

GOVERNANCE

BASEL INSTITUTE ON GOVERNANCE

Conference «Non-State Actors as Standard Setters: The Erosion of the Public-Private Divide» | February 8-9 2007 | Hotel Hilton Basel, Switzerland

Conceptualizing the use of public-private partnerships as a governing mechanism in critical information infrastructure protection

Dan Assaf, Doctoral Candidate, University of Toronto, Canada

This paper provides a descriptive, positive, and normative analysis of the use of public-private partnerships as a governing mechanism in addressing the problem of critical information infrastructure protection¹ ("CIIP"). CIIP has become a very topical issue since the late 1990s, and especially since the 9/11 attacks. An important part of addressing this issue is the choice of regulatory tools and governing mechanisms. Many Western countries endorsed the creation of public-private partnerships to govern CIIP, including in setting security standards. Notwithstanding this, the dynamics of such arrangements remains significantly under-researched and under-conceptualized. The aim of this paper, therefore, is to conceptualize the use of this governing mechanism in the context of CIIP.

This paper is divided into two parts. In the first part, it provides a positive explanation for the emergence of the unique relationship between the public and private sectors in protecting critical information infrastructures. The tendency of governments to promote public-private partnerships in order to protect critical information infrastructures is an outcome of two developments. First, the bias of neo-liberal democracies toward privatization has led to the transfer of ownership and operation of critical infrastructures to the hands of the private sector. The second development was the dramatically changing nature of global security threats in the 21st century – in the form of information warfare, cyber-crime, and economic espionage– targeting, inter alia, critical information infrastructures. The convergence of these two develop-

ments created a "security gap": While the protection of critical information infrastructures is an essential part of a nation's national security, the potential targets are mostly private entities, pursuing private objectives rather than public values such as national security. The existence of this security gap, together with the bias toward private provision of public goods and services, provided the underlying rationale for the decision of governments to endorse the use of public-private partnerships in governing CIIP.

Having pointed to the rationale for the use of public-private partnerships in governing CIIP, the second part of this paper demonstrates the implications of this governing arrangement on such notions as accountability, transparency (with the former two being strongly related) and legitimacy, and questions the suitability of using this arrangement in the security realm. It will draw from existing literature that critically analyzes the merits and limits of privatization in general and privatization in the security domain in particular, and analyze the advantages and drawbacks of such phenomenon. This analysis will lead to an argument that the state should be cautious in promoting the use of public-private partnerships in the security domain, and where it chooses to do so, it should assume a more dominant role (in the forms of guidance and oversight). Eventually, the conclusions of this paper may serve as a test case for future instances of "security gaps" that require the active collaboration of the public and private sectors.

¹ "Critical Information Infrastructures" is an incorporation of two terms. The first is "Critical Infrastructures" and the second is "Information Infrastructures". Altogether, critical information infrastructures are those parts of the information infrastructure that are essential for the continuity of critical infrastructure services. In other words, they are the communications and information networks and facilities underlying the critical infrastructures, such as telecommunication, power grids, transportation, emergency services, financial institutions, etc.