CRN ROUNDTABLE REPORT

6th Zurich Roundtable on Comprehensive Risk Analysis and Management

Network Governance and the Role of Public-Private Partnerships in New Risks

27 November 2009

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

This report is available on the Internet: www.crn.ethz.ch

Center for Security Studies, ETH Zurich

Author: Jennifer Giroux and Manuel Suter

Postal address:

Center for Security Studies
ETH Zurich SEI
8092 Zürich
Switzerland
Tel. +41 44 632 40 25
Fax +41 44 632 19 41
www.crn.ethz.ch
crn@sipo.gess.ethz.ch

TABLE OF CONTENTS

ZURICH ROUNDTABLES ON COMPREHENSIVE RISK ANALYSIS AND MANAGEMENT

The 6th CRN Roundtable, which took place on 27 November 2009 at ETH Zurich, continued the Zurich Roundtable series on Comprehensive Risk Analysis and Management of the Crisis and Risk Network (CRN). It was successfully launched in December 2005 as a new format of discussion on topics related to security risks and vulnerabilities, risk analysis and management, emergency preparedness, and crisis management. The Roundtables are intended as a platform for bringing together a select group of experts to explore the character and dynamics of the contemporary risk environment. By establishing a collaborative relationship and exchange among like-minded experts, they foster a continuous international risk dialog and contribute to a better understanding of the complex challenges confronting the risk community today.

Topics of previous roundtables include:

- Strategic Early Warning and Public Policy Planning (5th CRN Roundtable, 5 December 2008)
- Crisis Management in the Case of Critical Infrastructure Breakdowns (4th CRN Roundtable, 30 November 2007)
- How to Detect Emerging Risks (3rd CRN Roundtable, 24 November 2006)
- Risk Communication in Turbulent Times (2nd CRN Roundtable, 12 May 2006)
- National Approaches to Risk Profiling (1st CRN Roundtable, 9 December 2005).

The CRN reaches out to professional communities in public policy, corporate management, academia, and the civil society. The CRN is comprised of a research team that is part of the Center for Security Studies (CSS) at ETH Zurich, a renowned academic institute in the field of international and national security policy. More information about the CRN (www.crn.ethz.ch) and the Center for Security Studies (www.css.ethz.ch) can be found on the internet.

1 INTRODUCTION

Globalization has opened the gates to a dynamic world where societal, governmental, and economic actors have a collective role in managing modern complex interdependent security challenges. New risks such as a breakdown of critical infrastructures, cyber-attacks, and international terrorism blur the boundaries between the public and private sectors and thus cannot be handled via traditional hierarchical top down approaches. Over the last decade, Public-Private Partnerships (PPPs), collaborative platforms for actors in the public and private sector, have gained importance in the field of security policy and proliferated across the globe. Yet, despite the popularity of PPPs, such structures come with challenges in their formation, management, and effectiveness. To date a comprehensive approach has yet to be developed as academics and policy analysts continue to grapple with understanding this approach to governing the contemporary landscape.

The growing body of research within the field of network governance has brought to light some interesting insights that have added the understanding of PPPs. Most notably, public management scholars have developed the network governance approach to describe and analyze the role of private and non-profit actors in public administration. In doing so, theoretical concepts for public-private collaboration have been developed and applied to the management of new risks yet questions persist. Thus, this roundtable was held to help shed some light on the network governance approach and the role that PPPs play in addressing modern-day risks. More specifically, this roundtable sought to meet the following objectives:

- Bring together experts from academia and the public and private sectors
- Provide a platform to enhance participants understanding of governance structures and network governance in particular
- Examine the emerging field of network governance in the area of new risks such as information security, critical infrastructure protection, and international terrorism
- Provide examples of Public-Private Partnerships (PPPs) used to address today's risks

The roundtable was structured in way that sought to fuse insights from practitioners and scholars. Session 1 delved into the theoretical background on network governance and the significant role that trust plays in networks and partnerships. The second session was a platform for practitioners to exchange their experiences using PPP to address security issues – critical infrastructure protection, information security, and international terrorism. The final session brought the experts together for a moderated discussion guided by some of the following questions:

- What are the specific challenges of public-private partnerships in the field of security?
- Are there some fields in security in which public-private collaboration is easier?
- What are the factors of success?
- What are potential organizational forms for public-private collaboration?
- How does one address the issue of accountability in networks operating in the field of security policy?
- How can governments better manage networks?
- What are the incentives for private actors to collaborate with the public sector?

2 SESSION I: THEORETICAL CONSIDERATIONS

Session I successfully established the theoretical background for the discussion on network governance and Public-Private Partnerships (PPPs) in new risks. Dr. Patrick Kenis (TiasNimas Business School, Tuniversity of Tilburg) first explained the concepts and definitions of governance in its various forms and highlighted different forms of network governance. Following this, Dr. Erik-Hans Klijn (Erasmus University of Rotterdam) focused on the crucial question of trust in networks and emphasized the importance of network management. Both presentations were followed by lively and informative discussions.

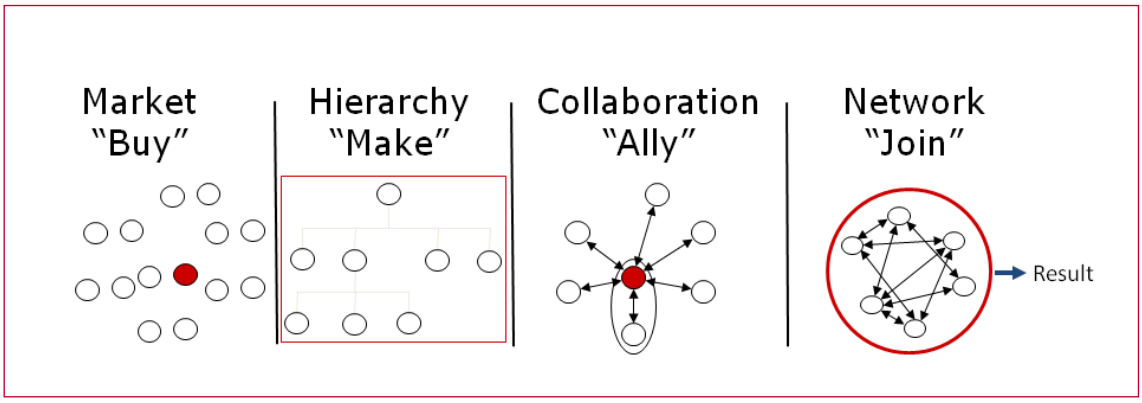
2.1 Structure, Forms, Functions of Public-Private Collaborations

Dr. Patrick Kenis opened by describing key concepts and defined governance as the use of institutions, structures of authority and collaboration to allocate resources and coordinate or control activity in society or the economy. He explained ways in which governance can be achieved; the two classic forms known as markets and hierarchies. In the former, the actors are independent and their interactions are determined by prices. In the latter, hierarchies are characterized by vertical relationships between the actors and are steered by the use of authority. However markets and hierarchies are not the only governance forms. Collaborations and networks are also types of governance. Collaboration emerges when actors cooperate in order to acquire access to resources and reduce uncertainties. Networks, on the other hand, involve actors that not only collaborate but also develop collective goals. Network governance can thus be defined as governance through relatively stable cooperative relationships between three or more legally autonomous organizations based on horizontal rather than hierarchical coordination, recognizing one or more network or collective goals.

In the following, Dr. Kenis focused on the network form of governance. He highlighted different policy areas in which network governance is applied: health care, prevention of drug abuse and disaster preparedness. Networks have become prevalent because they are seen as superior way to deal with wicked problems. It is often only in networks (which include different specialized organizations) where enough resources and knowledge is available to deal with complex problems. In addition, networks are able to provide unique, flexible and tailored products, whereas the other governance modes depend on standardized processes and therefore lack this capability.

However, networks are in many ways the most demanding form of governance due to their complexity. In order to achieve results via network governance, the networks themselves need to be governed. Thus,

Four types of governance (extracted from Kenis' presentation)



the governance of networks has become a central topic of research.

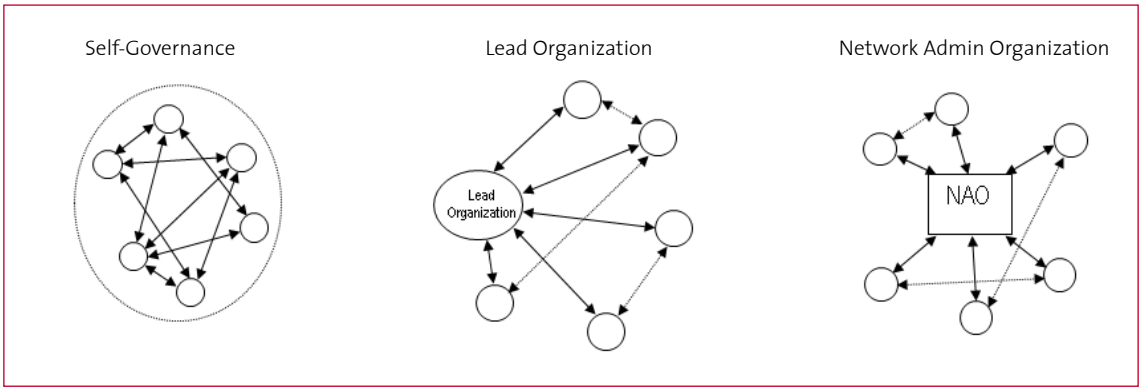
Based on research carried out with scholar Keith Provan, Dr. Kenis presented three ways to govern a network: There is self-governance, governance by a lead organization and governance by a network administrative organization. Self-governance has no administrative entity as the network is managed collectively by all participants. This form of governance is most likely to be effective in small networks (few participants), in which members trust each other and maintain a high level of goal consensus. The advantage of this form of governance is that it is relatively easy to establish and members tend to be committed to the network. In contrast, the drawbacks are that it requires frequent meetings (since all decisions have to be taken collectively), reaching consensus can be difficult and time-consuming, and that there is no "face" of the network (i.e. contact to the outside).

The second approach, governance by a lead organization, is an administrative entity that also operates as a member of the network. To be effective, members must trust the lead organization as it bears the responsibility for management and goal-setting - though consensus is not as important as it is the case in self-governance. Overall, lead organization governance can be an efficient and effective approach however there is the risk that it can create a large imbalance within the network. For example, the lead organization can become too authoritative or the members lack internal commitment.
Governance by a network administrative organization (NAO) is the third approach. In this form, an external administrative entity is set up to manage and serve as a coordinator for a specified network. This allows outcomes to be produced even though many of the members may not trust or interact with each other. In other words, the relationships between the individual network members are not crucial to produce network outcomes. As a result, Dr. Kenis revealed that this approach has proven to be more efficient and sustainable although it can be more costly to maintain.

Dr. Kenis concluded his presentation by referring to a paper on the role of network governance in crisis management, published by Donald P. Moynihan in 2008. This article argued that in a crisis the Incident Command Systems (ICS) can be described as networks which are governed by a Network Administrative Organization. Since today's crisis often require collaboration of many different partners, they can only be dealt with by inter-organizational networks. This proves that the concepts of network governance are highly relevant in the context of security policy and new risks.

Dr. Patrick Kenis is Academic Dean of TiasNimbas Business School and Professor of Policy and Organisation Studies at the University of Tilburg, the Netherlands

Three forms of network governance (extracted from Kenis' presentation)



2.2 The Challenges of Network Management: Coordinating, Mediating and Building Trust in Networks

Dr. Erik-Hans Klijn provided the second presentation which delved more deeply into the characteristics of networks by discussing the role of trust in PPPs. Like Dr. Kenis, he identified networks as a key component to managing the complexity of today's policy challenges that require information exchange and cooperation between public, private and semi-private partners. He emphasized that the basic driver for the development of networks is the mutual dependency of these actors on each other. While the multiplicity of organizations in a network increases its capabilities (since more resources and knowledge are available), it also renders the network itself more complex. Dr. Klijn highlighted three levels of complexity within networks:

- Strategic complexity: all actors in networks are autonomous and act strategically;
- Content complexity: all actors have their own perception of the problem and may interpret information in different ways;
- Institutional complexity: the decisions taken by the network cross different sectors and must be implemented in different contexts.

Because of their complexity, networks need to be managed. Referred to as "Network Management", Dr. Klijn noted how this involves three different types of activities: 1) Process design (the definition of rules for the interactions between network members); 2) Process management (connecting actors, exploring content, arranging interactions); 3) Institutional design (changing the institutional structure of a network). Within this, other factors to consider are content management and the management of interactions. Managing the content refers to the responsibility of a network manager to create valuable content for all members. This requires constant management as the content changes and must continue to remain in line with the values and needs of the participants. Because members in a network are different and act strategically, it is equally important to actively manage their interactions. This involves the stimulation or termination of specific interactions, the coupling of actors, or the facilitation of processes. In addition, the organizational arrangements need to be constantly evaluated. To emphasize the importance of network management, Dr. Klijn presented results of research on an environmental project where a strong correlation was found between the number of managerial strategies applied and the perceived (positive) outcomes of networks.

The second part of Dr. Klijn's presentation was dedicated to the crucial question of *trust* in networks. Trust can be defined as the stable perception of actor A about the intentions of actor B and as the expectation of actor A that actor B will refrain from opportunistic behavior. In the literature on network governance trust is often described as a prerequisite to the formation of networks. However, based on his empirical research Dr. Klijn argues that not all networks are characterized by a high level of trust among their members. Networks are therefore not necessarily based on trusted relationships, rather they should be regarded as a vehicle to build trust.

Three Benefits of Trust:

- *Trust facilitates cooperation* by reducing uncertainties, which lowers transaction costs.
- *Trust solidifies cooperation* by enhancing the stability of relations, which encourages investments in relationships.
- *Trust enhances network performance* by stimulating mutual learning & knowledge

While the benefits of trusted relationships are considerably high, trust is not easy to establish. First, trust is built over time and through regular interactions between members. It cannot be induced by the network manager and it becomes vulnerable to erosion when a member(s) exhibits opportunistic behavior. Second, though Dr. Klijn has found trust to be an important factor, it is not always beneficial for the network as it can lead to group-think that impedes innovation as well as the readiness of the network to include new members. Nevertheless, Dr. Klijn's referenced his empirical research on environmental projects which clearly supports the assumption that trust is crucial for networks in order to produce services. He concluded by emphasizing that network management activities and higher level of trust positively affect the performances of networks and are therefore crucial if one aims to use networks to deal with complex policy problems.

Dr. Erik-Hans Klijn is professor at the Department of Public Administration at Erasmus University Rotterdam and visiting professor at the School of Public Policy at the University of Birmingham.

3 SESSION II: PUTTING THEORY INTO PRACTICE

Session II illustrated how network governance has been put into practice. Presentations highlighted the importance of PPPs in today's complex environment and explained ways in which they are being used to address contemporary security issues, specifically: critical infrastructure protection (CIP), information security, and counter-terrorism. To show the diversity and similarities in perspectives and experience, the CRN invited speakers from the public and private sector as well as intergovernmental. Common themes that emerged in each presentation were that partnerships take time to develop and information sharing is key.

3.1 Public Sector Perspective: Role of PPP in Critical Infrastructure Protection

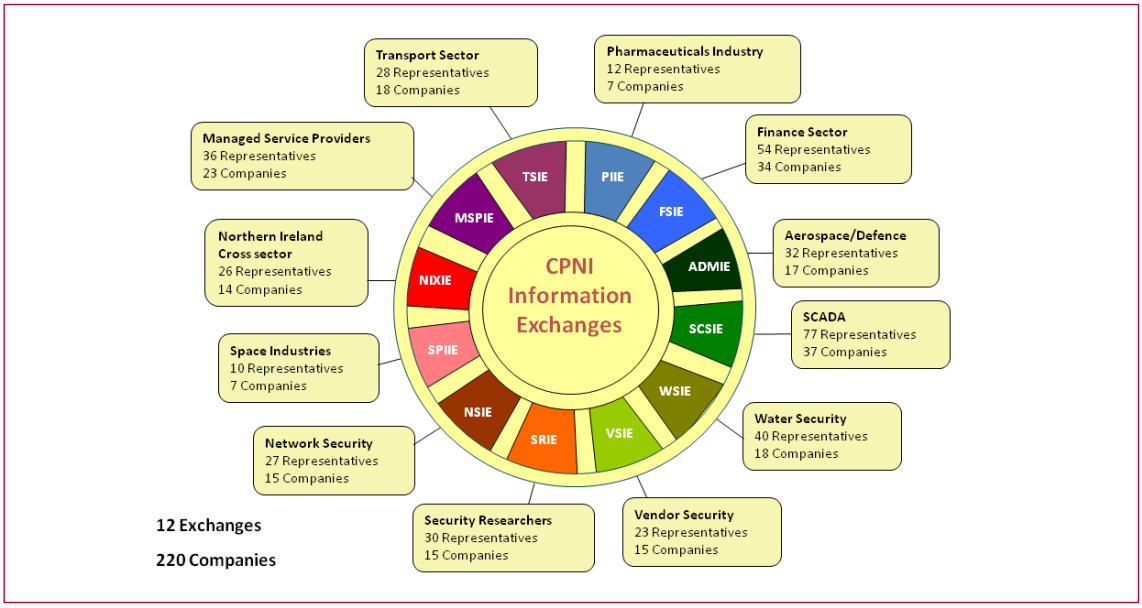
Dr. Andrew Powell, from the United Kingdoms Center for the Protection of National Infrastructure (CPNI), focused on initiatives that CPNI has developed to engage public and private actors and develop tailored partnerships that aim to enhance the protection of CI. The goal of the PPPs is to bring stakeholders together to build relationships and share information.

The CPNI Information Exchanges, as illustrated, were launched in 2003 and modeled after the US Network Security Information Exchange. Today, there are 12 sector-specific exchanges with 220 participating companies. Through these PPP platforms, the UK aims to communicate:

- Risks and mitigation
- Private sector-to-private sector security incident and vulnerability information
- Private sector-to-public sector confidential incident and vulnerability reporting where public sector can respond and warn
  - Public sector issued good practices and incident and vulnerability alerts
  - Has to be relevant to the UK's Critical Infrastructure Protection (CIP)
  - Based on partnership with private sector

In addition to the Information Exchanges, CPNI has also developed: Information sharing portals; Warning, advice and reporting points (http://www.warp.gov.uk) and; Provides support for international groups

CPNI Information Exchanges (extracted from Powells' presentation)



and projects. However, Dr. Powell acknowledged that information sharing does not come easily. To have effective sharing occur, there must be a level of trust and information sharing protocol. In the former, CPNI has found that members build trust over time through regular contact, ensuring that confidentiality is honored, and providing information on a regular basis. He noted that it takes roughly two years for a group to develop a good level of trust. Furthermore, members are active in the selection of new members. In the latter, members are encouraged to share information, which can occur through a shared area on an extranet or during meetings. Dr. Powell spoke about cases where members were dismissed from the partnership if they did not contribute information, participate in activities, and/or follow the rules of membership. In terms of the overall structure, he noted that the Information Exchanges are:

- Free and organizations can send 2 members
- Private sector and public sector co-chairs
- CPNI main coordinator and host of meetings
- Meetings are face-to-face and further supported by email and members only extranet web pages
- Some information exchanges have working groups which develop good practice
- Members have access to CPNI security advice documents

Reflecting on the overall initiative and effectiveness of the UK Information Exchanges, Dr. Powell stated that CPNI has found that exchanges must be kept small in numbers as this helps build and maintain trust. Large groups disrupt the balance and can actually breed mistrust. Furthermore, meetings must be face-to-face and supported by messaging standard. He also noted that not only can membership changes hinder progress made in trust-building but also non-contribution, referred to as "lurking", can undermine trust as members question the motives of member not providing information and/or engaging in the process.

Overall he noted that in the future three areas needed to be addressed within the Information Exchange initiative and PPPs in general: scalability, legal and regulatory changes, and finding a balance between need-to-know and need-to-share. First, scalability would involve federated information sharing structures, developing a group of all information exchanges, and creating the tools for groups to be supported by the use of a common messaging system. Second, he noted the need to agree on a system of internal need-to-know controls so that law makers and regulators can be aware of problems without penalising honest participants. Third, to achieve greater balance of information he suggested educating participants on what information should only be shared within their respective company and what information could be provided on organizational intranets.

Dr. Andrew Powell is the Manager of advice delivery to the communications, emergency services and health sectors at the Centre for the Protection of National Infrastructure (CPNI), United Kingdom

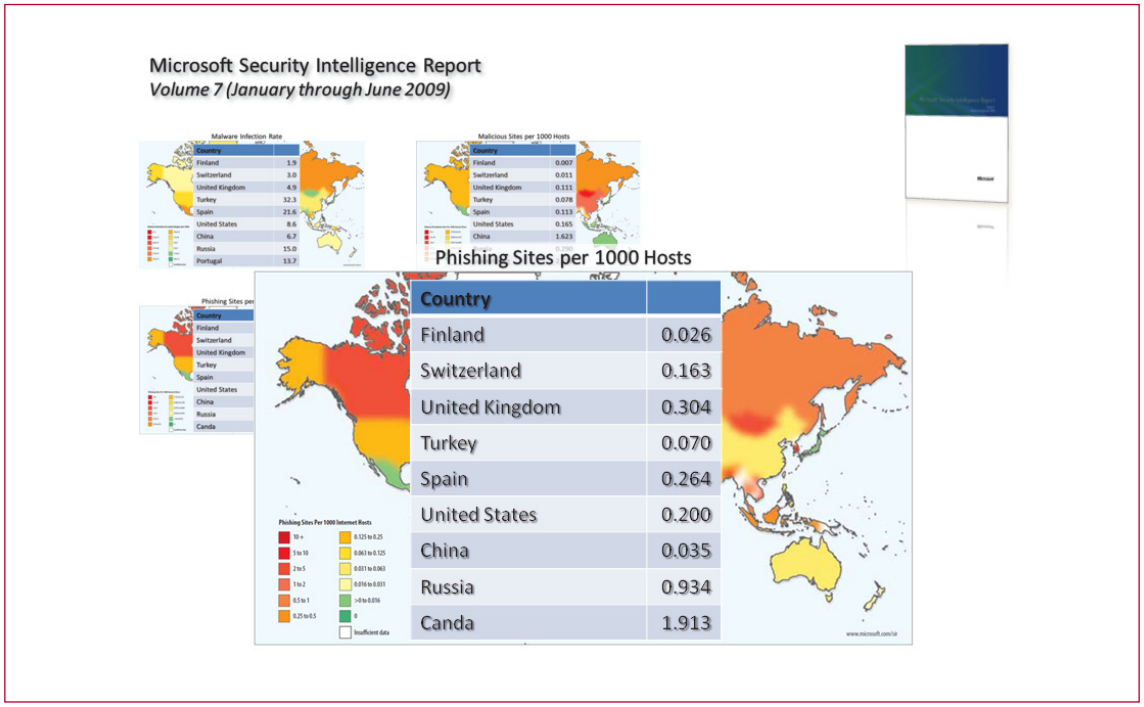
3.2 Private Sector Perspective: Role of PPP in Information Security

Roger Halbheer provided a presentation that discussed the importance of PPPs in the area of information security and, in doing so, focused on the role that the private sector plays. To illustrate the role of the private sector, he outlined the factors that should be taken into account when developing a cybersecurity agenda. They are:

- Your Threat Landscape
- Public Sector Best Practices
- Next Generation Government
- Your External Studies
- Your Government's Agenda

Within this, he highlighted how the private sector shares an interest with the public sector in maintaining the robustness of the infrastructure of information systems. He also added, that as a major company in the information technology domain, Microsoft can work with governments to provide information on security breaches it has found in its operating systems. The Microsoft Security Intelligence Report is an example of the information that Microsoft can provide. This report highlights global trends in malware infection rates as well as malicious and phishing sites. For more private information exchanges, Microsoft has also launched initiatives to share vulnerability information with governments that seek to ensure the protection of national information infrastructure. Mr. Halbheer also highlighted information provided by other bodies, such as "the Global Information Technology Report" which is a product provided by the

Microsoft Security Intelligence Report
Volume 7 (January through June 2009)



World Economic Forum & INSEAD that offers a way to illustrate how networked the world is by providing the network readiness index.

Reflecting on challenges, he first emphasized the difficulty that comes with achieving collaboration and coordination between stakeholders on an issue that has multiple themes. Due to the ubiquitous nature of information technology in today's society, he mentioned various areas where cybersecurity concerns are present – ranging CIP to other domains such as military & intelligence, rights to privacy, and emergency response, amongst others. With this, he recommended that governments need to adopt a more holistic view and improve external and internal coordination in order to enhance the security of complex information systems. This makes PPPs extremely important as platforms used to develop relationships, build trust, and coordinate security measures.

Roger Halbheer is the Chief Security Advisor for Microsoft in Europe, the Middle East and Africa (EMEA)

3.3 Inter-Governmental Perspective: Role of PPP in Countering Terrorism

To illustrate how inter-governmental organizations are using PPPs to counter terrorism, Mehdi Knani explained how the Action against Terrorism (ATU) at the Organization for the Security and Co-operation in Europe (OSCE) was established in 2002 to serve as the co-ordinating and facilitating body for OSCE initiatives and capacity-building programmes in combating terrorism. He highlighted a number of the projects that the ATU has been involved in, namely:

- *Working to strengthen the international legal framework against terrorism* – This is accomplished by working with various organizations to organize national and sub-regional workshops on the ratification of antiterrorism conventions and protocols.
- *Working on matters to address criminal matters* – The ATU works with the United Nations Office for Drug and Crime to host training workshops on international co-operation in criminal matters related to terrorism. Such activities bring

public and private actors together to address issues such as mutual legal assistance and extradition, as well as promoting a European legal framework related to terrorism and co-operation in criminal matters, and encouraging the broader use of technical assistance

- *Combating terrorist use of the Internet* – ATU identifies emerging trends as well as potential counter-measures.
- *Promoting public-private partnerships (PPPs)* – This is done by bringing together state authorities, the business sector and civil society in most of its counter-terrorism activities.

Focusing on ATUs effort to examine PPPs utility, Mr. Knani highlighted a 2007 high-level political PPP conference which explored the potential of such co-operation and identified existing gaps and best practices. He also reflected on recent efforts to bring together diverse stakeholders to address the protection of critical energy infrastructure from terrorist activity. While such efforts have rendered some positive results, they do not come without challenges. He noted how coordinating meetings and getting stakeholders engaged on issues take time, especially in the international arena. However, the ATU has also created a web-based Counter-Terrorism Network (CTN) to further strengthen efforts and build relationships.

Mehdi Knani is the Program Officer for the Action against Terrorism Unit (ATU) at the Organization for Security and Co-operation in Europe (OSCE)

4 SESSION III: CONCLUDING PANEL

The final session brought the five speakers together to discuss theoretical and practical observations. Many in the audience observed gaining a better understanding of network governance and the role that PPPs play in particular. In terms of challenges with PPPs, the issue of trust re-emerged as a point of interest and debate. Panelists and participants alike discussed *how much trust* was necessary for PPPs to be successful and whether trust is truly an essential component. Reflections toggled between absolutely essential to debatable. Dr. Powell referenced the issue of opportunistic behavior, which Dr. Klijn also addressed, as issues that can emerge and negatively affect a network and disrupt its balance. To address this, a network manager must work with the members to decide a course of action that could involve removing members that are not contributing. Though disruptive, such experiences can also build relationships in a network and actually reinforce trust between those that are committed to sustaining the network.

Dr. Kenis referenced academic studies that have examined the characteristics of successful and failed PPPs. He noted that those that have been successful were formed organically rather than through mandate. In other words there needs to be some type of individual and group interest for a network to operate at its fullest potential. Comments were also made regarding the cycle of partnerships to experience high and low points. Dr. Powell chimed in that both sectors must realize that both have shared interests and resources to offer when it comes to ensuring the protection of national infrastructure, for example.
The panel concluded with final reflections that emphasized keeping partnerships small and ensuring that customization is possible.

5 ROUNDTABLE PROGRAM AND PARTICIPANT LIST

5.1 Agenda

08:30	Arrival of participants / Coffee & Tea
09:10 - 09:20	Opening of the 6th CRN Zurich Roundtable
09:20 - 09:30	Introduction
Session I:	**"Network Governance: Theoretical Considerations"**
09:30 - 10:30	"Introduction to the Network Governance Approach"
	Prof. Dr. Patrick Kenis, Academic Dean of TiasNimbas Business School Professor of Policy and Organization Studies
	+ Moderator for discussion
10:30 – 11:00	Coffee Break
11:00 – 12:00	"The challenges of network management: coordinating, mediating and building trust in networks" Prof. Dr. Erik-Hans Klijn, Department of Public Administration at Erasmus University Rotterdam and visiting professor at the School of Public Policy at the University of Birmingham
	+ Moderator for discussion
12:15 – 13:45	Lunch Break: Dozentenfoyer, ETH Zentrum Hauptgebäude
Session II:	**"Putting Theory into Practice"**
14:00 - 15:30	Andrew Powell, Center for the Protection of National Infrastructure, UK
	"Trusted Information Sharing in the UK"
	Mehdi Knani, Programme Officer, Organization for Security and Co-operation in Europe (OSCE) Action against Terrorism Unit (ATU)
	Roger Halbheer, Chief Security Advisor for Microsoft Europe, the Middle East and Africa (EMEA) "Why Public Private Partnerships are essential"
15:30 – 16:00	Coffee Break
16:00 – 17:00	Collaborative Panel: All invited speakers will sit on a moderated panel to discuss theoretical and practical positions.
17:00 - 17:10	Conclusion and final remarks followed by snacks and drinks

4.2 List of Participants

Name	Email	Organization
Walter Ammann	info@grforum.org	Global Risk Forum
Corinne Bara-Zurfluh	corinne_kalimpong@yahoo.com	EDA: CH Government
Jörg Berlinger	joerg.berlinger@risiko-dialog.ch	Risk Dialogue Foundation
Christoph Bleiker	bleiker@sipo.gess.ethz.ch	Center for Security Studies, ETH
Stefan Brem	stebrem@gmail.com	BABS: CH Government
Elgin Brunner	brunner@sipo.gess.ethz.ch	Center for Security Studies, ETH
Christoph Doktor	doktor@sipo.gess.ethz.ch	Center for Security Studies, ETH
Serge Droz	serge.droz@switch.ch	SWITCH
Myriam Dunn	dunn@sipo.gess.ethz.ch	Center for Security Studies, ETH
Jennifer Giroux	giroux@sipo.gess.ethz.ch	Center for Security Studies, ETH
Roger Halbheer	Roger.Halbheer@microsoft.com	Microsoft
Kai Jensen-Kusk	kai.jensen-kusk@db.com	Deutsche Bank
Prof. Dr. Patrick Kenis (Speaker)	p.kenis@uvt.nl	Tilburg University
Prof. Dr. Erik-Hans Klijn (Speaker)	klijn@fsw.eur.nl	Erasmus University Rotterdam, Department of Public Administration
Matthias Klopfstein	matthias.klopfstein@gs-vbs.admin.ch	FED-POL: CH Government
Mehdi Knani (Speaker)	mehdi.knani@osce.org	OSCE Action Against Terrorism Unit
Andrew Powell (Speaker)	andrewp@cpni.gsi.gov.uk	The UK Centre for the Protection of National Infrastructure (CPNI)
Maria Sedova	MSedova@TRAXINTL.COM	TRAX International
Malin Samuelsson	malin.samuelsson@irgc.org	International Risk Governance Council
Bianca Sarbu	Sarbu@sipo.gess.ethz.ch	Center for Security Studies, ETH
Gagik Sargsyan	gagik.sargsyan@hsbcpb.com	HSBC Private Bank (Suisse) SA
Jan Störger	storger@sipo.gess.ethz.ch	ISN, Center for Security Studies, ETH
Manuel Suter	suter@sipo.gess.ethz.ch	Center for Security Studies, ETH
Parisa Tabriz	parisa@google.com	Google

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.

The **Crisis and Risk Network (CRN)** is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness. As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)