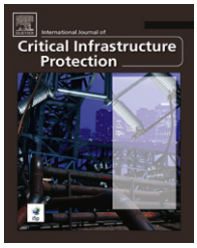
available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip



Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection

*Myriam Dunn Cavelty, Manuel Suter**

Center for Security Studies, ETH Zurich, 8092 Zurich, Switzerland

ARTICLE INFO

Article history:
Received 13 March 2009
Received in revised form
28 July 2009
Accepted 27 August 2009

Keywords:
Critical infrastructure protection
Public–Private Partnerships
Governance theory
Meta-governance

ABSTRACT

For more than a decade, efforts have been underway to establish *Public–Private Partnerships* (PPP) for Critical Infrastructure Protection (CIP). Due to issues arising in connection with their implementation, there has been increasing criticism in recent years questioning the usefulness of such PPP. However, cooperation between the state and the private corporate sector in CIP is not only useful, but inevitable. This paper will therefore sketch a new and above all broader approach to public–private cooperation to help solve some of the problems that have become apparent. Based on the network approach developed by governance theory, it is argued that CIP policy should increasingly rest on self-regulating and self-organizing networks. Thus, the government's role would no longer consist in directing and monitoring, but of coordinating the networks and identifying instruments that can help motivate networks to meet the task of CIP.

1. Introduction

Critical infrastructure protection (CIP) is currently seen as an essential part of national security in numerous countries around the world and a broad range of political and administrative initiatives and efforts is underway in the US, in Europe, and in other parts of the world in an attempt to better secure critical infrastructures [1,2].[1] One of the key challenges for such protection efforts arises from the privatization and deregulation of many parts of the public sector since the 1980s and the globalization processes of the 1990s, which have put a large part of the critical infrastructure in the hands of private enterprize. This creates a situation in which market forces alone are not sufficient to provide security in most of the CI 'sectors' [3]. At the same time, the state is incapable of providing the public good of security on its own, since an overly intrusive market intervention is not a valid option either; the same infrastructures that the state aims to protect due to national security considerations are also the foundation of the competitiveness and prosperity of a nation. Therefore, any policy for CIP must absorb the negative outcomes of liberalization, privatization, and globalization, without canceling out the positive effects.

Public–Private Partnerships (PPP), a form of cooperation between the state and the private sector, are widely seen as a panacea for this problem in the policy community—and cooperation programs that follow the PPP idea are part of all existing initiatives in the field of CIP today [1]. A large number

* *Corresponding address:* Center for Security Studies (CSS), ETH Zurich WEC E 23, Weinbergstrasse 11, CH-8092 Zurich, Switzerland. Tel.: +41 0 44 632 63 49; fax: +41 0 44 632 13 72.
E-mail address: suter@sipo.gess.ethz.ch (M. Suter).

[1] Critical infrastructures (CI) are systems or assets so vital to a country that any extended incapacity or destruction of such systems would have a debilitating impact on security, the economy, national public health or safety, or any combination of the above. The most frequently listed examples encompass the sectors of banking and finance, government services, telecommunication and information and communication technologies, emergency and rescue services, energy and electricity, health services, transportation, logistics and distribution, and water supply [1, p. 527ff.].

1874-5482/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2009.08.006

of them is geared towards facilitating information exchange. While some of these arrangements are successful, others have scarcely generated more than joint statements of intent of the actors involved. In recent years, therefore, increasing criticism has been heard condemning the lack of efficiency in existing arrangements or even questioning the validity of the entire cooperation concept [4,5]. However, if we take into account the origins of the PPP-idea, it comes as no big surprise that the initial high expectations have been lowered somewhat: The PPP concept was originally conceived in a completely different context, namely in the field of administrative reform and the concept of New Public Management in the 1980s. The aim of PPPs in this context was the debureaucratization of public services and the promotion of privatization. In his article "Conceptualizing the Use of Public–Private Partnerships as a Regulatory Arrangement in Critical Information Infrastructure Protection", Dan Assaf highlights that the PPP concept was adopted rather uncritically by the US for its CIP policy at the end of the 1990s [6]. The PPPs in CIP were in line with the neoliberal conceptualization of PPPs as an instrument of outsourcing of public services from the state to private companies (in this case the owners and operators of CIs). Assaf criticizes this approach and discusses the normative problems of accountability, transparency and legitimacy of a "de facto privatization" in the field of CIP which is highly relevant for national security. He concludes that a greater role of government is needed to ensure the provision of the public good of security in CIP [6].

But for all the legitimate critique on the concept PPPs and its use in the field of CIP, we should not risk throwing the baby out with the bathwater. Clearly, cooperation between the state and private enterprize on CIP is not only sensible, but simply essential. The question is not whether Public–Private collaboration is necessary, but how it should be organized. Therefore, this article examines the following (timely) questions: *What is the benefit of the PPP concept and what are the limitations as far as CIP is concerned? What other approaches are conceivably (more) suitable? And what exactly is the role of the government with regard to the collaboration with the private sector?*

We will first trace the provenance of the term "PPP" and how it is embedded in a larger (economic policy) context. We then analyze the specific characteristics of PPP in the field of CIP and elicit the practical problems arising in connection with the concept. It is important to note that this article does not question the notion of cooperation in general, but only the way in which it has been organized and conceptualized so far. Specifically, we point out that direct partnerships between public and private actors do not constitute the only possible form of cooperation, but rather are one of several instruments that can be deployed for governance in the field of CIP [7]. In order to develop a new and broader understanding of public–private cooperation, we will therefore take recourse to governance theory. We argue that CIP policy should be based as far as possible on self-regulating and self-organizing networks. The potential of self-regulating networks for the provision of security of infrastructures has already been highlighted by Amitai Aviram [8]. While he is focusing on the aspect of self-regulation within these networks, we will discuss the role of the government with regard to these self-regulating networks. We argue that the government's role no longer consists of close supervision and immediate control, but of coordinating networks and selecting instruments that can be used to motivate these networks for CIP tasks. In this, the article stays on a fairly theoretical level, though some examples are provided. We believe that the debate needs a theoretical infusion at this stage to move out of the deadlock—though more detailed studies should follow later.

2. Critical infrastructures and Public–Private Partnerships

The concept of PPP became popular during a wave of debureaucratization from the late 1970s onwards. Against the background of the global economic crisis, neoliberal critics diagnosed a crisis of the state and of the administration rather than of the market. They encouraged the public bureaucracy to hand over tasks to private actors, i.e., to privatize them, or at least to carry them out in partnership with private businesses, since this was allegedly the only way to enhance the efficiency of the public administration [9]. In concrete terms, the idea of PPP was first realized in urban construction in order to facilitate joint development and renewal of urban problem zones [10, p. 42f.]. Later, the term also came to include joint technology or ecological projects, as well as partnerships in the area of education, health services, and the prison industry [11]. In short, it has become an extremely heterogeneous concept and critics point out that it has now evolved into a catch-all label for all possible new or known forms of collaboration between the public administration and the private sector [12], [10, p. 47].

Beyond definitional and conceptual fuzziness, the fundamental character of PPP can be described as follows: Its goal is to exploit synergies in the joint innovative use of resources and in the application of management knowledge, with optimal attainment of the goals of all parties involved, where these goals could not be attained to the same extent without the other parties [13, p. 5f.]. The primary conditions for such cooperation are the complementarity of goals as well as pre-existing interdependence of the actors and their goals [10, p. 54]. Their collaboration is most often formalized contractually [14, p. 120]. Further conditions mentioned in the literature are mutual trust and precautions to limit the scope for abuse; the existence of clear, undisputed goals and strategy fixed in writing; a clear distribution of risks; a clear separation of responsibility and authority as well as market- and success-oriented thinking [14, p. 124]. In view of these comprehensive conditions for the success of PPP, one may wonder to what extent the notion of PPP can be applied to CIP. In this chapter, we first investigate how PPP in the form of information-sharing arrangements have become the preferred solution in the field of CIP. Subsequently, we identify the limitations of this "solution".

2.1. *Information sharing as "the most immediate need"*

The foundation of the CIP concept is the study of the *President's Commission On Critical Infrastructure Protection* (PCCIP) [15]. It was established by President Bill Clinton in order

Please cite this article in press as: M. Dunn Cavelty, M. Suter, Public–Private Partnerships are no silver bullet . . . , International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.006

to produce a comprehensive report on the security of all infrastructure systems in the US. The PCCIP's task was to assess risks, develop defensive mechanisms, and to contribute to the identification of the required institutional and legislative reforms. The commission was staffed by representatives of *all* relevant government departments, i.e., no longer only the security-relevant bodies. Additionally, the owners of privately operated infrastructures were integrated [16]. By expanding the range of security policy actors to include other ministries and civilian corporations, the spectrum of possible CIP strategies was expanded beyond the traditional core area of security policy. This approach rested on the assumption that security policy in the case of CIP could no longer be the exclusive domain of the state, but implied "shared responsibility". Indeed, the mere composition of the commission was an expression of the merger of the PPP concept with that of critical infrastructure.

Following the key idea of PPP, the PCCIP report strongly emphasized that CIP was a challenge that could only be met through joint efforts of the state and the private sector. It noted that the interdependent infrastructures generate an environment of shared risks that could only be prevented through joint risk management. The report appealed not only to the sense of responsibility of the private corporations, who as owners and operators of most infrastructures must contribute to their security [15, p. i], but also to the self-interest of owners and operators of critical infrastructures, who were "on the frontline" and most directly threatened by cyber-attacks. Subsequently, the commission identified information-sharing between all relevant actors in the field of CIP as "the most immediate need" for the protection of critical infrastructures [15, p. 21 and 27]. President Clinton's *Presidential Decision Directives* PDD-62 and -63 [17,18] largely followed the commission's recommendations. Among other suggestions, it called on the individual sectors to create PPP in the form of *Information Sharing and Analysis Centers* (ISACs), the exact form and work of which is to be determined by the private operators themselves [19]. In 1999, the financial sector witnessed the birth of the first ISAC, soon to be followed by ISACs for other sectors [20].

The purpose of an ISAC is to exchange information on security, disruptions, and best practices among companies in the same line of business and with other ISACs. Although most ISACs are subsidized or even fully funded by the government, companies are completely at liberty to organize their ISACs as they see fit, which results in major differences between the structures of sector-specific ISACs [21]. In addition to the US, many other governments maintain similar programs where information exchange between the operators of critical infrastructures is fostered—and many even regard the exchange of information to be a top priority. The main form of PPP in the field of CIP therefore consists of information sharing platforms [49].[2]

2.2. *The limitations of a miracle solution*

However, difficulties have surfaced in recent years in terms of realizing forms of cooperation that are sometimes due to practical, sometimes to conceptual matters [14]. The core problems are, first of all, that the term "PPP" can only describe the nature of existing partnerships in a very rudimentary way, and that the majority of so-called PPP in CIP are not really PPP at all; second, that the interests of private business and of the state are often not convergent when it comes to CIP and that PPP are therefore hardly suitable as solutions; and third, that the existing forms of cooperation are too limited. All these points are discussed in some more detail below.

As described above, PPP by definition require a complementarity of goals, mutual trust, clear goals and strategies, clear distribution of risks, clear sharing of responsibilities and authority, and market- and success-oriented thinking [14, p. 124]. PPP are therefore project-based and aim to achieve lower costs and heightened efficiency. Cooperation efforts in the field of CIP, however, are often program-based (i.e., not limited by time periods) and aimed not at enhancing efficiency, but at increasing security. Especially information-sharing efforts differ clearly from project-based PPPs: It is difficult, if not impossible to formulate measurable project targets for information-sharing, since the initial aim is to build mutual trust. This process is time-intensive and hardly measurable and thus incompatible with the concept of raising efficiency, which is the foundation of traditional PPP. Furthermore, there is a dissonance that is hard to overcome between the logic of security and the logic of PPP: Generating security for citizens is a core task of the state; therefore it is an extremely delicate matter for the government to pass on its responsibility in this area to the private sector [22].

It has become quite clear that the interests of the private industry and of the state in CIP are only partially convergent and that synergy effects are therefore not always easily obtained. Specifically, private companies fear that sensitive information on past security incidents that is passed on to the state might not be treated with the necessary degree of confidentiality and cause damage to their reputation.[3] Furthermore, the majority of companies do most of their business abroad and are only partially appreciative of the necessity of national cooperation—international approaches would be of much greater interest for transnational businesses. Third, the private sector perceives the issue mainly from the perspective of business administration and thus regards it primarily as a matter of ensuring business continuity, not as a security-policy issue, which imparts a different sense of urgency concerning the problem [25,7]. But even for governments, divulging information on potential threats is a risky matter, since an accidental or intentional exposure of classified intelligence can jeopardize the activities of intelligence services and other institutions [26].

An even more serious problem is that the majority of existing instances of PPP are too narrow. Most PPP in the

[2] As argued in Section 1, the argument brought forward by this article stays on a general level, valid for the entire CIP debate. A focus on different sectors/industries would add beef to the bone, but it cannot be accomplished in this article.

[3] Studies have shown a negative correlation between the publication of security vulnerabilities and the market value of the companies concerned: cf. [23,24].

Please cite this article in press as: M. Dunn Cavelty, M. Suter, Public–Private Partnerships are no silver bullet . . . , International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.006

field of CIP today involve cooperation between a specialized agency and selected partners from the private sector (infrastructure operators). This cooperation design fails almost completely to make sufficient allowance for the horizontal and vertical integration of contemporary infrastructures. On one hand, the mostly sector-specific PPP models (such as ISACs) are hardly suited for efficient management of the interdependencies between the various infrastructures or sectors (horizontal links). On the other hand, not even large-scale businesses are able on their own to guarantee the security of the infrastructures they operate, but are dependent on a multiplicity of smaller actors (vertical links). Smaller and medium-sized enterprizes (SMEs) also have a strong need for support in the field of information security. They may be severely affected by adverse events, but in general have few resources for defending themselves against them. From the point of security-policy considerations, it is therefore important to develop models for cooperation with SMEs, since the distinction between critical infrastructures and "ordinary" companies is becoming increasingly difficult due to the ever increasing integration of all companies.

The necessity for better horizontal, vertical, and international cooperation poses significant challenges to governments. Cooperation in the form of information exchange demands strong mutual trust, since it involves the exchange of extremely sensitive information. This trust is very difficult to establish [27,21]. The fundamental problem is that trust can only be developed through collaboration, which in turn also depends on trust. The establishment of public–private information exchange is therefore an example of the "chicken-and-egg" paradox—or in other words, a classic assurance problem [28,8]. For this reason, information exchange between public and private partners usually only succeeds in a small framework with selected partners who have already established a certain degree of trust or in cases where such trust can be established reasonably easily.

3. An expanded governance model for CIP

Although some partnerships for information sharing seem to operate quite successfully, the PPP model is subject to narrow limitations in the context of CIP. Therefore, the question of alternative solutions arises. In concrete terms, what is required is an approach that does not reduce cooperation between the state and the private sector to direct partnership (as in the case of PPP), but also takes into account other forms of interaction. In order to develop such an approach, we take recourse to governance theory.[4] The theoretic foundations of governance theories consist of the differentiation from traditional government, with the government no longer being conceived as the only actor in the public sphere [30–33]. *Governance* takes place wherever political power is highly fragmented. Fragmentation of political power can occur through decentralization when government tasks and authority are delegated downwards (localization), upwards (supranationalization), or sideways (privatization) [31]. It also takes place inside the government itself through ever-increasing functional differentiation of the administration [34].

Within governance theory, a major distinction is made between neoliberal governance theory and the network governance approach [34, pp. 3–8]. The core demand of the neoliberal approach is "less government and more governance" [35, p. 34], and its main aim is the enhancement of efficiency in public administrations by transferring authority from the government bureaucracy to the private sector. As mentioned, the goal of CIP is not to raise efficiency, but to enhance security. The neoliberal approach is therefore only of limited use as the theoretical foundation of a CIP policy. In the following, we will attempt to develop an alternative model using the approach of network governance, which we describe and contrast against the neoliberal model in the Section 1. Based on the network approach, which is founded on a different understanding of public–private collaboration, the second subsection will describe the new role of the government. The third subsection will apply these theoretical considerations to CIP and show how this can help resolve some of the issues elaborated in earlier sections. The Section 4 proposes a road map for CIP meta-governance.

3.1. *The network approach of governance theory*

The main difference between the network approach and the neoliberal understanding of governance theory is that the introduction of governance structures is not regarded as a measure to raise the efficiency of the public administration, but as a consequence of *progressive specialization* in modern societies [36–38] [34, p. 18f.]. Increasingly, performing tasks requires highly specific expert knowledge. The increasing division of labor, which is seen as a hallmark of modern societies, blurs the lines between the public and the private sector. Many tasks that were previously performed by the state are today handled by specialized companies. This differentiation of the public administration can become an issue when problems arise that touch upon the essential functioning of society. The question is how the state can guarantee that such tasks will be fulfilled when the state itself no longer has the necessary capacities.

Neoliberal approaches resolve this issue of control by assuming that the state will precisely define and contractually stipulate how the tasks it delegates to companies must be fulfilled. In this way, it maintains control and can intervene if the private sector fails to meet its obligation to provide essential services. However, in conditions of increasing specialization, this assumption is no longer valid. The government simply does not have the required specialized knowledge to ensure an appropriate degree of control over outsourced functionalities and services. The example of CIP is an especially vivid manifestation of this fact: Governments are hardly able to

[4] The importance of the governance concept for CIP is already mentioned by Donahue and Zeckhauser [29]. In their article "Sharing the Watch–Public–Private Collaboration for Infrastructure Security" they use the concept of "collaborative governance" to describe public–private cooperation in the field of CIP. Their concept is based on the idea of "shared discretion" between public and private partners and is clearly distinguished from contracting-out schemes (p. 431). While Donahue and Zeckhauser discuss the rationale, risks, and opportunities of collaborative governance and point to the important role of governments in such collaborative arrangement, they do not elaborate on the theoretical background of the governance concept.

Please cite this article in press as: M. Dunn Cavelty, M. Suter, Public–Private Partnerships are no silver bullet . . . , International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.006

assess the quality of protective measures for each company that operates a critical infrastructure, as the level of protection depends on many technical and organizational factors which differ widely from business to business [29, p. 437ff], [5, p. 149]. The network approach to governance therefore assumes that modern societies require new forms of public administration [39]. The government can no longer simply issue instructions and monitor their implementation, but must shape the framework conditions in such a way that cooperation operates smoothly even without constant oversight. Public administration thus becomes a team sport where persuasion, negotiations, and mutual trust are more important than control and regulation [40].

In order to facilitate such new forms of cooperation, small and relatively homogenous networks are required that involve all actors who will and can contribute to the fulfilment of a public service in their own interest. Such actors, most of whom come from both the public and the private sectors, then organize themselves quasi autonomously. They fix rules for common action and determine the responsibilities and commitments of the individual partners [33, p. 658f.]. The various networks monitor themselves, because it is only within the network that sufficient expertise can be found to check whether all parties are meeting their obligations.

Thus, public services are provided by a plethora of independent, self-regulating, and self-organizing networks. Governments are typically also represented by the responsible agencies. It is important, however, that these agencies do not have a special status within the network. Although they represent the government, they are *primi inter pares* without authority, since the network can only function if decisions are made in negotiations where all parties are on an equal footing. The independence of these networks from the government is the crucial element of the governance concept. In the literature, reference is therefore often made to the idea of "governance without government" [32,39].

3.2. A new role for government: Meta-governance

While under traditional administration models, the government itself carries out all public tasks, the neoliberal approach recommends that it outsource services to the private industry while always retaining ultimate control. Under the network approach, the governments have a new role. Instead of distributing tasks and monitoring their fulfilment, governments take on the role of coordinators and stimulators of networks. Governments must ensure that public tasks are met by self-regulating networks and if they are not, they must initiate and fund new networks or incentivize existing networks to achieve these tasks. This indirect control is referred to as "organization of self-organization" or "meta-governance" [41,42].

Part of this meta-governance consists in the creation of framework conditions that allow networks to organize themselves. Scharpf and Mayntz point out that self-regulation can only work in the "shadow of the hierarchy", because even the internal rules and agreements between networked actors must ultimately be in line with the central state's institutions and laws [43,44]. In addition to creating framework conditions, meta-governance mainly implies coordination and promotion activities. Governments must activate new networks wherever necessary and orchestrate and modulate the existing ones [45]. In concrete terms, this means that governments first define public tasks and then verify whether they are already being carried out. If they find that a function is not being fulfilled sufficiently, the governments must create new networks or convince existing networks to fulfil it.

In this way, choosing the right instruments to promote the specialized networks becomes the most crucial responsibility of governments. One possible instrument is the traditional direct partnership between public and private actors, where the authorities engage in the network in order to contribute to the fulfilment of public services. But the governments also have a wide range of other instruments at their disposal: The scope of options ranges from regulative measures (e.g., making membership in special-purpose associations mandatory for companies) and incentives to simple support of networks through promotion or consultancy. Other possible instruments are social and economic regulation; definitions of liability; contracts between public and private partners; subsidies; loans; deficit guarantees; issuing licenses and concessions; state insurance; tax relief; or fines [45, p. 21], [42, pp. 100–103]. The choice of the appropriate instrument is crucial because the way in which the government fosters networks can change their internal structure. Although it may often be necessary to motivate networks from outside to fulfil a certain task, the self-regulation mechanisms of the network should not be undermined, as the control function would otherwise revert to the government's responsibility.

3.3. Network governance in the case of CIP

In the following, we aim to show how most of the difficulties identified above – presented here in a simplified and condensed form – can be resolved or at least alleviated by applying the network approach. We purport that if more care is taken to differentiate between the various instruments of public–private cooperation and to select and apply the most appropriate of these, some of the challenges in the field of CIP can be overcome.

Problem 1. The state has no way of monitoring whether private companies are fulfilling their functions in the area of CIP.

The loss of the government's monitoring function is a core argument for applying the network approach in CIP policy. It is difficult to establish in the framework of information sharing whether corporations are indeed passing on the relevant information. The solution of this problem is to be found in self-regulation (and self-policing) of the networks. The partners within a network know each other well and are thus able to assess whether the degree of cooperation is sufficient. Amitai Aviram therefore speaks of "network responses to network threats". He argues that pre-existing networks are often better suited to enforce norms of network security among their members than the government [8]. 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. In the US, for example, the task of reducing vulnerabilities in the financial sector's information systems was

Please cite this article in press as: M. Dunn Cavelty, M. Suter, Public–Private Partnerships are no silver bullet . . . , International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.006

largely left to the existing networks in this sector.[5] However, these arguments do not mean that the government has no monitoring function at all, but only that there should be a shift from direct monitoring of the owners and operators of CI towards the monitoring of self-regulating networks. The role of the government will be further discussed below.

Problem 2. Public–private cooperation is often difficult due to diverging interests.

The problem of divergent interests arises when partners are forced to cooperate under duress. Networks can only be successful if they are based on a sufficiently large common denominator. A direct partnership between companies and governmental agencies from the field of security policy is difficult, since they have completely different backgrounds. Furthermore, such a partnership can only be of use if the government can make a meaningful contribution to the functioning of a network. This is certainly the case with CIP, for example when governments can help the companies to assess the threat picture more clearly [46]. However, since the security agencies often lack an understanding of the specific requirements of the private sector, it may be necessary to establish new networks for cooperation. Often, these networks, located at interfaces, constitute what is known as PPP in the field of CIP. They can be successful if the actors involved focus on the common interest and have established a mutual trust. As an example, the Swiss Reporting and Analysis Centre for Information Assurance (Melde- und Analysestelle Informationssicherung, MELANI) is a successful partnership at the interface between the networks of security policy and the private industry.[6]

Problem 3. PPP can only be carried out with selected companies and must be small, since they are based on mutual trust. The number of PPP must remain limited, since an overly large number would exceed the government's capacities.

The problem of the limited number of possible partners in a PPP is only an issue if one assumes that it is mandatory for the government to work together with private businesses directly. This perspective ignores the possibility of self-regulating networks. Businesses themselves have an interest in security, and some of them are already engaged in sub-areas of CIP. The government's role can therefore frequently be limited to that of promoting existing networks with similar mandates or supporting the emergence of new networks in the field of CIP with promotional measures [8, p. 185]. This is the approach chosen in the area of information security, for example, by the British government, which supports exchange of information between SMEs in so-called Warning Advice and Reporting Points (WARPs) without being directly involved itself.[7] In addition, the network governance approach also helps to overcome the difficulties posed by the interdependence of different sectoral infrastructures. The basic idea of meta-governance as the organization of self-organization highlights the crucial role of coordination between individual sectoral networks. Examples for cross-sectoral networks that aim for coordination are the Critical Infrastructure Advisory Council (CIAC) in Australia or the Strategic Board for CIP (SOVI) in the Netherlands.[8] Such cross-sectoral networks are usually initiated and supported by the government and serve to organize the self-organization of sectoral networks.

Problem 4. Due to the intensive involvement of the government, PPP are not suited for fostering international cooperation.

International cooperation is often obstructed rather than advanced by the direct involvement of governments. Large corporations that operate critical infrastructures are frequently well-connected at the international level. Cooperation between experts can therefore evolve quite naturally. However, the impartiality of governments is often a precondition for successful cooperation. One example of an international network that has emerged independently of governments is the Forum of Incident Response and Security Teams (FIRST), where experts in the field exchange their experiences.[9]

Problem 5. There is a dissonance between the logic of security and the logic of PPP. The core function of the state cannot be outsourced.

The fifth problem can *not* be resolved with a network approach. On the contrary, the outsourcing of essential functions in the field of CIP to self-regulating networks that are not subject to government oversight is quite problematic from a security-policy point of view. Compared to the PPP concept, where the state also confers authority on private actors, but continues to monitor the fulfilment of tasks, the problem of responsibility is further accentuated in network governance, since the state limits itself to the coordination of networks. The problem of unclear allocation of responsibilities is also broadly discussed in the general literature on governance. Advocates of the network approach argue that the government is responsible for coordinating and stimulating networks, but not for the direct fulfillment of functions. However, many authors point out that in real life, expectations towards the state are really much higher [47]. The dissonance between the logic of security policy and the logic of public–private cooperation requires an open debate on the potential and the limitations of state control in the context of CIP.

3.4. *Road map for CIP meta-governance*

In an attempt to render the previous chapters more actionable we propose a four step approach for CIP meta-governance below.

[5] The Financial Service Information Sharing and Analysis Center (FS-ISAC), http://www.fsisac.com/files/FS-ISAC_Overview_2007_04_10.pdf.

[6] Melde-und Analysestelle Informationssicherung (MELANI), http://www.melani.admin.ch/index.html?lang=en.

[7] Warning Advice and Reporting Point (WARP), http://www.warp.gov.uk/Index/indexintroduction.htm.

[8] Critical Infrastructure Advisory Council (CIAC): http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/AbouttheTISN_CriticalInfrastructureAdvisoryCouncil_CriticalInfrastructureAdvisoryCouncil. Strategic Board for CIP (SOVI): cf. [1, p. 287].

[9] Forum of Incident Response and Security Teams (FIRST), http://www.first.org/about/.

Please cite this article in press as: M. Dunn Cavelty, M. Suter, Public–Private Partnerships are no silver bullet . . . , International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.006

Step 1: The fundamental idea of meta-governance is that the government coordinates existing networks in such a way that the required task is performed optimally according to the government's requirements. However, the coordination of various networks is only feasible if the ultimate intention is clear. The first step, therefore, is a clear definition of goals and priorities. They must be imbedded in a larger (security) political, but also economic and social context. Once the goals and priorities have been established, the next step is to communicate them to the existing networks. According to meta-governance theory, optimal communication by the government of the importance of a task and of the related expectations plays a substantial role in encouraging the existing networks to perform the task (voluntarily) [42, p. 101]. The more clearly the priorities and expectations are defined, the easier subsequent steps will be.

Step 2: The second step in meta-governance is to analyze the status quo and to identify where action is required. It is important to study which networks exist, whether they are already engaged in fulfilling the tasks defined in Step 1, and how they could be motivated to undertake further efforts. Additionally, cooperation between the various networks must be monitored and the need for coordination identified. Clear, politically founded, and applicable definitions and concepts – what is part of CIP, what is not, what is to be achieved, what is the desired shape of functioning networks, etc. – are absolutely indispensable parts of such an analysis.

Step 3: When a requirement for action has been identified, the third step is to identify suitable instruments of meta-governance. This is the most difficult step in the process. It is sensitive because there is an inherent danger of selecting instruments that intrude too directly, thus undermining the self-regulation mechanism of networks. This danger can be reduced according to how well the priorities have been previously defined and how precisely the status quo can be described. Ideally, the choice of instrument is derived by default from the divergence between the goals and the status quo; in reality, however, the choice of instrument is always also determined by political processes [48]. It is thus important to take into consideration the entire range of direct and indirect instruments and not to be constrained to an (over-simplified) notion of PPP. In certain cases, coercion and regulation will still appear as valid option: The stronger the security policy aspects are emphasized in a particular (sub-)sector, the more likely market intervention becomes; more emphasis is then given to the negative outcomes of globalization than to its positive effects. The negotiation of governance elements is a continuous political process that depends strongly on threat perceptions and other factors.

Step 4: In the fourth and final step, the efficiency of measures is analyzed. A government authority checks whether, having applied the selected governance instruments, the networks now meet their tasks in such a way that the defined goals and priorities can be achieved. It is important that this step, too, should be based on a well-founded analysis of the status quo. The involved authorities should also realize that many of the networks cannot be steered directly and their goals cannot be reached within short time periods. In such cases, process management also involves a step-by-step approach, without having unrealistic expectations of partnerships that have only been recently established. Thus, the final step leads automatically back to the assessment of the status quo (Step 2). As the following illustration shows, meta-governance must therefore be regarded as a continuous process (Fig. 1).

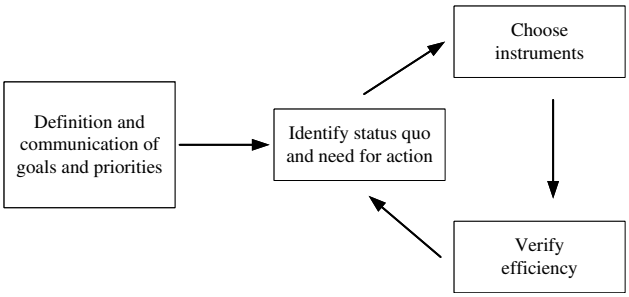


Fig. 1 – The meta-governance process.

4. Conclusion

We have attempted in this article to demonstrate the usefulness and limitations of PPP in the field of CIP by first offering a critical discussion of the concept and then setting it on a more solid theoretical foundation. We have shown that the PPP model was originally developed in a very different context and aimed primarily at enhancing efficiency. Nearly all of the problems that arise where PPP are formed for the purpose of CIP can be reduced to the fact that they are primarily intended to enhance security rather than efficiency. In reality, however, PPP are only one of many possible forms of cooperation: If they are perceived, in accordance with the network approach of governance theory, as part of a more diverse toolbox, the result is a liberating step away from the PPP concept, which restricts options, towards a new understanding of the role of the state in this area.

Because the network approach of governance theory is based on the notion of self-regulating networks, the state's main task is no longer (as in classic neo-liberal concepts of governance) to monitor the actors that collaborate with it, but rather to coordinate and stimulate functional networks so that they will fulfil the tasks required by the state in the best possible way. The network approach redefines the role of the state: Public administration no longer contracts tasks and monitors their fulfilment, but shapes the conditions for the self-organization of networks. Existing networks are coordinated and supported by the government and new networks are activated where existing networks have broken down or fail to provide the functions they are charged with.

In that way, the network approach to CIP constitutes a middle way between the poles of interventionist and hands-off CIP policies. The network approach takes into account that ubiquitous and absolute state control and provision of security are no longer possible in the field of CIP and that the state depends on the assistance of non-state actors even when it comes to core state functions. At the same time, the network approach defines new forms for government intervention: The activation, stimulation and coordination of networks, which can be described as the organization of self-organization or the meta-governance of CIP.

Please cite this article in press as: M. Dunn Cavelty, M. Suter, Public–Private Partnerships are no silver bullet . . . , International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.006

REFERENCES

[1] 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.

[2] M. Dunn Cavelty, K.S. Kristensen (Eds.), Securing the Homeland: Critical Infrastructure, Risk, and (In)Security, Routledge, London, 2008.

[3] R. Anderson, T. Moore, The economics of information security, Science 314 (2006) 610–623.

[4] P.E. Auerswald, L.M. Branscomb, T.M. La Porte, E.O. Michel-Kerjan, Who will act—Integrating public and private interests to make a safer world, in: Idem (Ed.), Seeds of Disaster Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, 2006, pp. 483–505.

[5] J.J. Andersson, A. Malm, Public–Private Partnerships and the challenge of critical infrastructure protection, in: M. Dunn, V. Mauer (Eds.), International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects, Center for Security Studies, Zurich, 2006, pp. 139–168.

[6] D. Assaf, Conceptualizing the use of Public–Private Partnerships as a regulatory arrangement in critical information infrastructure protection, in: A.O. Peters, L. Koechlin, T. Förster, G.F. Zinkernagel (Eds.), Non-State Actors as Standard Setters, October 2009 (in press).

[7] D. Assaf, Models of critical information infrastructure protection, International Journal of Critical Infrastructure Protection 1 (2008) 6–14.

[8] A. Aviram, Network responses to network threats: The evolution into private cyber-security associations, in: M.F. Grady, F. Parisi (Eds.), The Law and Economics of Cybersecurity, Cambridge University Press, Cambridge, 2006, pp. 143–192.

[9] E.S. Savas, Privatizing the Public Sector—How to Shrink Government, Chatham House Publishers, Chatham, 1982.

[10] D. Budäus, G. Grüning, Public Private Partnership—Konzeption und probleme eines instruments zur verwaltungsreform aus sicht der public choice theorie, in: D. Budäus, P. Eichhorn (Eds.), Public Private Partnership—Neue Formen öffentlicher Aufgabenerfüllung, Nomos Verlagsgesellschaft, Baden-Baden, 1997, pp. 25–65.

[11] P. Vaillancourt Rosenau (Ed.), Public–Private Policy Partnerships, The MIT Press, Cambridge, MA, 2000.

[12] S. Linder, Coming to terms with the Public–Private partnership—A grammar of multiple meanings, in: P. Vaillancourt Rosenau (Ed.), Public–Private Policy Partnerships, The MIT Press, Cambridge MA, 2000, pp. 19–36.

[13] S. Linder, P. Vaillancourt Rosenau, Mapping the terrain of the Public–Private policy partnership, in: P. Vaillancourt Rosenau (Ed.), Public–Private Policy Partnerships, The MIT Press, Cambridge, MA, 2000, pp. 1–19.

[14] V. Kouwenhoven, Public–Private Partnership: A model for the management of Public–Private cooperation, in: J. Kooiman (Ed.), Modern Governance. New Government–Society Interactions, Sage, London, 1993, pp. 119–130.

[15] PCCIP President's Commission on Critical Infrastructure Protection, critical foundations, Protecting America's Infrastructures, Washington, DC, 13 October 1997.

[16] B. Lopez, Critical infrastructure protection in the United States since 1993, in: P.E. Auerswald, L.M. Branscomb, T.M. La Porte, E.O. Michel-Kerjan (Eds.), Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, 2006, pp. 37–50.

[17] W.J. Clinton, Protecting America's Critical Infrastructures: Presidential Decision Directive 63, Washington, DC, 22 May 1998.

[18] W.J. Clinton, Protection Against unconventional threats to the Homeland and Americans overseas: Presidential Decision Directive 62, Washington, DC, 22 May 1998.

[19] National Security Council, White Paper, The Clinton Administration's policy on critical infrastructure protection: Presidential Decision Directive 63, Washington, DC, May 1998.

[20] US general accounting office, critical infrastructure protection: Establishing effective information sharing with infrastructure sectors, General Accounting Office, Washington, DC, 2004.

[21] D.B. Prieto, Information sharing with the private sector: History, challenges, innovation, and prospects, in: P.E. Auerswald, L.M. Branscomb, T.M. La Porte, E.O. Michel-Kerjan (Eds.), Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, 2006, pp. 404–428.

[22] S. Percy, Mercenaries: Strong norm, weak law, International Organization 61 (2007) 367–397.

[23] K. Campbell, L.A. Gordon, M.P. Loeb, L. Zhou, The economic cost of publicly announced information security breaches: Empirical evidence from the stock market, Journal of Computer Security 11 (2003) 431–448.

[24] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers, International Journal of Electronic Commerce 9 (2004) 69–104.

[25] I. Abele-Wigert, Challenges governments face in the field of critical information infrastructure protection: Shareholders and perspectives, in: M. Dunn, V. Mauer (Eds.), International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects, Center for Security Studies, Zurich, 2006, pp. 69–88.

[26] J.D. Moteff, G.M. Stevens, Critical Infrastructure Information Disclosure and Homeland Security, Congressional Research Report for Congress, RL31547, 29 January 2003, Congressional Research Service, Washington, DC.

[27] E. Frye, Information-sharing hangups: Is antitrust just a cover? The CIP Report 1, 2003, pp. 6–7.

[28] A. Aviram, A. Tor, Overcoming impediments to information sharing, Alabama Law Review 55 (2004) 231–279.

[29] J.D. Donahue, R.J. Zeckhauser, Public–Private collaboration for infrastructure security, in: P.E. Auerswald, L.M. Branscomb, T.M. La Porte, E.O. Michel-Kerjan (Eds.), Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, 2006, pp. 429–456.

[30] B. Jessop, The changing governance of welfare: Recent trends in primary functions, scale and modes of coordination, Social Policy and Administration 33 (1999) 348–359.

[31] E. Krahmann, Conceptualizing security governance, Cooperation and Conflict 38 (2003) 6–26.

[32] E.-O. Czempiel, J.N. Rosenau, Governance Without Government: Order and Change in World Politics, Cambridge University Press, Cambridge, 1992.

[33] R.A.W. Rhodes, The new governance: Governing without government, Political Studies 44 (1996) 652–667.

[34] M. Bevir, R.A.W. Rhodes, A decentered theory of governance: Rational choice, institutionalism, and interpretation, Working Papers of the Institute of Governmental Studies, Number 10, Berkeley, 2001.

[35] D. Osborne, T. Gaebler, T. Reinventing, Government: How the Entrepreneurial Spirit is Transforming the Public Sector, Addison-Wesley, Reading, MA, 1992.

Please cite this article in press as: M. Dunn Cavelty, M. Suter, Public–Private Partnerships are no silver bullet . . . , International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.006

[36] J. Kooiman, Findings, speculations and recommendations, in: J. Kooiman (Ed.), Modern Governance. New Government–Society Interactions, Sage, London, 1993, pp. 249–262.
[37] G. Stoker, Governance as theory: Five propositions, International Social Science Journal 50 (1998) 17–28.
[38] G. Stoker, Theory and urban politics, International Political Science Review 19 (1998) 119–129.
[39] G. Peters, J. Pierre, Governance without government? Rethinking public administration, Journal of Public Administration Research and Theory 18 (1998) 223–243.
[40] L.M. Salamon, The tools approach and the new governance: Conclusion and implications, in: L.M. Salamon (Ed.), The Tools of Government: A Guide to the New Governance, Oxford University Press, Oxford, 2002, pp. 600–610.
[41] B. Jessop, The rise of governance and the risk of failure: The case of economic development, International Social Science Journal 50 (1998) 29–46.
[42] E. Sorensen, E. Metagovernance, The changing role of politicians in processes of democratic governance, The American Review of Public Administration 36 (2006) 98–114.
[43] F. Scharpf, Die Handlungsfähigkeit des Staates am Ende des zwanzigsten Jahrhunderts, Politische Vierteljahresschrift 32 (1991) 621–634.
[44] R. Mayntz, F. Scharpf, Steuerung und Selbstorganisation in staatsnahen Sektoren, in: R. Mayntz, F. Scharpf (Eds.), Gesellschaftliche Selbstregulierung und politische Steuerung, Campus, Frankfurt, New York, 1995, pp. 9–38.
[45] L.M. Salamon, The new governance and the tools of public action: An introduction, in: L.M. Salamon (Ed.), The Tools of Government: A Guide to the New Governance, Oxford University Press, Oxford, 2002, pp. 1–47.
[46] M. Suter, A generic national framework for critical information infrastructure protection, Meeting background paper for the 2nd facilitation meeting for WSIS Action Line C5, International Telecommunication Unit, ITU, Geneva, 2007.
[47] P.L. Posner, Accoutability challenges of third-party government, in: L.M. Salamon (Ed.), The Tools of Government: A Guide to the New Governance, Oxford University Press, Oxford, 2002, pp. 523–551.
[48] G. Peters, The politics of tool choice, in: L.M. Salamon (Ed.), The Tools of Government: A Guide to the New Governance, Oxford University Press, Oxford, 2002, pp. 552–564.
[49] US General Accounting Office, Information Sharing—DHS should take steps to encourage more widespread use of its program to protection and share critical infrastructure information, General Accounting Office, Washington, DC, 2006.

Please cite this article in press as: M. Dunn Cavelty, M. Suter, Public–Private Partnerships are no silver bullet . . . , International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.006