Regulating a Moving Nerve

On Legally Defining Critical Infrastructure

*Kristian Cedervall Lauta**

Regulation of critical infrastructure (CI) is in vogue; and accordingly every government presently develops legal governance regimes. In this paper, I try to analyse some of the present efforts to identify and govern CI. I argue that while the legal definitions introduced contribute little to the actual identification of critical infrastructure, they alter the responsibility and modus operandi of the identification. Political discretion is re-organized into administrative decisions. By relying on similar observations from risk sociology, I set out to criticize the present implementation for masking the hard political choices inherent in the work with CI, and thereby creating a dysfunctional governance regime for the protection of CI.

I. Introduction

I live with my family in Beirut, Lebanon. I am reminded on a daily basis of the value of societal infrastructure. Every day we experience scheduled three-hour-power cuts, municipal water-availability is entirely depended on the preceding winter's rainfall, central heating is non-existing, and Lebanon has one of the worst overall internet-connections in the entire world. In fewer words, the public common infrastructure is flawed to say the least. Yet, while such disturbances, without a doubt, would be critical to the function of daily life say in Denmark or Switzerland, it is not in Lebanon. We have a power-generator that automatically goes on during power-cuts, a 2000-liter water-tank on the roof, our own furnace in the basement, and a $150 a month internet-connection (providing mesmerizing 2 Mbit/s, wired through an extra power back-up to ensure an unbroken deliverance of internet). Those who cannot afford such luxuries – mind you; the vast majority of the Lebanese population – simply adjusts. They do not watch television or use their appliances during power-cuts; they gather rainwater to flush the toilets; and they live (happily) without YouTube and Facebook on a daily basis. For all I know, our indispensable housekeeper, Rita, deals significantly better with the continuous infrastructural crisis than we do. In other words, the failures of infrastructure services are not experienced as *critical* by the population of Lebanon on a day-to-day basis.[1]

What is considered *critical* in a given society is inherently depended on the level and character of the expectations to daily life. Furthermore, it is a political decision which level of services a society should provide to its citizens, who should provide it, and with what consistency. Even if this, as in the case of Lebanon, means leaving the accommodation of the country's infrastructure almost entirely to its citizens. While this seems like an almost naïvely simple insight – it is easily forgotten in a modern complex society.

In this paper I aim to examine the ongoing efforts to legally define critical infrastructure as part of disaster management. The overall argument of the paper is that while legal definitions of, and governmental programs on, critical infrastructure (CI) have little material value in terms of actually identifying CI, they fundamentally change *the way* in which critical infrastructure is identified. While the increased regulatory focus on CI-protection (CIP) is well timed, and called for, the implementation of CI designation through law also raises concern. As we adopt legislations, definitions and comprehensive programs, the responsibility for the identification, maintenance and protection of CI shifts. Thus, increasingly CIP is no longer a political problem, but become an admin-

* Assistant Professor, PhD, Center for Enterprise Liability, Faculty of Law, University of Copenhagen. The article is made as part of a post-doctoral project under the Danish Maritime Cluster. Furthermore, it is published as part of University of Copenhagen 2016 excellence program for interdisciplinary research-project Changing Disasters. For correspondence: klau@jur.ku.dk.

1 Obviously, the lack of well-developed infrastructure has other consequences for a society. For Lebanon, the lack of a well-functioning infrastructure might be the biggest factor limiting industrial and economic growth.

istrative, legal problem. That is, instigating legal definitions and accompanying programs of CI does not make it easier to identify CI, but changes *who* is responsible and thereby also, though less obvious, *how* the identification takes place.

The paper embarks by investigating how critical infrastructure is understood today, and how the concept is transformed into an institutional, legal concept (section II). This latter investigation will draw up examples of legal definitions (II.1) and present a case of CI-protection (CIP) from Switzerland (II.1a). I will thereon present some contemporary insights from risk sociology describing a change in the implementation and function of risk in modern society in general and in CIP in particular (section III). These insights are presented to allow for a more general critique (section IV) of the present regulatory efforts, before finally, drawing up the paper's findings (section V).

II. Critical Infrastructure: The Heart of a Nation

In spite of its intuitive relevance, critical infrastructure is not a concept traditionally applied in disaster management. The concept first entered modern government with US President Bill Clinton's establishment of a national program on "Critical Infrastructure Protection" in 1998.[2]

Obviously, societies have made categorical prioritizations of its infrastructures before this time. As part of defence planning, authorities have systematically analysed society, and assigned special attention to particularly vulnerable and/or important key points at least since the 1940s.[3]

In an industrialized, non-networked society this was an accomplishable, meaningful and fairly straightforward task.[4] Ironically, CI thereby only came into existence as an institutionalized government-tool, as it became problematic to identify the critical from the non-critical.

Today's societies are in this regard particularly difficult entities to navigate in. They are systems constituted by many adaptive and dynamic parts, which, often co-creates fundamentally unforeseeable outcomes (for better and for worse),[5] including second- and third order effects. Therefore, modern theory on the management and identification of critical infrastructure often addresses ways to decode, balance, and control these "interdependencies" (or merely "dependencies") that are characteristic in a complex system: physical, virtual, cultural and geospatial. With the purpose of mitigating or *managing* these complexities network-theory[6], vulnerability analysis[7] or resilience-considerations[8] are applied.

Thus, while it often seems easy to agree on what is surely functionally critical in a society (electricity, internet, water, food, money), both the exact limit between critical and non-critical, and the concrete identification of critical infrastructures, are problematic in practice. Therefore, the idea of "critical infrastructure" is troublesome politically (actually deciding on the borderline between critical and non-critical) as

2 See Presidential directive PDD-63 of May 1998. Altered by Presidential Directive HSPD-7 for Critical Infrastructure Identification, Prioritization, and Protection from December 2003.

3 See the really well-written article on the Cold War's possible implications for urban planning in the US, Peter Galison, 'War against the Center', *Grey Room,* 4 (2001), 5-33. According to Galison, the fear of a potential nuclear attack on a US city created "the architectures of dispersion, counter-urbanization, and non-hierarchical grids", *ibid.*, at 33. The article convincingly points out that critical infrastructure planning is much older than the Clinton administration, even though the aim, means and the complexity of the exercise is changing.

4 Galison documents how difficult it was for the British to identify "the interconnections that held together the German economy and war machine", and how this exercise became self-reflexive during the cold war, *ibid.*, at 8.

5 Or a complex adaptive system (CAS), see more with John H. Holland, 'Studying Complex Adaptive Systems', Journal of Systems Science and Complexity, 19/1 (2006), 1-8.

6 See for instance the highly functional approach suggested by Ted Lewis in Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation* (Wiley, 2006). For a literature review putting emphasis on network theory, see Laurie Anne Schintler et al., 'Moving from Protection to Resilliency: A Path to Securing Critical Infrastructure', *Critical Infrastructure. Reliability and Vulnerability* (Springer, 2007) at 297f.

7 See for instance A.T. Murray and T.H. Grubesic, *Critical Infrastructure. Reliability and Vulnerability* (Advances in Spartial Science: Springer, 2007). This anthology contains a number approaches using vulnerability analysis to model critical infrastructure protection within a given sector, hereunder transportation and electricity.

8 Schintler et al., 'Moving from Protection to Resilliency: A Path to Securing Critical Infrastructure'. See also Arjen Boin and Allan Mcconnell, 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resillience', *Journal of Contingencies and Crisis Management,* 15/1 (2007), 50-59. In this article the authors advocates to entirely leave behind traditional crisis thinking in conjuncture with accidents and disasters in the critical infrastructure and rather build and support local and community resilience. See also in this regard the influential mathematician and philosopher Nassim Nicholas Taleb, not least Nassim Nicholas Taleb, *The Black Swan* (London; New York: Penguin Books, 2010).

well as operably (figuring out what is critical to ensure the function in matter). This is definitely the case in a globally connected information-society. Yet, it is no less important to be able to prioritize the protection of society's infrastructure today than, say, 40 years ago.

One of the main governance strategies applied to cope with this increasing complexity has been to develop legal programs on critical infrastructure protection (CIP). Thus, in the course of the last 15 years, we have witnessed an explosion in legal instruments regarding CI government. As Alessandro Lazari notes in *European Critical Infrastructure*, policy makers have produced "wagon loads of legislation, industrial standards, security certification and labelling, multiplied rules, procedures and protocols"[9]. For this purpose governments and public officials have worked diligently to finitely capture which parts of the society's infrastructure should be considered critical, and which should not. Thus, almost any highly developed country today has a working (legal) definition and an accompanying (legal) program on the governance of critical infrastructure.

1. Legal definitions of CI

Definitions of critical infrastructure are overall similar. Some take departure solely in an asset's or element's (e.g. a bridge's) function in a system,[10] while others focus purely on the consequences of a break down.[11] Some definitions include sectorial or specific functional considerations,[12] while yet others leave it to pure considerations of causality to determine whether an asset is critical.[13] In spite of these small differences, they are all characterized by attempting to capture what is necessary to secure the continuation of the society in question (due to either the impact of failure or present function in society).

The Canadian definition, for example, specifically focuses on "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government"[14]. Similarly, critical infrastructure in the Netherlands must be able to cause "major social disturbance", "tremendous loss of life" or "economic damage".[15] The German definition, however, fully hedges against unforeseen incidents by referring to "sustained supply shortages, significant disruption of public safety and security, or *other dramatic consequences*" [italics added].[16]

The national definitions of critical infrastructure are supplemented at the European level via the so-called European Program for Critical Infrastructure Protection (EPCIP), which defines critical infrastructure as:

> "(...) an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have

9 Alessandro Lazari, *European Critical Infrastructure Protection* (Springer, 2014) at 104.

10 See for instance the Swedish MSB's definition: "Fysisk struktur vars funktionaltiet bidrar till att säkerställa upprätthållande av viktiga samhällsfunktioner" [physical structures which function contributes to secure the maintainance of important society functions], cf. "Ett fungerande samhälle i en föränderlig värld, Publ. Nr MSB 266 – dec 2011, p. X.

11 See for instance the Swiss definition: "Kritische Infrastrukturen sind Infrastrukturen, deren Störung, Ausfall oder Zerstörung gravierende Auswirkungen auf die Gesellschaft, die Wirtschaft und den Staat hat" ["Critical infrastructures are infrastructures whose disruption, failure or destruction would have a serious impact on the functioning of society, the economy or the state"], cf. "Nationale Strategie zum Schutz kritischer Infrastrukturen" of 27 Juni 2012, p. 7718, available on the internet at http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.parsysrelated1.82246.downloadList.6453.DownloadFile.tmp/natstratski2012d.pdf (last accessed on 23 October 2014).

12 See for instance the Norwegian definition: "Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse." [critical infrastructure is the installations and systems that are entirely necessary to maintain the society's critical functions, which in turn covers the society's basic needs and the feeling of comfort among the population], cf. Ullring et al: "Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner", Norges offentlige utredninger 2006: 6. Innstilling fra utvalg oppnevnt ved kongelig resolusjon 29. oktober 2004.

13 See the description of the DHS-approach in the following.

14 See the National Strategy for Critical Infrastructure, available on the internet at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf (last accessed on 23 October 2014).

15 See Kathryn Gordon and Maeve Dion, 'Protection of "Critical Infrastructure" and the Role of Investment Policies Relating to National Security', (OECD, 2008). For more on CIP in the Netherlands see Eric Luiijf, Helen Burger, and Marieke Klaver, 'Critical Infrastructure Protection in the Netherlands: A Quick-Scan', *EICAR* (Copenhagen, 2003).

16 See Bundesministerium Des Innern, 'National Strategy for Critical Infrastructure Protection (Cip Strategy)', (Berlin: Federal Republic of Germany, 2009).

> a significant impact in a Member State as a result of the failure to maintain those functions".[17]

Focusing on mainly cross-border infrastructures, the EPCIP thereby supplements the national level with an international governance scheme.[18] Many other definitions could have been highlighted.[19] While these definitions supposedly should provide direction for the identification of critical infrastructure, they leave little or no guidance in terms of actually understanding what "serious impact", "essential for the maintenance of vital societal functions" or "dramatic consequences" means or should be interpreted. They are at best "fuzzy"[20].

In his analysis of the present critical infrastructure frameworks, Lazari notes (...) "it seems that the legal frameworks that should govern such a delicate environment are, in some cases, experiencing serious difficulties in reaching the target". I will, in the following, go one step further than Lazari. The definitions basically leave the interpreters with the two problems, they were initially adopted to solve: (a) How can we, *a priori*, establish the necessary causalities to identify critical parts of a complex system; and (b) even if we can, who is to determine what "serious impact" is (i.e. is it a serious impact for USA or for Maryland that Baltimore down-town is without power for a few days). However, the definitions and CI-programs are not without effect. While the problems as such might be unsolved, the responsibility for their solution shifts. This shift in both governance and *governmentality* is, as we shall see below, well-described in risk studies. In order to investigate the consequences of the collective interest in regulating CI I will analyse a case-country often highlighted for its comprehensive approach to CIP.

Through the case I hope to demonstrate that, when legally defining CIP, the interpreter of what CI is, and thereby the rationale of CIP, changes. The "fuzzy" definitions, and the problems inherent in CIP, are thereby no longer given efficacy through political decision, but rather through technocratic, administrative interpretation. This changes what is considered CI, but also opens a realm of responsibility for potential mistakes. I will elaborate on this in section IV.

a. Case Study: The Heart of Switzerland

Switzerland is most likely the worst possible country to study and simultaneously claim to say something general about the world. The country has a special tradition of democratic governance, is not member to the European Union, though geographically in European heartland, and has a longstanding history of scepticism towards central government. Yet, Switzerland has one of the best-developed, modern and reflexive CIP-strategies in the world. In spite of Switzerland's particularities, I will in following analyse the Swiss approach to CI, considering this an exemplary case of CIP.[21]

The Swiss defines critical infrastructure similarly to the definitions highlighted above:

> "Kritische Infrastrukturen sind Infrastrukturen, deren Störung, Ausfall oder Zerstörung gravierende Auswirkungen auf die Gesellschaft, die Wirtschaft und den Staat hat"[22] ["Critical in-

17 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, art. 2(a).

18 NATO also entertains a CI-program, available on the internet at: http://www.hazar.org/blogdetail/blog/understanding_nato's_new_critical_infrastructure_protection_cip_politics_common_efforts_and_solidarity_830.aspx (last accessed on 23 October 2014).

19 Bill Clinton's commission ended up defining CI as "Systems and assets, whether physical or virtual, so and vital that the incapacity or destruction of such may have a debilitating impact on national security, national economic security, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction", cf. the Presidential Commission on Critical Infrastructure Protection (1997): Final report. The British definition is simpler: "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends.", available on the internet at http://www.cpni.gov.uk/about/cni/ (last accessed on 23 October 2014). An overview of contemporary approaches to critical infrastructure in drawn up in Jose M. Yusta, Gariel J. Correa, and Lacal-Arántegui, 'Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art', *Energy Policy,* 39 (2011), 6100-19. See also D.A. Belluck et al., 'Environmental Security, Critical Infrastructure and Risk Assessment: Definitions and Trends', in B. Morel and I. Linkov (eds.), *Environmental Security and Environmental Management: The Role of Risk Assessment* (Springer, 2006).

20 Lazari, *European Critical Infrastructure Protection* at 4.

21 In the following I will use this model as my subject of criticism. Rather than a straw man fallacy, I hope that it serves as an ideal type for the management of critical infrastructure. The aim is thereby not to claim that all countries working with CI works like Switzerland, but that the Swiss-model is an ideal type of something that influences other countries governance-systems, and as such should be subject to criticism.

22 "Nationale Strategie zum Schutz kritischer Infrastrukturen" of 27 Juni 2012, p. 7718, available on the internet at http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.parsysrelated1.82246.downloadList.6453.DownloadFile.tmp/natstratski2012d.pdf (last accessed on 23 October 2014).

> frastructures are infrastructures whose disruption, failure or destruction would have a serious impact on the functioning of society, the economy or the state"].[23]

The underlying regulatory program covers ten "critical sectors" (for example energy) grouped into 28 "sub-sectors" (for example oil supply).[24] The sectors and sub-sectors were identified through a comprehensive process, and approved by the Federal Council (the Swiss equivalent to a Federal government). The 28 subsectors are then re-grouped into three categories depending on their criticality: "very high criticality", "high criticality" and "regular criticality".

The criticality-measure refers to the importance of the subsector in terms of interdependency, the population, and the economy (and not the sectors' isolated importance for society or its mission-criticality). While banks have very high criticality; civil defence and research institutes have regular criticality, and while rail transportation has very high criticality, media have high criticality. Within each subcategory individual CI-elements are identified and inventoried in a national "CIP Inventory" (SKI-Inventar). This is coordinated by the Federal Office for Civil Protection "in cooperation with the responsible authorities of the federal administration, the Cantons, and the operators". According to the strategy, the inventory is "a basis for planning and decision making processes at the various levels (federal administration, Cantons, and operators)"[25]. In other words based on this system of sectors, sub-sectors, criticality categorization and individual assessments, Swiss authorities are to make concrete prioritizations in case of an incident, as well as decisions on general resource allocation. Thus, this categorization of a subsector or CI-element has implications not only for the protection of a society during crisis, but also for the preventive measures initiated (as well as daily maintenance).

The Swiss CIP program relies on a principle of integral risk management, which consist of two phases or parts. Initially, "a detailed threat and risk assessment is performed", thereon this assessment is applied across five temporal phases around an incident: Prevention (e.g., structural-technical or zoning measures); Preparation (e.g., contingency and business continuity planning); Intervention (e.g., physical protection through security staff and standardized crisis communication); Recondition (e.g., temporary restoration of infrastructures); Reconstruction (e.g. of infrastructures).[26]

Furthermore, a thoroughly "standardized process" is followed in the development of protection concepts:

> "Initially, the existing responsibilities and regulations are reviewed, and protection goals are defined. In the next step, an in-depth analysis of threats and vulnerabilities is conducted. Subsequently, the risk analysis and the existing regulations are taken as the baseline to verify whether the protection goals have been achieved. If not, appropriate measures are elaborated. (...) This entire process is repeated periodically".[27]

Overall an impressive administrative process designed to involve and embed the necessary technical and societal knowledge in every step of the way, and anchored in a firm believe that this knowledge will provide the best possible defence against threats towards society.

In other words, this wet, positivistic dream of any engineer, entirely rationalizes the approach to CI, leaving the assessment and decision-making up to our ability to map the existing system (and the risks against it). While the Swiss authorities, according to a standardized process, periodically asks the government to consider the implementation of concrete initiatives or adjustments of the CIP, the measurements, recommendations and presumptions relies on advanced, technical knowledge. It is embedded in an impressive clockwork of modern administration.

In order to understand the consequences of approach taken by the Swiss authorities, I will in the following introduce a few perspectives on the general perception of risk that we have seen developing through the 90's, in particular in the English-speaking world.[28] Thus, the Swiss institutionalization of

---

23 Notably the likelihood of a given section of the infrastructures disruption, failure or destruction is unimportant to its categorization as "critical".

24 See The Federal Council's Basic Strategy for Critical Infrastructure Protection, 18 May 2009

25 *Ibid*.

26 *Ibid*., section 4.

27 *Ibid*.

28 The link between risk assessment and critical infrastructure also have a more institutional nature, as "most critical infrastructure protection plans have been based on risk management frameworks", cf. Yusta, Correa, and Lacal-Arántegui, 'Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art', at 6113.

CI identification seems to follow the trajectories of a risk perception as something to be calculated and *managed*[29], rather than discussed and politically decided upon. The program on CIP thereby comes to introduce and sustain a somewhat functionalistic technocratic understanding of risk, with a series of implications for its governance.

III. The Realm of Lawyers and Engineers: The Risk Management of Everything.

There can be little doubt that risk[30] plays a major role in the formation and governing of modern society.[31]

Since the 70's the concept of risk seems to become increasingly relevant to the governance of states. In particular in the 90's risk seems to have gained momentum as a central, perhaps *the* central, governance grid. Professor of accounting and former director of Centre for the Analysis of Risk and Regulation (CARR) Michael Power fittingly describes this expansion of the realm of risk analysis as the "risk management of everything".[32] According to Power risk has become "an organizing concept as never before"[33], creating a governance framework for both public and private institutions. Power claims that, "risk analysis, the traditional technical home territory of risk management, has been subsumed within a larger accountability and control framework"[34]. Risks are in other words increasingly *managerialized*, and simultaneously colonize important governance areas traditionally undertaken by the political branch of government (i.e. critical infrastructure).

The British anthropologist Steve Rayner supplements that this *managerialization* of risk has consequences for political life and decision-making as such. In line with Power's suggestions, Rayner suggests that we now live in an "age of assessment"[35] or what has earlier been described as the "century of the professional expert"[36]. According to Rayner "a potential pathology arises from a subtle shift from the idea that science should *inform* policy to the idea that science should *drive* policy"[37]. Therefore, the rise of risk, according to Rayner, stipulates two important developments, (1) a growth of risk governance ("as government shifts towards governance, its policy discourse is increasingly reduced to a discourse of science which, in its turn, is reduced to one of risk"[38]) and (2) a change in the instrument of *governmentality*[39]. Accordingly, "it seems likely that reliance on expert assessments of all sorts, including risk assessments, has contributed to the decline of politics. In this context, risk is a metric that facilitates governmentality, with its attendant shifting of responsibility and blame!"[40]. It is exactly this shift, and its' consequences for law, that I believe can be traced, and should be attentively addressed in the context of CIP.

Power and Rayner share the overall idea that risk is a discourse replacing political elaboration with technical knowledge, and that this in turn changes the role and *modus operandi* of politics as such.[41] When analysing the Swiss CI-identification in this light, it becomes clear that every aspect of the standardized process used to identify critical infrastructures relies on technical knowledge and an underlying risk-assessment. Advanced technical calculations are crucial and absolutely determining in the integral risk management, as well as the standardized procedure. This means that every small decision along the

29 The American sociologist Craig Calhoun excellently discusses the consequences of this development in the broader field of emergencies, cf. Craig Calhoun, 'A World of Emergencies: Fear, Intervention, and the Limits of Cosmopolitan Order', in Didier Fassin and Mariella Pandolfi (eds.), Contemporary States of Emergency: The Poltics of Military and Humanitarian Interventions (New York: Zone Books, 2010).

30 In this paper risk is to be understood as something "equated with hazards and dangers" Michael Power, *The Risk Management of Everything. Rethinking the Polictics of Uncertainty* (London: DEMOS, 2004) at 14. And thereby not in line with ISO 31000 on Risk Management as "the effect of uncertainty on objectives".

31 Ulrich Beck, *Risk Society*, ed. Mike Featherstone (Theory, Culture and Society: SAGE, 2008).

32 *Ibid*.

33 *Ibid*., at 13.

34 *Ibid*.

35 Steve Rayner, 'Democracy in the Age of Assessment: Reflections on the Roles of Expertise and Democracy in Public-Sector Decision Making', *Science and Public Policy,* 30/3 (2003), 163-70.

36 H. Perkin, *The Rise of Professional Society: England since 1880* (London: Routledge and Kegan Poul, 1989).

37 Rayner, 'The Rise of Risk and the Decline of Politics', at 166.

38 *Ibid*., at 167.

39 *Ibid*., at 166f. It remains a somewhat "loose" concept with Rayner. Rayner understands *governmentability* as "the ability of the state to replace government by coercion and direct exercise of authority (…) by more subtle instruments of social control, largely by gathering and channeling information", cf. Ibid., at 167.

40 *Ibid*., at 171.

41 This observation seems to follow the trajectory of the concept of *techno-politics* from anthropology, see more Brian Larkin, 'The Politics and Poetics of Infrastructure', *The Annual Review of Anthropology,* 42 (2013), 327-43.

way is guided by the assessment and application of expert knowledge – knowledge on the administration, the infrastructure system in matter, and, obviously, nature.

This idea of risk and management belongs in the realm of engineers and lawyers; a system of rational thought and calculable outcomes. For the engineers because their ability to model the world, through rational models and complicated mathematical models, are central to risk assessment and mapping. For the lawyers because basing systems on such models follows perfectly the trajectories of transparency, accountability, and societal systematization. Thereby as society becomes bureaucratized, law becomes an entirely central tool both in terms of governing, and assigning responsibility.

IV. Critique: "Man Plans – God Laughs"

In our shared enthusiasm to create systems for protection of critical infrastructure, we must not forget the contingent character both in the assessment of risks against our society, and the complexity of society itself. The internalization and systematisation of uncertainty is a political, ideological manoeuvre driven through social and political constructions; risk is therefore, in the words of the Luhmann, a 'phenomenon of multiple contingency, which consequently offers different observers differing perspectives'[42]. Accordingly, decisions on what is critical are inherently normative; and decision with major potential consequences for the society.

Modern society is complex and interdepended and the uncertainty this brings along is challenging the pre-dominant risk-perception. When a technocratic CI-approach is applied, the idea of what is most important in society becomes entirely depended on the knowledge and technical know-how of the engineer writing the algorithm, and the lawyer interpreting the threshold for "serious impact".[43] This is problematic, as it masks the fundamental political choices inherent in this exercise. While thereby keeping the politicians ignorant of the actual state of the world, it does not ultimately enhance our ability to designate critical infrastructure.

In that light, it seems to be extra problematic to mask the hard choices behind advanced calculations and legal bureaucracy. Rather it should be an aim to address these choices in politically on a continuous basis. However, such an exercise takes substantial political courage, and a political environment able to comprehend and address the risks in question. Power puts it this way:

Risk-based regulation necessarily embodies the idea that failures are possible. However, the degree to which regulators and politicians are able to be publicly explicit about this will vary according to the perceived reputational and political risks of doing so.[44]

If the responsible political branch maintains that we through a general definition of critical infrastructure can address the complexity of the enterprise, they fail to acknowledge the inherent normative character of *criticality*. This is of course simultaneously attractive: both for the public officials not forced to formulate the sharp, but troublesome, questions, and for the politicians not forced to answer them.[45]

According to the American sociologist Sheila Jasanoff, the (re-)politicization of risk is already ongoing. According to Jasanoff "risk spilled out of the envelopes of measurements and prediction and became incalculable". Thereby, Jasanoff suggests that risk has already "escaped the control of expert mangers and [therefore] became a problem for democratic politics".[46]

She addresses this movement of risk (back) from the technical to the political domain as the distinction between government and governance:

Risk has shifted its locus almost imperceptibly form being principally a managerial problem to one that is seen also as deeply political; in other words, the bureaucratic task of risk management is now seen to be just one aspect of the broader enterprise of risk governance. Risk management was traditionally con-

42 Niklas Luhmann, *Risk: A Sociological Theory* (New York: Aldine De Gruyter, 1993) at 16.

43 This is, obviously, an idealized (American) model, but the designation of CI is unquestionably increasingly an administrative matter in Europe as well.

44 Power, *The Risk Management of Everything. Rethinking the Polictics of Uncertainty* at 22.

45 Such bureaucratization can even be suspected of being a deliberate political strategy: "On the one hand the development of specific regulatory regimes appears to be a rational response, much like auditing, to the management of first-order risks to health, financial security, etc. On the other hand, the very existence of such regulatory agencies can be interpreted as responsibility-shifting strategy by central government concerned with its reputation" Power, *The Risk Management of Everything. Rethinking the Polictics of Uncertainty* at 60.

46 Sheila Jasanoff, 'Beyond Calculation. A Democratic Response to Risk', *Disaster and the Politics of Intervention*, 14-40 at 36.

sidered a domain for experts. Risk governance by contrast requires the involvement of citizens and their political representatives.[47]

While this might be true for some instances of risk governance, I believe it is not the case for CIP. Even if the points raised by Jasonoff are no less relevant the governance of critical infrastructure; critical infrastructure governance seems to be increasingly embedded in a technocratic approach, as regulations and institutions emerge. The elaborate procedures institutionalized in the Swiss CI-approach accounted for above, create a technocratic jungle only navigable by experienced, highly educated experts. If anything, these procedures effectively re-enforce a technocratic risk model.

Furthermore, when risk is bureaucratized, responsibility follows troop. Power even claims that "institutional responses are very much guided by cultural demands for control, accountability and responsibility attribution" (Power 2004: 38). In other words, that the present efforts are guided by a general demand of more (legal) accountability. Notwithstanding whether the *depolitization* of CIP is in fact driven by a "cultural demand" for accountability, it is unarguably a direct consequence: When decisions on whether a given level of risk is "acceptable" rely on technocratic processes and knowledge, this decision become subject to legal scrutiny, and potentially liability.

In a best-case scenario this could lead to responsibility aversion:

> "In short, the risk management of everything amplifies responsibility aversity across a wide range of possible risk appetites. It is the specific dynamics of these amplification processes in society, rather than any generalised aversion to risk-taking at the individual level, which potentially inhibits organisational innovation".[48]

In the Swiss example, it is reasonable to assume that the public officials responsible for recommending e.g. the priority of CI or a concrete asset's inclusion in the CI-inventory will be precautious in doing so. Pursuing a similar approach to CIP, the American authorities had in 2009 included 77.000 assets in their CIP-inventory. With 77.000 elements needed to be prioritised it seems reasonable to claim that the very idea of prioritization is rendered absurd. In a best-case scenario such risk aversion could lead to nothing beyond wasted efforts and an highly inefficient prioritisation system.

In the worst case scenario however, central political and societal decisions are effectively hidden from politicians, and left to public officials, engineers and lawyers with major implications both for the public officials in question (potentially facing liability for such decisions) and for the political life of society. The *institutionalization* of CI governance schemes thereby also affects who could be legally responsible for the consequences of a CI-breakdown. While it makes perfect sense that decision and accountability should be tied together, it has major implications to leave these with institutions and individuals appointed rather than elected.

VI. Conclusion: Pushback

Complexity is no obstacle or excuse for not regulating certain particularly risky industries (e.g. the nuclear industry, the offshore sector, or chemical plants) or for acknowledging that Frankfurt airport is, for obvious reasons, more important than Spjald airstrip in Western part of Denmark. There are infrastructures in a given society that are more critical than others, and obviously we can, and should, identify and protect these assets more intensively than desolate islands. However, this does not mean that we can effectively leave this process to pure bureaucratic processes by drawing up legal definition and complicated models of governance. By making critical infrastructure manageable through legal definitions, algorithms, and risk mappings we risk moving fundamentally political decisions to engineers and lawyers, which in turn could face liability for making these hard, but necessary choices.

Risk analysis and models have blindsides, but it is the best we've got. As Douglas and Wildavsky famously opens their famous analysis of risk and culture from 1983: "Can we know the risks we face, now or in the future? No, we cannot, but yes, we must act as if we do."[49].[50] Thus, the claim in this paper is not

47 *Ibid.*, at 19.

48 Power, *The Risk Management of Everything. Rethinking the Polictics of Uncertainty* at 45.

49 Douglas and Wildavsky, *Introduction to Risk and Culture* (1983) at 1.

50 See also Power, *The Risk Management of Everything. Rethinking the Polictics of Uncertainty* at 59ff.

that we should stop listening to the technical experts when identifying critical infrastructures. The claim is that societies need to find a way to reintroduce clear political prioritization into this process. Rather than believing we can calculate, what is the most important to a society, we must remain reflective of the fundamental political, normative character of this exercise. The present efforts to address CI through the enactment of new regulation and institutions simultaneously de-politicize important decisions. This is problematic.

Modern society is not merely a complicated environment, but a complex environment, which interacts in unforeseeable ways. Simply speaking it becomes impossible to foresee all outcomes. We might have to act as if we understand this – but we should simultaneously maintain the insight that we cannot. The most feasible way to do so, I believe, is to keep the designation of CI in a political realm. Ironically, recent attempts to attach political value and priority to the designation of CI, simultaneously de-politicizes the process.

I have strived to document how this *depoliticization* takes place in the Swiss context, but I could have chosen any highly developed country in the world. Politicians have come under the impression that legal regulation can effectively address and designate CIP, while apparently overlooking the change of *modus* this invokes for the political prioritizations inherent.

Thus, looking forward we need to develop modes of governance in which these questions are re-politicized and simultaneously managed. Whether the solution is "intelligent risk management"[51], five focal points[52], or "popular connoisseurship of science and technology"[53] - the central academic and practical insight is the same: we need to form new forms of synergy between institutional knowledge and political decision, able to re-politicize the process: [54]

"The new politics of risk must retain the spirit of this critique while rehabilitating the authority of the expert. This will demand forms of leadership at the state, regulatory and corporate levels capable of developing a public language of risk that explicitly admits the possibility of failure, without this being understood as an excuse- or blame-avoiding strategy merely to manage expectations."[55]

Navigating a complex social system emphasizes the need for organizational flexibility and continuous political prioritization. To identify and secure critical infrastructure are not finite exercises. Rather, the criticality an important aspect of maintaining but a political dialogue, a procedural awareness, and the necessary organizational flexibility to effectively mitigate disaster risks.

In the end, whether or not it is critical to Switzerland that St. Gallen is provided with an unbroken delivery of internet-access or electricity is not an administrative, but political question.

---

51 *Ibid*., at 50f.

52 Jasanoff, 'Beyond Calculation. A Democratic Response to Risk', at 36. Jasonoff suggests five focal points: framing, vulnerability, distribution, deliberative learning.

53 Rayner, 'The Rise of Risk and the Decline of Politics', at 170.

54 While this might sound reasonable enough, the problem's roots might be deeper than I am leading the reader to believe. In the words of Rayner: "The solution to the problem of democratic participation is not as much dependent on the democratization of expertise, but on what Giddens (1999) has called "the democratisation of democracy"", cf. Rayner, 'Democracy in the Age of Assessment: Reflections on the Roles of Expertise and Democracy in Public-Sector Decision Making'. Thus, the problem might adhere to a larger, general need for a democratization of democracy.

55 Power, *The Risk Management of Everything. Rethinking the Polictics of Uncertainty* at 58.