Some Reflections on EU Governance of Critical Infrastructure Risks

*Marjolein B.A. van Asselt, Ellen Vos and Isabelle Wildhaber**

I. Introduction

Critical infrastructure (CI) sees to assets that are essential for the functioning of a society and economy[1], as they provide public services, enhance quality of life, sustain private profits and spur economic growth. Assets of CI differ considerably, ranging from hardware such as cables and wires, through to networks for the generation and supply of energy sources.[2] Critical infrastructures encompass many sectors of the economy, such as banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services. A breakdown of one or more of these critical systems has the potential of causing very serious problems.[3] The terrorist attacks of 9/11 made painfully clear that advanced economies are highly vulnerable in view of the increasingly efficient use of resources and highly networked production processes, which are increasingly dependent on information technologies and energy networks.[4]

The protection of CI systems therefore involves questions as to how societies can prevent a breakdown in CI and sees to crisis management of situations where the core values of a system or the functioning of life-sustaining systems which must be urgently dealt with under conditions of deep uncertainty.[5] The fundamental risk associated with CI is in a way already included in the notion 'critical': a breakdown, but also serious disturbances, of infrastructures qualified as critical are considered highly problematic. Such breakdowns and disturbances can, for example, be brought about by terrorism, criminal activities, natural and human-made disasters and other cascades of events and human actions. The governance of CI hence involves dealing with both security and safety issues, because both intentional behaviour aimed at derailing and accidental (courses of) event(s) have to be considered. Furthermore, in functioning societies, breakdowns of CI are by definition rare. So the issue of threats to CI actually boils down to the issue of how to identify and deal with high-impact – low-likelihood risks.

Dealing with 'high-impact - low-likelihood' risks to CI has, in particular after 9/11, been put high on the political agendas of many countries, including the EU and its Member States.[6] The Lisbon Treaty thus introduced prominently the solidarity clause in Article 222 TFEU which asks Member States to act together and assist each other in the event of a terrorist attack or a natural or man-made disaster.[7] Moreover, Lisbon equally introduced a formal supplementary competence for the EU in Article 196 TFEU to encourage cooperation between Member States in order to improve the effectiveness of systems for pre-

* Marjolein B.A. van Asselt is holder of the Risk Governance Chair at Maastricht University; Ellen Vos is Professor of European Union Law and co-director of the Magister Iuris Programme of the Faculty of Law at Maasstricht University; Isabelle Wildhaber is Professor of Private Law, Business and Labour Law at St. Gallen University.

1 See A. Van Aaken and I. Wildhaber, "State Liability and Critical Infrastructure: A Comparative and Functional Analysis", *EJRR* (2015), this issue.

2 A. Boin and A. McConnell, Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience, *Journal of Contingencies and Crisis Management Volume 15 Number 1 March 2007*, p. 50.

3 See Van Aaken and Wildhaber, see supra note 1.

4 R. Bossong, The European Programme for the protection of critical infrastructures – meta-governing a new security problem? European Security, 2014, p. 210-226.

5 U. Rosenthal, R.A. Boin and L.K. Comfort (2001), 'The Changing World of Crisis and Crisis Management', in U.Rosenthal, R.A. Boin and L.K. Comfort, (Eds.), Managing Crises: Threats, Dilemmas and Opportunities, Charles C. Thomas, Springfield, pp. 5–27.

6 See e.g. Communication From The Commission To The Council And The European Parliament on Critical Infrastructure Protection in the fight against terrorism, COM(2004) 702 final; Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final; 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, OJ 2008, L 345/75.

7 See T. Konstadinides, Civil Protection Cooperation in EU law: Is there Room for Solidarity to wriggle past? ELJ 2012, vol. 19, pp. 267-282.

venting and protecting against natural or man-made disasters. Already in 2001, the Commission had set up a Civil Protection Mechanism in order to coordinate the assistance that Member States give to another Member State having suffered a disaster.[8] Very recently, an Emergency Response Coordination Centre (ERCC) was set up within the European Commission's Humanitarian Aid and Civil Protection Directorate General (DG ECHO), to facilitate a coordinated and quicker response to disasters both inside and outside the EU.[9]

The protection of CI can be considered both as an act of risk governance[10] and of regional security governance.[11] This short reflection focuses on risk governance. Risk governance stresses the challenges associated with uncertain, complex and/or ambiguous risks, also referred to as systemic risks. Hereby, it is important to underline that CI risks are, unlike 'simple risks',[12] complex and inherently ambiguous and may be highly uncertain. They usually involve complex cause-effect relationships, accumulation of risks, highly contingent and unique interplays of a range of factors and situations not or rarely experienced before. So in statistical terms they are characterized as low-probability risks. The increasing interdependence and interference of risks to CI due to the economic, technological, and social processes of globalization add on to their impact and to their complexity.[13] Any attempt to regulate such risks therefore has to face enormous difficulties as they touch upon manifold geographical levels, economic sectors, and professional communities. The diverging public and private interests in critical infrastructure protection (CIP) and its transboundary nature are moreover particularly problematic for any government in establishing a coherent and effective approach to CIP. This equally explains the highly contested nature of the development of EU action in this area between 2005 and 2008.[14]

The question therefore arises how the EU should treat these systemic or uncertain risks to CI; a field that is relatively new for the EU. This query is dealt with in other contributions to this special issue and will not as such be answered here. This short essay seeks to contribute to this debate by looking at EU risk governance structures, in particular to trends to create EU agencies as a reaction to highly politicized policy domains such as food, and the focus on science.

II. The EU's Approach to Critical Infrastructure Protection

1. EU Initiatives

Whilst in the aftermath of 9/11 the Commission had set a striving package for EU involvement in CIP,[15] it appeared in the years after that the Commission had to cut down in its ambition. In its European Programme for Critical Infrastructure Protection[16] of 2006, the European Commission aimed to reduce the vulnerabilities of CI and to increase their resilience for two out of the 11 relevant sectors that the Commission had identified in 2005[17]: the energy and transport sectors. The Programme establishes a general EU framework for activities that respond to threats of terrorism, criminal activities, natural disasters and other causes of accidents, adopting an all-hazards cross-sectoral approach. Central in this is Council Directive 2008/114/EC on the identification and designation of European critical infrastructures (ECIs) and the assessment of the need to improve their protection, adopted on the basis of former Article 308 EC.[18] It determines a procedure for identifying and designating ECIs in these sectors and a common approach for assessing the need to improve

8 A. Boin, M. Busuioc, M. Groenleer, Building European Union capacity to manage transboundary crises: Network or lead-agency model? Regulation and Governance, 2014, pp. 418-436, at p. 421.

9 Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism, OJ 2013 L 347/924.

10 M.B.A. van Asselt and O. Renn (2011) Risk governance, *Journal of Risk Research*, 14:4, at 436.

11 Bossong, see supra note 4, at p. 211.

12 Such 'simple risks' can be dealt with by a simple cause and response model as the cause for the risk is clearly identified, the potential negative consequences are evident, the uncertainty is low, and there is hardly any ambiguity with regard to the interpretation of the risk. See M.B.A. van Asselt and O. Renn (2011) Risk governance, *Journal of Risk Research*, 14:4, at 436.

13 B. Auerswald, L. M. Branscomb, T. M. La Porte, E. Michel-Kerjan, *The Challenge of Protecting Critical Infrastructure*, October 2005, Center for Risk Management and Decision Processes – The Wharton School of the University of Pennsylvania, *Working Paper No. 05-11,* p. 3.

14 Bossong, see supra note 4, at p. 212.

15 Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final.

16 Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final; Bossong, see supra note 4.

17 Green paper, supra note 15.

18 Directive 2008/114/EC, OJ L 345 of 23.12.2008.

their protection. According to the Directive, Member States must go through a cooperative designation process of identifying potential ECIs, where necessary together with the Commission. This process involves interactions with other Member States, which could be significantly affected in case of the loss of service provided by an infrastructure. A Member State must approve of an infrastructure located on its territory to be formally designated as an ECI. The network of national contact points set up by this Directive sees to the exchange of information between the contact points that are appointed in each Member State and the Commission.

Whilst the adoption of this Directive was generally regarded positively, as it had been able to define a highly complex issue area for the first time since the 9/11 attacks, it was soon criticized for having become too narrow and not able to be extended to other sectors.[19] In addition to the political sensitivities, this was also due to the fact that the discussion on critical information infrastructures had become completely detached from CI. This had led the EU to set an agenda on cyber-security with the adoption of various legislative instruments and the creation of a European Network and Information Security Agency (ENISA).[20] Moreover, the creation of various networks such as the Critical Infrastructure Warning and Information Network (CIWIN), that the Commission had set up in 2004[21] to issue rapid alerts as well as the generation strategy of threat analyses from incident reports, appeared to be problematic. This was mainly due to serious concerns over the confidentiality of data on CI failures thus revealing the difficulties to sharing operational security information.[22] This led the Commission to finally withdraw its legislative proposal to formally strengthen the CIWIN.[23]

In 2013 the European Commission therefore revised its strategy and launched a new approach to the protection of CI and decided to focus only on four CI with a European dimension – EUROCONTROL, Galileo, the electricity transmission grid and the gas transmission network in order to optimise their protection and resilience.[24] This new approach determines a more realistic implementation of activities under the three main work streams – prevention, preparedness and response, aiming at building common tools and a common approach, taking better account of interdependencies.[25] At the same time, the Commission reinforced the CIWIN network, so that currently, whilst remaining an informal network, it offers virtual community allowing for exchange and discussion on CIP-related information, studies and/or good practices across all EU Member States and in all relevant sectors of economic activity.[26] Furthermore, in that same year, the Commission adopted a proposal for measures to ensure a high common level of network and information security across the Union.[27]

2. Supplementary Competence and Networks

The political sensitivities on CIP have led Member States to allow the EU to only undertake limited legal action over the years. The Lisbon Treaty has confirmed this with the conferral of a supplementary competence. The Commission views that Article 196 TFEU, albeit not allowing for harmonization, would not prevent the revision of the European Programme for CIP, establishing an obligatory framework for the EU as 'the participation in this framework would remain voluntary or allow the Member States a large degree of discretion in how they participate. For any measures under Article 196, the main role of the Commission is to monitor the general implementation of any legislation and to coordinate, supplement and support the Member States'.[28] In addition, the internal market competence of Article 114 TFEU allows

19 Bossong, see supra note 4, at p. 214.

20 Idem.

21 Commission of the European Communities, 2004. Communication from the commission to the council and the European parliament – Critical infrastructure protection in the fight against terrorism. COM(2004) 702 final.

22 Bossong, see supra note 4, at p. 217.

23 Withdrawal of obsolete commission proposals (2012/C 156/06). List of proposals withdrawn. OJ C 156/10.

24 COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD(2013) 318 final.

25 Boin, Busuioc, Groenleer, see supra note 8.

26 See https://europa.eu/sinapse/sinapse/index.cfm?fuseaction=login.redirect&redirect=cmtyrestricted.home&CMTY_ID=A0F55C70-0E9E-32D9-E5A7822B96D84471&request=1 (accessed on 1-2-2015).

27 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final.

28 COMMISSION STAFF WORKING DOCUMENT ON THE REVIEW OF THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (EPCIP), SWD(2012) 190 final.

for the adoption of sector specific security and protection measures.

Importantly, this has not prevented, or better perhaps, this has pushed the Commission to creating various informal networks and centres within DGs Home and ECHO among which the network of national points of contact on ECIP and the CIWIN mentioned above.[29] The Commission has furthermore developed an approach to build knowledge on how to better protect CI, thus trying to get a common approach on the underlying scientific methodologies and assessment, seemingly less political issues. To this end, it has funded various projects to provide expert knowledge and a deeper understanding of CI at all levels, feeding into policy priorities and providing the scientific basis for such work.[30] Examples hereof are studies on risk assessment and management methodologies. Importantly, the Commission has set up a network that it indicated as its 'flagship'[31] initiative, the European Reference Network for CIP (ERNCIP), that operates within the organisational framework of the Institute for the Protection and Security of the Citizen of the Commission's Joint Research Centre. Its mission is 'to foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities'.[32] In order to achieve this goal, ERNCIP develops a network of experts in a variety of CIP-related areas, explosives detection, cyber security and protection against earthquakes. Likewise it also contributes to standardisation activities.[33] This network links national laboratories and experimental facilities that work on CI vulnerabilities. It aims to influence or stimulate the harmonization of related technical standards.[34]

In sum, an important part of the Commission's strategy in protecting CI is to resort to science for the assessment of risks and the identification of risk management options. In that way, the European Commission attempts to provide a common basis for further action. With that effort institutional structures are created which facilitate and institutionalize this resort to science.

III. Governance of Critical Infrastructure Risks: Some Reflections

A key question in the risk governance literature is how to deal with complex, uncertain and/or ambiguous risks. Due to the nature of the threats to CI, the protection of breakdowns and disturbances involve dealing with high-impact – low-likelihood risks, which usually involve complex cause-effect chains, accumulation of risks, highly contingent and thus unique interplays of a range of factors and situations that are not or rarely experienced before. Any attempt to deal with CIP has to accept this nature of the risks, which complicates both the assessment and the management of CI threats. The question which can be raised is whether or not this is adequately addressed in the EU approach to CI risks.

In the risk governance literature, much scholarly attention has been focused on the actual and potential role of science and the interplay between science, policy and politics around systemic risks. Much of this research has examined governance practices around food risks and risks of agro-biotechnology in particular. Notwithstanding the differences in legal competences, the issues involved and the experience of the EU between such policy fields and the domain of CI, some of the insights gained seem relevant for reflection on the current EU approach to the governance of CI risks.

Risk governance research has revealed both the limits of science to resolve controversies in situations where the science is uncertain and the political stakes are high, and the problems of resorting to science in such situations.[35] Moreover, in such cases, especially in the field of GMOs, there is on the one hand an increasing resort to science and expert agencies such as EFSA as a neutral arbiter, whilst on the other, science seems to be increasingly instrumentalised and politicised in the political struggle involving high stakes. Hereby, it is important to understand that in such situations vicious circles of resort to science tend

29 See for a discussion, Bossong, see supra note 4, at p. 217.

30 Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks' (CIPS) during 2007-2012, see COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD(2013) 318 final.

31 Idem, at p. 7.

32 https://erncip-project.jrc.ec.europa.eu (accessed on 1-3-2015).

33 SWD(2013), 318 final, at p. 7.

34 Bossong, see supra note 4, at p. 218.

35 See e.g. the various contributions to M.B.A. van Asselt, E. Versluis and E. Vos (eds), *Balancing between Trade and Risk*, London: Routlegde, 2013.

to occur, whereby uncertainty is acknowledged, but current legal frameworks and political culture push regulatory authorities to ask scientists for more certainty; a situation that we have termed the 'uncertainty paradox'.[36] This kind of attitude has arguably led to increase the role of science and scientific agencies such as EFSA to the detriment of the precautionary principle.[37] In addition, it is evident that the precautionary principle does not see to politically sensitive issues where economic concerns need to be balanced against other concerns in relation to GMOs such as ethical concerns expressed by public opinion, or farmer traditions as for example Austria has tried to uphold. This necessitates the repoliticisation of risk governance on food.[38]

In the domain of CI risks, this resort to science and expert agencies is also visible. By means of resorting to science and in its effort to harmonize technical standards, the European Commission has thus attempted to provide for a science-based common basis for further action. We observe that both in reaction to the high politicisation of this area and the EU's limited competences, the European Commission has turned to the setting up of a scientific network ERNCIP, mentioned above, to provide for a framework for CIP-related experimental facilities and laboratories to share knowledge and expertise, and to harmonise test protocols throughout the EU, to better protect CI in the EU against all types of threats and hazards.[39] In this way, the Commission has thus attempted to compensate the lack of binding legal measures on CIP in line with its 'all hazard' approach, with the creation of informal networks and centres that vary from knowledge and expert gathering and building, such as ERNCIP to the coordination of actions such as the ERRC.

The complexity of dealing with risks to CIP is clear as it touches not only on safety risks but also on security governance, which equally explains the high political character of CIP. Although both safety and security deal with risks, the approaches are different. Academically, safety and security have developed into different research communities, with their own approaches, journals and networks. In the academic world, there is hardly any interplay between the field of safety and that of security. This complicates the assessment of the risks. It also complicates dealing with the risks, due to the diffusion of actions over various policy sectors, DGs and other actors and networks, which have quite different traditions and cultures. Attempting to provide a common basis for further action through technical harmonization in such a context is quite complicated, both content-wise and in terms of management. Furthermore, taken into account the EU's limited competences, the governance and regulation of CI risks is currently highly fragmented. Boin, Busuioc and Groenleer conclude, on the basis of their excellent study on the EU's capacity to manage transboundary crises, that the EU might well need to strengthen the existing networks. They observe in this context an already ongoing trend towards an institutionalistion of these networks, what they call an 'agencification' of networks.[40] As regards the critical information infrastructure protection, we do indeed observe this trend where the EU has set up an agency, ENISA.

In other fields of risk governance we can also discern a strengthening of existing informal institutional structures or even an introduction of novel institutional arrangements. Following various transboundary crises and disasters, such as the BSE crisis and other food scandals and the oil tanker Erika, for example, the EU reinforced its competences and created EU agencies. The EU has thus set up, for example, the European Food Safety Authority (EFSA), the European Maritime Safety Agency (EMSA) and the European Centre of Diseases Prevention and Control (ECDC).[41] These agencies all were established to improve the scientific underpinning of EU action. The choice for more centralised agencies rather than committees operating within the Commission or networks has often been the result from the EU's desire to (re)gain trust. Importantly, in response to problems of politicisation of science identified in the pre-BSE era, the EU reacted by focussing on objective science in the form of EFSA which has to give the 'best

36 M.B.A. Van Asselt & E.Vos (2006) 'The precautionary principle and the uncertainty paradox,' *Journal of Risk Research*, Vol. 9 (4), 313–336; Van Asselt M.B.A. & Vos E., (2008), Wrestling with uncertain risks: EU regulation of GMOs and the uncertainty paradox. Journal of Risk Research, 11(1-2), 281-300.

37 Van Asselt and Vos 2008, see supra note 36

38 Asselt, M.B.A. van, Everson, M. & Vos, E.I.L. (Eds.). (2014). Trade, Health and the Environment. The European Union put to the Test. London, New York: Routledge/Earthscan.

39 https://erncip-project.jrc.ec.europa.eu/download-area/finish/3-brochures/10-erncip-general.

40 Boin, Busuioc & Groenleer, see supra note 8, at p. 431.

41 See for a discussion M.. Groenleer, *The Autonomy of European Union Agencies: A Comparative Study of Institutional Development* (Delft: Eburon, 2009).

possible' scientific advice as a basis for EU food measures. In this manner, the creation of EFSA set a further step towards the Europeanization of the scientific basis of EU food safety regulation.[42] In the field of CIP, a comparable ambition can be observed, with ENISA and ERNCIP as the icons hereof. However, risk governance research in other fields has indicated that instead of serving as a neutral arbiter for the assessment of the risk and the advice on risk management options, either the agency's advices become politicised in the political and societal debates or the agency itself becomes distrusted by relevant actors. In other words, instead of being part of the solution, the experts become part of the problem. In our view, there is a role to play for experts in the identification and assessment of risks, to provide needed input to a system otherwise all too vulnerable to the demands of politics. But in which way and how expertise can be valuable in the governance of risk needs serious reflection.

These important insights should guide the thinking about the governance of CI risks. We suggest that risk assessment should be recognised as one of the elements of regulatory decisions in addition to the 'other legitimate factors' such as social, ethical and political concerns at the national and EU (and WTO) level. How risks are assessed is not a mere technical matter that can be left to institutions, but is a political question. These understandings with regard to the scientification and associated depoliticization of risk regulation in the field of food and GMOs are also relevant in shaping expectations to what science can and cannot offer to the governance of CI risks. Whereas risk governance can be informed by risks assessments and expert advice, the political responsibility cannot be concealed behind or delegated to scientific experts.

42 See Vos, E. 2000. EU food safety regulation in the aftermath of the BSE crisis. *Journal of Consumer Policy* 23: 227–55. See also Ansell, CK and Vogel, D (eds.) (2006) *What's the Beef? The Contested Governance of European Food Safety*, Cambridge, MA; Fisher, E. 2009, *Risk Regulation and Administrative Constitutionalism,* Hart Publishing.