

Heo, K., & Seo, Y. (2021). *Anticipatory governance for newcomers: Lessons learned from the UK, the Netherlands, Finland, and Korea. European Journal of Futures Research, 9*, Article 19.

Huddleston, P., Smith, T., White, I., & Elrick-Barr, C. (2022). Adapting critical infrastructure to climate change: A scoping review. *Environmental Science & Policy*, *135*, 67-76.

Jaikaran, C., & Parfomak, P. W. (2021). *Pipeline cybersecurity: Federal programs* (CRS Report No. R46903). Congressional Research Service. https://www.congress.gov/crs-product/R46903

Jaikaran, C., & Parfomak, P. W. (2022). *Pipeline cybersecurity—Updated directives* (CRS Insight No. IN12006). Congressional Research Service. https://www.congress.gov/crs-product/IN12006

Johnston, K. (2026). Anticipatory governance? Capacity for unintended policy outcomes. *Public Money & Management*, *46*(1), 1-2.

Kallo, J., & Välimaa, J. (2025). *Anticipatory governance in government: The case of Finnish higher education. Higher Education, 89*, 367–385.

Kapucu, N., Hu, Q., Sadiq, A. A., & Hasan, S. (2023). Building urban infrastructure resilience through network governance. *Urban Governance*, *3*(1), 5-13.

Kimbell, L., & Vesnić-Alujević, L. (2020). *After the toolkit: Anticipatory logics and the future of government. Policy Design and Practice, 3*(2), 95–108.

Knodt, M., Fraune, C., & Engel, A. (2022). Local governance of critical infrastructure resilience: Types of coordination in German cities. Journal of Contingencies and Crisis Management, 30(3), 307-316.

Kóczy, L. Á., Csercsik, D., & Sziklai, B. R. (2022). Nord Stream 2: A prelude to war. *Energy Strategy Reviews, 44*, 100982. https://doi.org/10.1016/j.esr.2022.100982

Krishnan, A., & Robele, S. (2024). *Anticipatory development foresight: An approach for international and multilateral organizations. Development Policy Review, 42*(Suppl. 1), e12778.

Leal Filho, W., Abeldaño Zuñiga, R. A., Sierra, J., Dinis, M. A. P., Corazza, L., Nagy, G. J., & Aina, Y. A. (2024). An assessment of priorities in handling climate change impacts on infrastructures. Scientific Reports, 14(1), 14147.

Lomba-Fernández, C., Hernantes, J., & Labaka, L. (2019). Guide for climate-resilient cities: An urban critical infrastructures approach. *Sustainability, 11*(17), 4727. https://doi.org/10.3390/su11174727

Macnaghten, P., & Owen, R. (2011). Good governance for geoengineering. Nature, 479(7373), 293-293.

Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, 11(5), 537-545.

McCabe, R., & Flynn, B. (2024). Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure. *European Security*, *33*(2), 324-344.

Mikac, R. (2023). Protection of the EU's critical infrastructures: results and challenges. *Applied cybersecurity & internet governance*, *2*(1), 1-25.

Miles, I. (2010). The development of technology foresight: A review. Technological Forecasting and Social Change, 77(9), 1448–1456.

MITECO – Ministerio para la Transición Ecológica y el Reto Demográfico. (2025a). *Plan para la recuperación y mejora de la resiliencia frente a inundaciones en el territorio afectado por la DANA del 29 de octubre de 2024*.

MITECO – Ministerio para la Transición Ecológica y el Reto Demográfico (2025b). *Sistema Nacional de Cartografía de Zonas Inundables (SNCZI)*.

Monstadt, J., & Schmidt, M. (2019). Urban resilience in the making? The governance of critical infrastructures in German cities. *Urban studies*, *56*(11), 2353-2371.

Nelson, J. P., Selin, C., Lambert, L., & Guston, D. H. (2023). *Amplifying the call for anticipatory governance. Journal of Responsible Innovation, 10*(1).

Nolte, I. M., & Lindenmeier, J. (2024). Creeping crises and public administration: a time for adaptive governance strategies and cross-sectoral collaboration?. Public Management Review, 26(11), 3104-3125.

Pestana, G., & Sofou, S. (2024). Data governance to counter hybrid threats against critical infrastructures. *Smart Cities*, *7*(4), 1857-1877.

Priebe, M., Veit, S., & Warnke, P. (2025). *Understanding foresight–policy interactions: The role of institutionalization. Futures & Foresight Science, 7*(1).

Pursiainen, C., & Kytömaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient infrastructure*, *8*(sup1), 85-101.

Ramos, J. M. (2014). *Anticipatory governance: Traditions and trajectories for strategic design. Journal of Futures Studies, 19*(1), 35–52.

Reuters. (2026, July 1). Germany indicts Ukrainian over Nord Stream pipeline blasts, German media report. https://www.reuters.com/world/germany-indicts-ukrainian-over-nord-stream-pipeline-blasts-german-media-report-2026-07-01/

Rhein, B., & Kreibich, H. (2025). Causes of the exceptionally high number of fatalities in the Ahr valley, Germany, during the 2021 flood. *Natural Hazards and Earth System Sciences*, *25*(2), 581-589.

Rotolo, D., Hicks, D., & Martin, B. R. (2015). What is an emerging technology?. *Research policy*, 44(10), 1827-1843.

Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. *arXiv preprint arXiv:2412.08084*.

Russell, M. (2021). *The Nord Stream 2 pipeline: Economic, environmental and geopolitical issues*. European Parliamentary Research Service, European Parliament.

Sakthivel, A. (2025). Agentic Ai In the Enterprise: How Autonomous Ai Systems Will Reshape Business Strategy, Operations, and Leadership. *Well Testing Journal*, *34*(S3), 767-785.

Soldi, G., Gaglione, D., Raponi, S., Forti, N., d'Afflisio, E., Kowalski, P., Millefiori, L. M., Zissis, D., Braca, P., Willett, P., Maguer, A., Carniel, S., Sembenini, G., & Warner, C. (2023). Monitoring of critical undersea infrastructures: The Nord Stream and other recent case studies. *IEEE Aerospace and Electronic Systems Magazine, 38*(10), 4–24. https://doi.org/10.1109/MAES.2023.3285075

Sonesson, T. R., Johansson, J., & Cedergren, A. (2021). Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Safety science*, *142*, 105383.

Statistisches Bundesamt. (2022). Fakten zur Gasversorgung: Erdgas wichtigster Energieträger für Industrie und private Haushalte (Pressemitteilung Nr. 044). Online: https://www.destatis.de/DE/Presse/Pressemitteilungen/2022/07/PD22_N044_43.html

Tanguay, L., Herzog, L. M., Audet, R., Beisner, B. E., Martin, R., & Pahl-Wostl, C. (2023). Opportunities for and barriers to anticipatory governance of two lake social–ecological systems in Germany and Canada. *People and Nature, 5*(3), 911–928. https://doi.org/10.1002/pan3.10464

Thistlethwaite, J., & Henstra, D. (2026). Policy instruments to strengthen the cybersecurity of critical infrastructure. *Journal of Cyber Policy*, 1-21.

Transportation Security Administration. (2021). *Security Directive Pipeline-2021-01: Enhancing pipeline cybersecurity*. U.S. Department of Homeland Security.

Transportation Security Administration. (2022). Enhancing surface cyber risk management. *Federal Register, 87*, 73527–73538.

Transportation Security Administration. (2022). *Security Directive Pipeline-2021-02C: Pipeline cybersecurity mitigation actions, contingency planning, and testing*. U.S. Department of Homeland Security.

Transportation Security Administration. (2024). *Security Directive Pipeline-2021-01D: Enhancing pipeline cybersecurity*. U.S. Department of Homeland Security.

Transportation Security Administration. (2024). *Security Directive Pipeline-2021-02E*. U.S. Department of Homeland Security.

U.S. Congress, House Committee on Homeland Security. (2021). *Cyber threats in the pipeline: Using lessons from the Colonial ransomware attack to defend critical infrastructure*. https://www.congress.gov/117/chrg/CHRG-117hhrg45310/CHRG-117hhrg45310.pdf

U.S. Department of Homeland Security (2021). After-Action Report on Colonial *Pipeline.*

U.S. Government Accountability Office. (2018). *Critical infrastructure protection: Actions needed to address significant weaknesses in TSA's pipeline security program management* (GAO-19-48). https://www.gao.gov/products/gao-19-48

U.S. Government Accountability Office. (2019). *Critical infrastructure protection: Actions needed to address weaknesses in TSA's pipeline security program management* (GAO-19-542T). https://www.gao.gov/products/gao-19-542t

U.S. Government Accountability Office. (2021). *Critical infrastructure protection: TSA is taking steps to address some pipeline security program weaknesses* (GAO-21-105263). https://www.gao.gov/products/gao-21-105263

van der Steen, M. A., & van Twist, M. J. W. (2013). Foresight and long-term policy-making: An analysis of anticipatory boundary work in policy organizations in

The Netherlands. *Futures, 54*, 33–42. https://doi.org/10.1016/j.futures.2013.09.009

Warren, K. (2025). *Overcoming challenges to New Zealand public sector risk management. Policy Quarterly, 21*(4), 23–36.

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in digital health*, *4*, 862221.

Wolbach, M., & Talukder, R. (2025). The value of EU research projects in critical infrastructure protection. Terroryzm-studia, analizy, prewencja, (Special Issue), 315-339.

Yin, R. K. (2018). *Case study research and applications* (Vol. 6). Thousand Oaks, CA: Sage.

Zhang, F., & van Valkengoed, A. M. (2025). Determinants of climate change adaptation in public organizations: a meta-analysis. *Climatic Change*, *178*(8), 147.