EDITORIAL

Public-Private Partnerships as the Solution to Critical Infrastructure

Traditionally, the role of the State has been as the conduit for providing public services. The term *public services*, which often refers to services that are offered to the general public, highlights that a service has been assigned a specific role in the public interest, or refers to the ownership or status of the entity providing the service. In the latter situation, public service fuses with the concept of *public sector*, which covers the State and its organs, bodies governed by public law and undertakings controlled by public authorities. Two models for the treatment and regulation of public services have been developed based on different theoretical and conceptual values. One model theorises that public services capture the general needs of the public and are delivered through external market-based mechanisms, whereby the public sector interfaces or competes with private sector undertakings; by contrast, other models describe public services as being essential facilities (for example defence, policing) which should be sheltered from competition in order to ensure the integrity of their delivery.

Technically, every PPP project is a long-term arrangement of transfer of risks which are traditionally borne by the public sector to the private sector for which the latter is financially compensated for the willingness to bear the risks. PPP is an effective approach to enhance project productivity by bringing in management efficiency and creative skills from business practice, and reducing governmental involvement by using private sectors in the provision of public services. A PPP contract mainly apportions the project-associated risks to the public and private sector. Best practice suggests an optimal rather than a maximum risk transfer from the public to private sector. A problem may, however, occur if risk is inappropriately transferred, as the government may pay a premium higher than necessary or jeopardise the long-term sustainability of a PPP arrangement or is merely gaining the illusion of risk transfer, since it is likely that the risk will be transferred back to the government in the form of higher risks, risk premiums, and project problems. The issue of balancing project risks is more exuberated in the context of complex projects where the potential for competition is much more limited than it is in other sectors.

Under the PPP approach, the project associated risks are transferred from the public to the private sector. The central issue to address is who best bears what risk. Efficient risk allocation dictates that risk must rest with the most able party to retain. If the principle is violated, the government may face higher risk premium than necessary or illusion of risk transfer. Additionally, the basic principles of transparency, cost effectiveness and quality soundness must be ensured in all decisions.

Understanding, therefore, the process of proper risk allocation will certainly help translate the project risks into effective PPP contracts, depending on the scope of defined tasks and responsibilities, and thus avoid the so-called “illusion of risk transfer” in the quest for more efficient service provision to the public.

Risk in critical infrastructure appears as *sui generis* risk. Such risk cannot be quantified and determined as enterprise risk, a generic category of risks which could potentially treated contractually and transferred by the public sector to the private sector or retained by the party to an arrangement which is suited best to borne such risks.

Risk in critical infrastructure, being either internal or external, is endemic to such services and when critical infrastructure is delivered by public-private partnerships or owned

by private actors, the treatment of such risk merits a third-party approach. Such third-party could be an industry in itself, such as insurance, re-insurance or hedge fund insurance, bond finance, or a sector / industry approach which related to the owners/operators of the relevant infrastructure, by means of collective apportioning and mitigation of risks associated with the failure of providing services from such infrastructure. The most innovative way of treating risk of critical infrastructure remains in the discretion of EU Member States, in the form of integrating costs related to risk assessment and security measures to protect critical infrastructure into tariff arrangements of relevant services. In such manner, the end-user / consumer of services ensures and collectively insures their delivery against any type of risk which is not quantified and determined as part of corporate arrangements between the State and the private sector provider of services.

The Stockholm Programme and the EU Internal Security Strategy have identified that critical infrastructure protection (CIP) must ensure that services vital to the society continue to function by increasing their resilience against all threats and hazards. An EU critical infrastructure is an *'asset or system located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'*.

The European Critical Infrastructures Directive – A Hint to PPPs as a Solution

In an attempt to co-ordinate efforts to quantify risk in critical infrastructure which cannot be contained in any contractual relation between the State and the providers of the services related to the relevant critical infrastructure, the European Critical Infrastructures Directive 2008/114/EC purports to identify and designate European critical infrastructures and assess the need to improve their protection. The Directive has forced Member States to establish a process to identify and designate European critical infrastructures in the energy and transport sectors. However, this process reflects on a sector-focused approach which in itself is the major challenge for Member States, as the criticalities of infrastructure do not recognise sectoral boundaries. The Directive has mainly encouraged bilateral engagement of Member States instead of a pan-European forum for risk assessment and regulation in critical infrastructure.

The Directive has encouraged policies for the protection of national critical infrastructures and the improvement of security which has resulted in concrete actions such as the creation of specific national bodies to deal with critical infrastructure protection policies. In the energy sector, despite the fact that main energy transmission networks are not included, there has been progress in putting in place both risk management and protection measures in cooperation with operators. This development reflects the major development of a cross-sectoral approach to risk in critical infrastructure. Operators of critical infrastructures, including those operating in the energy and transport sectors, would fall under the risk management and incident reporting requirements of the proposed Directive on Network and Information Security, thus creating a "system" or "service" approach of critical infrastructure protection.

A system or service approach of critical infrastructure protection reveals a different dimension of the problem. Risks which are related to the critical infrastructure protection could be internal or external to that infrastructure, the latter including material and IT assets, networks, services, and installations that, if disrupted or destroyed, could or would have a serious impact on the health, security, or economic well-being of citizens and the efficient functioning of the State. If risks are internal to the infrastructure, the contractual

arrangements between the State and the provider of the infrastructure can accommodate risk identification, treatment and subsequent management. The mechanism of risk transfer is the major instrument which calibrates the relation between the State and the operator of the infrastructure (often a PPP) and provides for a resolution of internal risks.

If risks are external to the infrastructure, they touch upon structural threats as well as intentional, actor-based attacks and distinguish between two types of risk categories; on the one hand, risks emanating from unforeseen natural catastrophes and on the other hand, risks emerging from human-induced disasters, including an extensive spectrum of external actor involvement ranging from cyber threats, organised crime, religious fanaticism, terrorism, unruly, disaffected or dissatisfied individuals.

In relation to risk assessment and risk management methodologies for critical infrastructure protection, the European Commission has encouraged the development of individual/sectoral approach and in particular, the development of a risk assessment methodology to enhance security awareness in air traffic management; the assessment of resilience to threats to control and data management systems of electrical transmission networks; and an interactive risk assessment in the critical infrastructure field based on earth observation data and an integrated geographic information system.

The European Union Programme for European Critical Infrastructure Protection (EPCIP) for energy, transportation, and finance focuses on four main areas:

- a) the creation of a procedure to identify and assess Europe's critical infrastructures and learn how to better protect them. This procedure was established for the energy and transport sectors in the Identification of European Critical Infrastructures Directive;
- b) measures to aid protection including expert groups at EU level and the creation of the Critical Infrastructure Warning Information Network (CIWIN) – an internet-based communication system for exchanging information, studies, and best practices;
- c) funding for over 100 critical infrastructure protection projects between 2007 and 2013. These projects focused on a variety of issues including national and European information sharing and alerting systems, the development of ways to assess interdependence between ICT and electricity transmission networks, and the creation of a “good practices” manual for policy makers; and
- d) international cooperation with European Economic Area (EEA) and European Free Trade Area (EFTA) countries, as well as expert meetings between the EU, USA, and Canada.

The individual/sectoral approach of risk assessment and risk management methodologies for critical infrastructure protection has identified a major deficiency where critical infrastructures are not treated as an interconnected network. The European Commission evaluated the progress made by EPCIP and suggested the programme enter a new more practical phase for the future. This phase involves launching a pilot project analysing four critical European infrastructures with regards to possible threats. These include the EU's electricity transmission grid; the EU's gas transmission network; EUROCONTROL – the EU's Air Traffic Management; GALILEO – the European programme for global satellite navigation.

A uniform and converged playing field on security at European level indicates the need for States, owners and operators of critical infrastructure to share information, data and systems in order to ensure efficient and secure operations at all times. In particular, for energy infrastructure, it is necessary to be subject to both European and national legislation and risk assessment to determine its criticality, reflecting its strategic importance. The costs related to risk assessment and security measures to protect critical infrastructure need to be integrated into EU Member States' tariff arrangements.

The recognition and the offering of public-private partnerships have been seen as a credible solution to bridge the *infrastructure deficit* in critical sectors. The infrastructure deficit reflects the gap between existing levels of assets and service networks, and the need and expectation of the citizens and the society at large for public services. The technical complexity and the enormity of investment for public service networks, the chronic underinvestment by States in critical infrastructure and the constant budgetary constraints imposed on contemporary governments appear as valid reasons for engaging the private sector in the delivery of public services and the relevant critical infrastructure.

Christopher H. Bovis