

# Critical Infrastructure Protection: The Challenge of Establishing Interagency Cooperation

Prof. Todor Tagarev

## Event

- ▶ International Expert Meeting on Critical Infrastructure Protection in Ukraine
- ▶ 15–16 October 2015, Kyiv
- ▶ National Institute for Strategic Studies
- ▶ Supported by the NATO Liaison Office

## Todor Tagarev

- ▶ Professor at the Institute of ICT, Bulgarian Academy of Sciences, and Head of the Centre for Security and Defence Management, [www.IT4Sec.org](http://www.IT4Sec.org)
- ▶ DCAF Associate Senior Fellow, Defence Management, [www.dcaf.ch](http://www.dcaf.ch)
- ▶ Governmental experience: defence planning, defence investments policy, leadership positions

## Outline

- ▶ CIP context and requirements
- ▶ Levels of 'Cooperation'
- ▶ Operational coordination
- ▶ Development of measures and capabilities

all with critical account of the experience of Bulgaria

## Context

- ▶ Multiple hazards
  - Threats – military & ‘civilian’
  - Negligence
  - Technical faults
  - Natural disasters
- ▶ Diverse scenarios
- ▶ ... do not fit in the remit of one, or a few, existing security agencies
- ▶ Cascading effects, i.e. an attack or malfunction of an ‘asset’ in one sector may have consequences (possibly unintended/ unexpected) across sectors and borders

## Requirements

- ▶ Within a ‘risk management’ decision-making framework
- ▶ Defining the scope of threats and challenges to be accounted for (e.g. war or ‘war-like’ situation)
- ▶ Assess likelihood and ‘total’ consequences
- ▶ Devise and implement measures & capabilities to minimise risk
- ▶ Several governmental agencies, local authorities, private sector, non-governmental, cross-border actors, international players

## Levels of 'cooperation'

- ▶ Central agency
- ▶ Collaboration in capability development, e.g. joint procurement, training centres, LL
- ▶ Coordinated capability development (incl. coordinated decisions on investment)
- ▶ Joined operational plans in place, exchange of lessons learned
- ▶ Multiagency training & exercises
- ▶ Established lines of communication
- ▶ Ad-hoc cooperation on urgent matters
- ▶ Organisational rivalry

## C3: Cooperation, Coordination, Collaboration

- ▶ Cooperation (As needed – *ad hoc*, informal relationships, no joint planning, authority and accountability rest with individual organisations)
- ▶ Coordination
  - reviewing missions and goals for compatibility
  - interaction around specific projects or tasks
  - established channels of communication
  - some sharing of leadership and control
  - most authority and accountability still rest with individual organisations
  - resources can be made available for a specific project

## C3: ... Collaboration

- ▶ defining new, common missions and goals
- ▶ projects, undertaken for long-term results
- ▶ new structure and/or formal division of labour are created
- ▶ comprehensive planning is required
- ▶ many levels of communication and channels for interaction
- ▶ leadership is dispersed and control is shared and mutual
- ▶ Resources are pooled or jointly secured for a long-term effort

## Operational vs Development coordination

- ▶ Operational coordination – how to act jointly when a need arises, who does what
- ▶ Development coordination – how to allocate resources, i.e. which organisation what measures implements and what capabilities develops and maintains
- ▶ [two well established disciplines in the military: “operations planning” and “defence/force planning”]

## Operational coordination

- ▶ 2005 and follow-up studies, Green Paper; Law on Crisis Management; Ministry of Emergencies
- ▶ 2008 – Directive 114
- ▶ 2010 – transposition of Directive 114:
  - Reorganisation; The CM Law revoked
  - POC – MOI GD “Fire Safety and Civil Protection”
- ▶ Specific circumstances
  - Political influence; strengthening the “Unified Rescue System”; lack of interest by sectoral ministries
- ▶ 2012–... “Security Council” to the Council of Ministers, with a “Situation Centre”

## Coordination in investments / capability development

- ▶ Lack of understanding of the concept
- ▶ Disaster Management Act
- ▶ 2012–... “Law on the System for Protection of National Security”
  - Expanding the role of the security “Security Council”
  - In the final version – rather small steps beyond the operational coordination via the “Situation Centre”
- ▶ Key issue: Who finances the necessary measures & capabilities for CIP
  - DM Act provides for, but in practice only symbolic amounts are spent on ‘prevention’ (see Hyogo/Sendai Framework for Action)

## Examples of good practice

- ▶ Examples from the experience of other countries and similar fields, e.g. counter-terrorism, cybersecurity
- ▶ Information fusion centres (shared situational awareness)
- ▶ Joint Terrorism Task Forces
- ▶ Multi-stakeholder exercises
- ▶ International cooperation (good practice, benchmarking, standards, etc.)

## Remaining challenges

- ▶ All-hazards, comprehensive approach
- ▶ Agreeing what that means, i.e. defining the scope of 'critical infrastructure' & CIP
- ▶ Joint risk assessment
- ▶ Balancing investments in prevention, protection, reaction, resilience
- ▶ Characteristics of decision-making:
  - Limited rationality
  - 'Prospect' considerations, i.e. personal and political gains and losses
  - Groupthink, i.e. importance of loyalty to real or perceived group norms
  - Competition among the actors

## Overall examination

<i>Looking for a solution</i>	
Top-down	Bottom-up
<i>Who bears the cost</i>	
Public	Owner/Operator (private)
<i>Initiation</i>	
Local	Outside
<i>Overall organisation</i>	
Specialised	Within an existent CM framework
<i>Coordination</i>	
Operational	Development

## The experience of Bulgaria

<i>Looking for a solution</i>	
<b>Top-down</b>	Bottom-up
<i>Who bears the cost</i>	
Public	<b>Owner/Operator (private)</b>
<i>Initiation</i>	
Local	<b>Outside</b>
<i>Overall organisation</i>	
Specialised	<b>Within an existent CM framework</b>
<i>Coordination</i>	
<b>Operational</b>	Development



## Commissioner N. Nikolov, Director, GD “FSCP”, 11 Sep 2015

- ▶ ... Legal requirements and the ways critical infrastructures are defined do not allow to create clear policies for critical infrastructure protection.
- ▶ ... We need a new concept for defining critical infrastructures and their sectors and assets in order to provide continuity in providing essential products and services.
- ▶ ... There is no state policy for stimulating private insurance against disasters.

## Conclusion

- ▶ Bottom-up approaches might be beneficial
- ▶ Tools:
  - Exchange of experience
  - Testing interoperability
  - Joint, multi-agency, multi-stakeholder training and exercises
  - Benchmarking
  - Free flows of information and knowledge & continuous learning
- ▶ Proof of concept; developing a culture of cooperation

## References

1. Tagarev, Todor, and Nikolay Pavlov. "Planning Measures and Capabilities for Protection of Critical Infrastructures." *Information & Security: An International Journal* 22 (2007): 38–48.  
<http://dx.doi.org/10.11610/isij.2205>
2. Tagarev, Todor. "Capabilities-based Planning for Security Sector Transformation." *Information & Security: An International Journal* 24 (2009): 27–35.  
<http://dx.doi.org/10.11610/isij.2404>.

3. Prezelj, Iztok, and Joe Airey. "Interagency Cooperation in Counter-Terrorism." In *Combating Transnational Terrorism*, edited by James K. Wither and Sam Mullins, 237–253. Sofia: Procon, 2016.
4. Prezelj, Iztok. "Comprehensive Security and Some Implemental Limits." *Information & Security: An International Journal* 33 (2015): 11–32.  
<http://dx.doi.org/10.11610/isij.3301>.