

On the notion of “Partnership” in Critical Infrastructure Protection

Patricia Wiater*

This article is a critical reflection on the manifoldness of the notion of “partnership” in Critical Infrastructure Protection. It is argued that the partnership arrangement can be a promising political approach to CIP if the details of public-private cooperation – that is: the participants, the duration, the responsibilities and duties, as well as possible financial compensation – are formalized. Illusionary ideas of a “partner-like” relationship between the public and the private, such as those laid down in the German “National Strategy for Critical Infrastructure Protection”, are, however, doomed to fail. State authorities have to actively offer binding regulatory arrangements to private CI firms in order to establish which companies genuinely agree to cooperate – and which do not. Due to the state’s constitutional obligation to guarantee national security and protect the life and health of its citizens, introducing legal requirements is the only possible reaction to a company’s refusal to cooperate. In order to avoid overly intrusive market intervention, the state’s offer to private firms or their industry associations to conclude binding regulatory contracts on CIP matters may serve as a promising compromise between a laissez-faire approach and regulation.

I. Introduction

In the aftermath of the 9/11 terror attacks there was increased political awareness that civil infrastructure is in fact a potential terrorism target and its protection hence a matter of national security. Yet, this new awareness was confronted with a situation which could not be changed by political stakeholders – at least not easily: the privatization and deregulation of the 1980s and 90s led to a large number of critical infrastructures (CI) nowadays being owned or operated by private firms.

When they realized that the state is no longer able to guarantee national security in the field of Critical Infrastructure Protection (CIP) by its own means, policymakers started to refer to “partnerships” between the state and private stakeholders. As a result the term

“Public Private Partnership” (PPP) is often used in current CIP-policies,¹ albeit in a rather vague manner.

In the following paper it is argued that a distinction must be made between assessing the success of PPP in the context of CIP in the past and its possible deployment in the future. When “looking back” on existing CIP-policies, the dominant issue is that the state – responsible for protecting the life and health of its citizens by means of adequate CIP – found itself in a policy area that, due to privatization, is dominated by private firms. However, when looking at the possible future of CIP one may abandon this initial position to contemplate more promising applications of PPPs in CIP-policies. As an example for these different perspectives on PPP in CIP, this paper will refer to the German national CIP-strategy.

II. Dealing with Different Types of Partnerships in CIP

1. Looking back: The “Illusionary Partnership” at the Example of the German Approach to CIP

When German politicians started to consider CIP from the perspective of national security, mainly af-

* Dr. iur. Dr. phil. Patricia Wiater is Senior research fellow at Ludwig Maximilian University. The author thanks the participants of the St. Gallen symposium and an anonymous referee for helpful comments.

1 For an overview of different policy approaches see E. Brunner, M. Suter, “The International CIIP Handbook 2008/2009.—An Inventory of Protection Policies in 25 Countries and 6 International Organizations”, Center for Security Studies, Zurich, 2008. Available on the Internet at < <http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf>> (last accessed on 27 November 2014).

ter the terrorist attacks of 2001, *direct* political influence on the safety and security standards of these infrastructures based on government ownership was no longer possible. As in other Western nations, former state-owned enterprises had been privatised in Germany in the 1980s and 1990s. It is estimated that about 80 % of German critical infrastructures are nowadays in private ownership. Examples are companies in the energy, water, food, transport and telecommunications sectors.²

As the re-nationalisation of CI-companies was politically infeasible – primarily due to the costs associated with expropriation³ and in light of the fact that these recently privatized infrastructures significantly contribute to the competitiveness and prosperity of the economy –,⁴ alternative political instruments had to be created. The idea of entering into a partnership with CI-companies arose:⁵ In the German “National Strategy for Critical Infrastructure Protection (CIP Strategy)”⁶ of 2009, the notion of “partnership” is referred to in order to describe a more or less vague concept of collaboration between the state and those private corporations which own or operate CI.⁷

The approach is rather vague as it is not laid down in any kind of written or clearly formulated agreement between the state and private CI-enterprises. Nor is the duration of the collaboration defined. Instead, the German Federal Ministry of the Interior (BMI), which is responsible for internal security, issued different guidelines and recommendations on how to improve security measures and business continuity management of all possible enterprises con-

nected with CI.⁸ The concrete addressees of this political appeal remain unclear. The lack of any formal contract defining participants, responsibilities and risk allocation distinguishes the approach from the conventional concept of PPP.⁹

In contrast to the fuzziness of this foundation of the cooperation between the public and the private sector, the informal guidelines formulate the tasks of private CI-enterprises contributing to the security and safety of the complex network of CI in a very clear and detailed manner. In Germany, for example, CI-companies are called upon to improve their risk and crisis management by creating redundant capacities. Furthermore, they are asked to participate in a dialogue on safety and security incidents with state authorities in a spirit of partnership. For this purpose they have to create “single points of contact” in their specific industry sector.¹⁰ Again, the enterprises’ obligation to fulfil these concrete tasks is not laid down in any kind of contract or law.

This political approach provokes some critical remarks: It seems obvious that – as a result of privatization – guaranteeing national security in the field of CIP can no longer be the exclusive domain of the state. However, simply assuming the existence of a “shared responsibility” between the public and the private sector without any legal basis, as is done by the BMI,¹¹ is not a reasonable or responsible political strategy.

German authorities assume that fulfilling the complex catalogue of CIP tasks, mainly formulated by state authorities, is in the self-interest of the owners and operators of CI. In other words, the state presup-

2 For an overview of German companies owning or operating CI see Patricia Wiater, *Sicherheitspolitik zwischen Staat und Markt. Der Schutz kritischer Infrastrukturen* (Baden-Baden: Nomos, 2013), at pp. 40 *et seq.*

3 Under German constitutional law (Article 14 (3) Basic Law), the European Convention on Human Rights (Article 1 of Protocol No. 1) as well as under different guarantees of international law expropriation generally requires the payment of adequate damages.

4 Myriam Dunn Cavelti and Manuel Suter, “Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection”, 2 *International Journal of Critical Infrastructure Protection* (2009), pp. 179 *et seq.*, at p. 179.

5 This was mainly inspired by the policy approach adopted by the United States. For the development in Germany see Stefano Bruno and Myriam Dunn, “International CIIP Handbook 2002. An Inventory of Protection Policies in Eight Countries”, Center for Security Studies, Zurich, 2002, at pp. 41 *et seq.* Available on the Internet at <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=251> (last accessed on 27 November 2014).

6 Federal Ministry of the Interior, “National Strategy for Critical Infrastructure Protection (CIP Strategy)”, Berlin, 17th June 2009,

available on the Internet at http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf (last accessed on 27 November 2014).

7 CIP Strategy, *supra* note 6, at p. 12: One of the “guiding principles” regarding critical infrastructure protection is, in particular, a “trusting co-operation between the state and business and industry at all levels”.

8 Wiater, *Sicherheitspolitik zwischen Staat und Markt*, *supra* note 2, at p. 162 *et seq.* with further references.

9 By “conventional” PPPs it is referred to partnerships dealing with public procurement in areas such as urban construction or prison industry. On the characteristics of PPPs of this type see Christopher Bovis, “Public-private partnerships in the 21st century”, 11 *ERA Forum* (2010), pp. 379 *et seq.*, at p. 384 *et seq.*

10 See the summary of CIP tasks of private operators in Germany at Wiater, *Sicherheitspolitik zwischen Staat und Markt*, *supra* note 2, at pp. 111 *et seq.* with further references.

11 CIP Strategy, *supra* note 6, at p. 8: „As a result of this tendency towards private ownership, also the responsibility for the security, reliability and availability of such infrastructure increasingly passes to the private sector or, at least, becomes a shared responsibility.”

poses that the private interest in ensuring business continuity and the state's interest in realizing national security policies are largely conform. This supposed conformance is not only the reason for refraining from written arrangements between the public and the private sector, it is also the reason why the state refrains from employing other political instruments – such as regulation or the funding of CIP tasks.

There are fundamental aspects that caution against this assumed complementarity of interests:¹² First of all, it is misleading if state authorities speak about their “shared responsibility” with private stakeholders, as this language might distract from the core responsibility of the state to guarantee national security. This responsibility is, in the German case, founded in the constitutional obligation of the state to protect the life and health of its citizens.¹³ Even if state authorities and the legislator have broad political discretion in how to organize and realize their responsibility, the role of government in providing the public good of security in CIP must be clear.¹⁴ “Corporate social responsibilities” of private CI firms might be a legitimate subject of debate.¹⁵ However, in formulating policies, the state cannot blindly trust in private actors to fulfil CIP obligations voluntarily – as long as these obligations are not legally binding, or as long as there is no adequate compensation for the costs connected with performing these tasks.¹⁶

In addition, the complex and costly nature of CIP tasks entrusted to private companies suggests that not all of these tasks reflect the self-interest of the

owners and operators of critical infrastructure. It is a main characteristic of CIP measures that they contribute to the safety and security of the complex network of critical infrastructure as a whole. If the concrete safety measure does not serve the business continuity of the company in question, but contributes to increasing security of the CI network structure, in terms of public goods theory realizing this measure means creating so-called “additional social costs” for the company concerned.¹⁷ As long as state policies trust in the private sector to pay for these social costs voluntarily, the “illusion of a risk transfer to the private sector”¹⁸ is perpetuated.

Furthermore, the question of equality in cooperation calls for caution in assessing the quality of “loose partnerships” of this type: Private CI companies are asked to communicate sensitive information about security incidents to their public partners. It is questionable how they could really step into a dialogue in a spirit of partnership – as suggested by the BMI – if the public cooperation partner is often the very supervisory authority responsible for taking action against security deficiencies. As to the role of public authorities in this dialogue: Improving CIP in general depends on improving the protective measures of every single company operating critical infrastructure, be it a large-scale company or a small-scale company. Thus, realizing CIP policies effectively depends on a range of technical and organizational factors which vary tremendously from CI sector to CI sector and from business to business.

12 See also Dunn Cavelty and Manuel Suter, “Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection”, *supra* note 4, p. 181; Jan Joel Andersson and Andreas Malm, “Public-Private Partnerships and the Challenge of Critical Infrastructure Protection”, in Myriam Dunn and Victor Mauer (eds.), *International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects* (Zurich: Center for Security Studies, 2006), pp. 139 *et seq.*, at pp. 141 *et seq.* Available on the Internet at < <http://e-collection.library.ethz.ch/eserv/eth:31123/eth-31123-04.pdf>> (last accessed on 27 November 2014).

13 The German Constitutional Court found that the state's obligation to protect the security of its population is a constitutional value of core relevance as it justifies the very existence of the state; BVerfGE 49, 24 at 56 *et seq.* (“Die Sicherheit des Staates als verfaßter Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit seiner Bevölkerung sind Verfassungswerte, die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet.” See also Dietrich Murswiek, “State Duties to Protect”, unpublished draft paper submitted for the International Symposium “Risk, Responsibility and Liability in the Protection of Critical Infrastructures” on May 23 and 24, 2014 in St. Gallen; Friedrich Schoch, “Die Staatliche Einbeziehung Privater in die Wahrnehmung von Staatsaufgaben”, XVI JURIDICA INTERNATIONAL (2009), at pp. 17 *et seq.*; available at the Inter-

net at < http://www.juridicainternational.eu/public/pdf/ji_2009_1_14.pdf> (last accessed on 2 April 2015); Matthias Sonntag, *IT-Sicherheit kritischer Infrastrukturen. Von der Staatsaufgabe zur rechtlichen Ausgestaltung* (München: Beck, 2005), at pp. 82 *et seq.*

14 In this regard, the German Constitutional Court found that no concrete form of action of the state can be deduced from its obligation to protect the life and health of its citizens; nevertheless, the Court requires the state's protection measures to be *effective*; BVerfGE 46, 160 at 164 *et seq.* („Wie die staatlichen Organe ihre Verpflichtung zu einem effektiven Schutz des Lebens erfüllen, ist von ihnen grundsätzlich in eigener Verantwortung zu entscheiden.“). Guaranteeing the effectiveness of political measures requires assessing and controlling their practical effects – a duty which is neglected in the current German CIP approach.

15 Gail Ridley, “National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience”, 103 *Journal of Business Ethics* (2011), pp. 111 *et seq.*

16 Wiater, *Sicherheitspolitik zwischen Staat und Markt*, *supra* note 2, at pp. 224 *et seq.*

17 Wiater, *Sicherheitspolitik zwischen Staat und Markt*, *supra* note 2, at pp. 247 *et seq.*

18 Christopher Bovis, “Risk in Public-Private Partnerships and Critical Infrastructure”, *EJRR*, this issue.

This initial condition not only complicates the design of a “one size fits all” policy approach to CIP; it also reveals the inability of the state to properly guarantee or control the implementation of CIP measures by the private sector. If “efficient risk allocation dictates that risk must rest with the most able party to retain”,¹⁹ the state is obviously unable to bear the risk of either producing CIP or controlling the private production by its own means. In this regard, the so-called “capture theory” cautions against the state becoming mired in non-transparent lobbying if public authorities depend on information and knowledge provided by private players.²⁰ Research findings on PPP point to the fact that it is a fundamental challenge to structure PPP contracts in detail.²¹ The challenge of realizing national security collaboratively without explicitly formulating responsibilities and risks is even greater. If, in addition, it remains unclear which enterprises of those owning or operating CI are willing and able to cooperate with state authorities, this challenge seems to be too big to be met. The state, trying to offer a partnership in CIP retroactively and *ad incertas personas*, neglects its constitutional obligation of guaranteeing national security.

2. The Turning Point: Regulation as the Alternative to PPP?

Interestingly, the “illusionary nature” of this political approach to partnerships in CIP seems to have caught the attention of German politicians: In 2012²² the

German Federal Ministry of the Interior issued a draft law on IT security of CI.²³ Although a multitude of (public and private) laws define differing safety and security standards for different CI-sectors,²⁴ this draft law on IT security is the first attempt to address CI-operators directly and comprehensively. If the law is passed, a high number of the tasks which were formerly formulated in informal guidelines and recommendations would then be prescribed by law: Based on a legal definition of CI, their operators are obliged to establish technical and organizational minimum standards of IT security, to specify emergency plans, to report significant IT security incidents to the Federal Office for Information Security (BSI) and to guarantee availability with public authorities in case of emergency.²⁵ These obligations are mainly of a procedural nature.

In justifying its political turnaround by introducing regulation to protect CI, the ministry argues that – in the specific field of cyber security – the collaboration between the public and the private needs to be improved in order to ensure the necessary minimum standards of safety and security of IT-CI.²⁶ Obviously, also from the viewpoint of state authorities, the relationship between the public and the private “in a spirit of partnership” has failed. In order to overcome deficiencies in the loose partnership concept, there are good reasons for the state to define CIP tasks of private companies in regulation: The law provides a clear separation and distribution of responsibilities between private and public stakeholders and establishes the state’s right to directly control private ac-

19 Bovis, “Collaboration in PPPs in Critical Infrastructure”, *supra* note 18.

20 Ernesto Dal Bó, “Regulatory Capture: A Review”, 22 *Oxford Review of Economic Policy* (2006), pp. 203 *et seq.*

21 Bovis, “Public-private partnerships in the 21st century”, *supra* note 9, pp. 391 *et seq.*; Bovis, “Risk in Public-Private Partnerships and Critical Infrastructure”, *supra* note 18.

22 The law was not adopted during the last legislative period under the government of the Christian Democratic Union/Christian Social Union (CDU/CSU) and the liberal Free Democratic Party (FDP), ending in September 2013. The bill was taken up again after the election by the Federal Ministry of the Interior, still administered by a member of CDU/CSU, under the grand coalition between CDU/CSU and the Social Democratic Party (SPD). The Federal Ministry of the Interior forwarded its draft bill to the other federal ministries involved for further consultation on 19 August 2014. In the meantime, after completion of this article, the draft bill was adopted by the Federal Government (on 17 December 2014, see “Bundestags-Drucksache 18/4096”) and, subsequently, with a few changes passed by the German Bundestag (on 12 June 2014, see “Bundestags-Drucksache 18/5121”). As changes do not concern the aspects referred to in the following, the reference to the original draft bill was not altered.

23 Federal Ministry of the Interior, “Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)”, 18 August 2014, available on the Internet at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?jsessionid=1561991D3361D692471345121CF795F8.2_cid364?__blob=publicationFile (last accessed on 27 November 2014).

24 For a comprehensive overview of German legal standards distinguishing among the different CI sectors see Bernd Holznagel and Christian Koenig, “Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen”, Federal Office for Information Security (BSI) (ed.), last updated on 5th May 2005, available on the Internet at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Regelungsumfang_ITSich_KRITIS.pdf?__blob=publicationFile (last accessed on 27 November 2014).

25 See the English Information sheet on the IT Security Act of 19 August 2014, available on the Internet at http://www.bmi.bund.de/SharedDocs/Downloads/EN/News/information-sheet-it-security-bill.pdf?__blob=publicationFile (last accessed on 27 November 2014).

26 Draft law on IT security, *supra* note 23 at p. 2.

tivities and to enforce CIP standards by sanctioning failure to comply. At the same time, “command and control” regulation of this type is, besides government ownership, the most interventionist and centralist policy instrument for the state to achieve adequate levels of protection for critical infrastructure.²⁷ As current state policies are predominantly guided by a *governance* model (to be differentiated from a *government* model), incorporating the self-regulating capacities of the private sector to the largest possible extent, the search for alternatives seems worthwhile.

3. Looking into the Future: Chances for “genuine Partnerships” in CIP

Is this German shift towards regulation paradigmatic for the overall failure of the partnership model in CIP?²⁸ In other words: Is there a middle way between the objectionable concept of loose and illusionary partnerships and formal regulation?

One possibility of maintaining the concept of collaboration without reducing it to direct partnerships is the “expanded governance model for CIP”.²⁹ In this

approach, state authorities have the task to coordinate and stimulate self-regulating networks of private companies running or owning CI. After defining and communicating policy goals and priorities, the state exercises *indirect* control by funding or providing incentives for private networks to achieve these tasks. Some of the disadvantages of the German “illusionary partnership model” – as discussed above – could be minimized by this approach: Instead of over-extended state authorities, private companies control each other thereby enforcing new standards of CI safety and security.³⁰ Instead of grounding the partnership between the public and the private on the illusion of mutual trust, the role of public authorities is reduced to promoting existing or supporting the emergence of new self-regulating private networks.

Nevertheless, one major challenge cannot be met by the network model either: The outsourcing of essential functions in the field of CIP to self-regulating networks entails an unclear allocation of responsibilities as long as these networks are not subject to government monitoring.³¹ This deficit points to the, in my view, most important aspect in discussing different policy instruments for CIP: the fact that the state cannot acquit itself of the constitutional duty to ensure inner security of the nation – which inevitably calls for some kind of direct state control.³² At the same time, the dependency of state authorities on the knowledge and expertise of private stakeholders cannot be overlooked.

A possible arrangement for reconciling these two constraints is to introduce “flexible elements” in legal standards, as proposed in the German draft law on IT security: The operators of CI and their branch associations will be called upon to propose to the Federal Office for Information Security (BSI) sector-specific criteria for necessary minimum standards on IT security. If this proposal is accepted by the responsible public authorities, private stakeholders themselves define the suitable precautionary measures for their IT security.³³ In case of noncompliance, the duty to fulfil these measures can be enforced by the state.³⁴ This is an example for “regulated self-regulation” with particular emphasis on the regulatory aspect.

An alternative way more focused on reinforcing the concept of partnership between the private and the public, by putting particular emphasis on the cooperative aspect, is the concept of “regulation by con-

27 Dan Assaf, “Conceptualising the use of public-private partnerships as a regulatory arrangement in critical information infrastructure protection”, in Anne Peters et al. (ed.), *Non-State Actors as Standard-Setters* (Cambridge: Cambridge University Press, 2009), pp. 61 *et seq.*, at pp. 64 *et seq.*

28 See on the “(minor) deviation from non-intervention” in the U.S. in the field of the chemical and the energy sector Assaf, “Conceptualising the use of public-private partnerships as a regulatory arrangement in critical information infrastructure protection”, *supra* note 27 at pp. 71 *et seq.*

29 The governance model described is elaborated and discussed by Dunn Cavely and Suter, “Public-Private Partnerships are no silver bullet”, *supra* note 4, at pp. 182 *et seq.*

30 The network model links the effectiveness of control to the phenomena of “group pressure” and expertise; Dunn Cavely and Suter, “Public-Private Partnerships are no silver bullet”, *supra* note 4, at p. 183: “The partners within a network know each other well and are thus able to assess whether the degree of cooperation is sufficient. (...) While companies may find it easy to gloss over their weaknesses and vulnerabilities towards the government, it may be more difficult to embellish their performance in communication with other experts.”

31 Dunn Cavely and Suter, “Public-Private Partnerships are no silver bullet”, *supra* note 4, at p. 184.

32 Again, this obligation to exercise direct state control results from the constitutional duty to guarantee *effective* protection; see *supra* note 14. Effective protection requires at least that the state has knowledge about the risk situation and the level of preparedness of private CI companies to handle these risks.

33 In order to avoid standards set too low by private CI companies, public authorities have to conduct a plausibility check of the precautionary measures proposed. This can e.g. be achieved by using comparative data from other countries.

34 Draft law on IT security, *supra* note 23 at p. 13.

tract”.³⁵ This political instrument takes up an element of the “classical” PPP concept: the contractual formalization of the partnership, defining participants, responsibilities and risk allocation. Contractual regulation has been successfully applied in the sphere of environmental law.³⁶ Here, one can distinguish between contractual arrangements between governments or public authorities and private stakeholders which *replace, realize or supplement* legal norms.³⁷ Some countries have, for instance, refrained from implementing an energy tax, electing to conclude negotiated agreements instead. In return, private firms have committed to reducing their CO₂ emissions.³⁸ In agreements supplementing pre-existing regulation, companies have agreed to reduce pollution beyond what is required by law and have conversely benefitted from facilitated permit procedures implemented by public authorities.³⁹

Comparable to the long-term objective of CIP, agreements on environmental matters pursue a desirable social result. Thus, the same policy approach could work in the realm of CIP: Instead of introducing a legal “one size fits all” standard for CIP, public authorities could conclude bi- or multilateral contracts with private CI companies or their industry associations. Contractual regulation reacts to the concrete conditions of the private stakeholders concerned. Thereby, it avoids over-regulation and an overly intrusive state intervention in the market, as well as under-regulation which permits safety and security standards in CI companies which do not comply with current CIP policies.

As mentioned above, the network character of today’s economic relations presents a major challenge for CIP. Large-scale companies of different sectors are interdependent and depend, at the same time, on the proper working of smaller and medium-sized companies (SMEs) – and *vice versa*. The multiplicity of stakeholders would be an indisputable challenge to the contractual CIP approach if one public authority (in the case of IT security: the Federal Office for Information Security) had to bargain thousands of contracts with different partners and different contents. However, this challenge does not have to be seen as an obstacle but can be perceived as the opportunity to align the political approach to CIP with the realities of the market: The regulatory approach to CIP is inevitably “abstract-general” as a law on CIP applies to a multitude of cases (*abstract*) and a multitude of different addressees (*general*). The addressees are, in

the language of the draft law on IT security, the “operators of critical infrastructures,” i.e. the operators of facilities of different sectors, e.g. energy, IT and telecommunication, transport, water supply, health, which are “*of major importance to the community*”.⁴⁰ An indeterminate formulation of this kind creates legal uncertainty⁴¹ if every single company is obliged to self-evaluate its importance to the functioning of the CI network.⁴² While this importance seems obvious for big players such as the German Railway system (Deutsche Bahn), this is not the case for SMEs.

Here, regulation by contract offers the chance to strike a fair balance: In *bilateral* agreements between the public authority and a large-scale company which is of crucial importance to the community’s security (e.g. energy supplier, atomic plants, German Railways), the state can command particularly high standards of security measures, for example with regard to reporting duties, creating redundant capacities or guaranteeing 24/7 availability for public authorities in case of emergency. If the same CIP measures were applied to SMEs, disproportionate expenditure of personnel and finance would be needed to implement them.⁴³

As bilateral contractual relationships with the huge number of SMEs engaged in CI would create

35 See the comparison of Government-Private Contracts and Regulatory Contracts by Jody Freeman, “The Contracting State”, 28 *Florida State University Law Review* (2000), pp. 155 et sqq.

36 For an overview see Jody Freeman, “The Contracting State”, *supra* note 34, at. p. 196 et sqq.

37 Alexander Proeß and Ursula Blanke-Kießling, „Der Verwaltungsvertrag als Handlungsform der Naturschutzverwaltung“, *Neue Zeitschrift für Verwaltungsrecht* (2010), pp. 985 et sqq., at p. 986.

38 Magali Delmas and Ann Terlaak, “Regulatory Commitment to Negotiated Agreements: Evidence from the United States, Germany, The Netherlands, and France”, 4 *Journal of Comparative Policy Analysis: Research and Practice* (2002), pp. 5 et sqq. at p. 6 with further references.

39 *Ibidem*.

40 See the legal definition of CI in the German draft law on IT security, *supra* note 23 at p. 9.

41 On the fuzziness of the notion “critical” in CIP see Fred Cohen, “What makes critical infrastructures Critical?”, 3 *International Journal of Critical Infrastructure Protection* (2010), pp. 53 et sqq.

42 See in this regard the commentary of the Federal Association of SMEs of the IT sector (Bundesverband IT-Mittelstand e.V.) from 2 September 2014, available on the Internet at < http://www.bitmi.de/custom/download/bitmi_140903_stellungnahme_it_sicherheitsgesetz_1409727767.pdf> (last accessed on 27 November 2014).

43 The Federal Association of SMEs of the IT sector (*supra*, note 41) criticizes, in this respect the discriminatory potential of the German draft law on IT security.

unnecessary red tape and bureaucracy, concluding *multilateral* or *collective* agreements would be more suitable. The different industry associations – those the draft law on IT security calls upon to deliver proposals for sector-specific minimum standards of CIP – could be mandated by their members to authoritatively bargain contractual CIP conditions. Model agreements could serve as guidelines for the negotiations. The approach of concluding collective agreements was adopted in the German agreement on Global Warming Prevention in 1995, in which the major industry associations agreed on reducing CO₂ emissions by the end of 2005.⁴⁴

The advantage this approach offers to the state is obvious: The “command and control” element, inherent in traditional regulation, is replaced by “command and covenant”.⁴⁵ The state avoids restrictive market intervention by adjusting the required CIP standards to the particularities of the company or sector concerned and, at the same time, respects its core responsibility to ensure national security by means of direct control. One important component of this core responsibility of the state is the financial responsibility for measures relevant for protecting nation-

al security: The draft law on IT security was and is subject to the resistance of industry. Considering that the law imposes “additional social costs” on CI enterprises, caused by CIP measures which do not comprehensively serve the business continuity of the company in question, but contribute to increasing security of the CI *network* structure, this resistance is understandable. If, in individual cases, these “additional social costs” impose a disproportionate burden on the company in question, the contractual approach allows the companies to bargain for state compensation.⁴⁶ This aspect can be of particular relevance for SMEs belonging to the core CI-community.⁴⁷

While the above-mentioned German environmental agreement was non-binding, the state’s constitutional duty to protect the life and health of its citizens by means of adequate CIP requires the conclusion of legally binding contracts, enforceable through courts. This condition might, in some countries, necessitate the approval of Parliament.⁴⁸ In Germany, the constitutional principle of “requirement of formal law” would in all likelihood require the specific enactment of a parliamentary statute authorizing public authorities to conclude legally binding contracts on CIP measures. This involvement of elected representatives can be of crucial importance for guaranteeing transparency and avoiding the lobbying referred to above.

What are the incentives of private CI companies to accept the state’s offer of contractual regulation? Here a distinction is needed: While the state can require accepting the contractual CIP approach as a condition for an impending privatisation of the small number of CI enterprises which are still state-owned (e.g. water supply), the same does not apply to privatized companies. For profit-oriented privatized CI companies, avoiding costly and disproportionate market intervention triggered by over-regulation is of fundamental importance. A core incentive in this regard is the avoidance of formal regulation. The state actively creates this incentive by threatening in-depth regulatory intervention if the private sector takes no action.⁴⁹ “Legislators can threaten to enact adverse legislation unless potentially affected actors alter their behaviour to accommodate the legislators’ demands.”⁵⁰ For the companies participating in the environmental agreement of 1995, the expected benefit of concluding the agreement was that it would ensure that the waste heat ordinance would not come

44 Bundesverband der Deutschen Industrie e.V., *Updated and Extended Declaration by German Industry and Trade on Global Warming Prevention* (Cologne: BDI 1996); Delmas and Terlaak, “Regulatory Commitment to Negotiated Agreements: Evidence from the United States, Germany, The Netherlands, and France”, *supra* note 37, at p. 7 *et seq.*, p. 14 *et seq.* On the evolution of the agreement and the criticism on it see EEA (European Environment Agency), *Environmental Agreements. Case Study 3: Germany* from 21 July 1999, available on the Internet at < <http://www.eea.europa.eu/publications/92-9167-052-9-sum/page006.html>> (last accessed on 27 November 2014).

45 Freeman, “*The Contracting State*”, *supra* note 34, at p. 196.

46 This is the case in some of the environmental agreements discussed above.

47 Imagine a small supplier company producing bolts which are an essential element for the working of the train system. The breakdown of this small company might cause tremendous cascade effects on the network of CI which might necessitate higher security standards than those of other companies of comparable size.

48 Legally-binding environmental agreements are concluded in the Netherlands, where these agreements are linked to a permit system and have the status of contracts of civil law; see Delmas and Terlaak, “Regulatory Commitment to Negotiated Agreements: Evidence from the United States, Germany, The Netherlands, and France”, *supra* note 37, at p. 8.

49 Assaf, “Conceptualising the use of public-private partnerships as a regulatory arrangement in critical information infrastructure protection”, *supra* note 27, at p. 68.

50 Adrienne Héritier and Dirk Lehmkuhl, “The Shadow of Hierarchy and New Modes of Governance”, 28 *Journal of Public Policy* (2008), pp. 1 *et seq.*, at p. 2.

into force and that the carbon/energy tax would not be levied.⁵¹ This is what can be called the “shadow of hierarchy”.⁵² Even if the contractual arrangements were of legally binding nature, the threat of formal regulation remains. A regulatory “one size fits all” approach (abstract, vague standards, etc.) necessarily ignores the different needs of private addressees; this fact alone may constitute a major disadvantage of regulation for CI companies.

III. Concluding Remarks

In this article, the manifoldness of the notion of “partnership” in Critical Infrastructure Protection has been critically reflected. It has been argued that the partnership arrangement can be a promising political approach to CIP if the details of public-private co-operation – that is: the participants, the duration, the responsibilities and duties, as well as possible financial compensation – are formalized. It is up to the state to refrain from conveying unrealistic illusions of a partnership with the private CI sector and instead take a fresh look at the instrument of partnership agreements. State authorities have to actively offer binding regulatory arrangements to private CI firms to establish which companies genuinely agree to cooperate – and which do not. Due to the state’s constitutional obligation to guarantee national security and to protect the life and health of its citizens, introducing legal requirements is the only possible reaction to a company’s refusal to cooperate. In order to avoid overly intrusive market intervention, the state’s offer to private firms or their industry associations to conclude binding regulatory contracts on CIP matters may serve as a promising compromise between a laissez-faire approach and regulation.

However, the “regulation by contract” model is not a miracle cure either. Problems might arise if some of the “big players” of an important CI sector agree to contract with state authorities, and others, operating CI of core relevance for national security, do not. In this case, total state control by means of regulation which is binding on all operators of CI must prevail. Moreover, contracts are imperfect policy instruments as they cannot react to anticipated issues that extend beyond the scope of the specific contract.⁵³ New kinds of threats to national security can require new security measures which might not be covered by the contractual duties of CI operators. At this instant, the crucial question of supplementary commitments of private companies for the desirable social objective “national security” revives. This challenge presupposes a level of flexibility which cannot be met by any type of binding arrangement – be it a legal or a contractual requirement.

However, the contractual formalization of CIP partnerships offers chances which should not be underestimated: If public and private stakeholders enter into result-oriented negotiations, dialoguing on security matters occurs on a realistic level. This helps the state to refrain from formulating policy approaches based on wishful thinking about the functioning of the market and to fulfil, thereby, its constitutional obligation to protect its citizens.

51 EEA, *Environmental Agreements. Case Study 3: Germany*, *supra* note 43.

52 Héritier and Lehmkuhl, “The Shadow of Hierarchy and New Modes of Governance”, *supra* note 50.

53 Austen D. Givens and Nathan E. Busch, “Realizing the promise of public-private partnerships in U.S. critical infrastructure protection”, 6 *International Journal of Critical Infrastructure Protection* (2013), pp. 39 *et seq.*, at p. 42. The authors argue for “collaborative leadership” instead, see p. 46 *et seq.*