SEC.GAL/155/10
13 September 2010

ENGLISH only

osce.org

OSCE Action against Terrorism Unit

Critical Energy Infrastructure Protection from Terrorist Attacks




OSCE Organization for Security and Co-operation in Europe

The OSCE Action against Terrorism Unit

DECISION No. 6/07 on Protecting Critical Energy Infrastructure from Terrorist Attack

Herein OSCE participating States decided:

- **to consider all necessary measures at the national level to ensure an adequate protection of critical energy infrastructure from terrorist attack;**
- **to continue co-operation amongst them and to better co-ordinate measures to increase protection of critical energy infrastructure from terrorist attack;**
- **to develop public-private cooperation to protect critical energy infrastructure.**

OSCE Organization for Security and Co-operation in Europe

2

The terrorist threat to CEI is a reality

- CEI are vulnerable – *factors: complexity, interdependencies, underinvestment*
- CEI are attractive targets for terrorists – *factors: dependence on energy, impact amplified systemically*
- Increased targeting of energy infrastructure by violent non-state actors over the years
- Cyber security as one of the main challenges

OSCE Organization for Security and Co-operation in Europe

3

What has been done?

- *2008 ATU/OCEEA Expert Meeting on Protecting Critical Energy Infrastructure from Terrorist Attacks*
- *2010 Public-Private Expert Workshop on Protecting Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks*
- *2010 Special CTN Bulletin on Critical Energy Infrastructure Protection from Terrorist Attacks*

OSCE Organization for Security and Co-operation in Europe

4

CEIP should be all-hazard, comprehensive but tailored

❖ Protection should be:

➢ based on holistic risk assessment, taking into account interactions between different levels and interdependencies between sectors.

➢ designed to mitigate against series of hazards, whether natural, technological or manmade;

➢ tailored to particular infrastructure and scalable.

More emphasis on resilience …

➢ Preparedness and recovery capabilities are key because disruptions cannot be completely ruled out

➢ Early warning/alert systems, contingency planning, communications plans, testing and exercising, specialized agencies with rapid deployment capabilities

➢ Building up resilience and energy reliability is not only about infrastructure

Drawing on Public-Private Partnerships (PPPs)

- State authorities cannot counter terrorism alone; they need to draw on businesses and civil society;
- Voluntary, mutual benefits and trust as critical enabler;
- Create trustworthy environment for information-exchange on risks and vulnerabilities to improve situational awareness and allow for early warning and scalable security;
- Engage to define adequate regulations providing a level playing field, while encouraging additional voluntary measures as part of business continuity management;
- Promote the exchange of good practices;
- Tap into potential for community-based security;

The way ahead …

- **ATU can organize national/sub-regional CEIP workshops/simulations/trainings**
- **ATU is developing a pilot project on PPP for CEIP with United Nations Interregional Crime and Justice Research Institute (UNICRI)**
- **ATU can compile a handbook on non-nuclear CEIP good practices**
- **ATU can facilitate capacity-building on cyber security**

OSCE Action against Terrorism Unit

Thank you for your attention!

For more information please contact:

Reinhard.Uhrig@osce.org