

osce.org

TNTD/ATU

21ST OSCE ECONOMIC AND ENVIRONMENTAL FORUM
“Increasing stability and security: Improving the environmental footprint of energy-related activities in the OSCE region”

CONCLUDING MEETING
Prague, 11 – 13 September 2013

Session I: OSCE Guidebook on Critical Infrastructure Protection

Address by Mr. Thomas Wuchte
Head/Action against Terrorism Unit
Transnational Threats Department
OSCE



TNTD ATU
osce.org

21ST OSCE ECONOMIC AND ENVIRONMENTAL FORUM
Prague, 11 – 13 September 2013

- Outline of the importance of energy infrastructure security in general and in the OSCE framework, in particular.
- Overview of the OSCE Ministerial Council Decision on Protecting Critical Energy Infrastructure from Terrorist Attack.
- Overview of OSCE efforts to protect critical infrastructure.
- Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace.

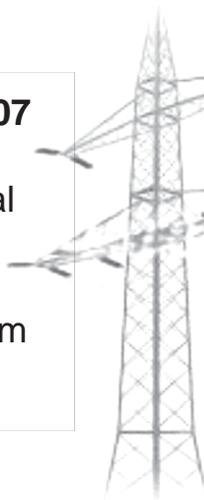
There can be no argument against
closer collaboration...



Vulnerable Critical Energy Infrastructure

Decision No. 6/07

Protecting Critical
Energy
Infrastructure from
Terrorist Attack



- Nuclear power-plants
- Dams of hydroelectric power plants
- Oil and gas producers
- Refineries
- Transmission facilities
- Supply routes & facilities
- Energy storage
- Hazardous waste storage facilities

It is visionary to turn words into action,
and to turn action into partnership



OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP)

Good Practices Guide
on Non-Nuclear Critical Energy
Infrastructure Protection (NNCEIP)
from Terrorist Attacks
Focusing on Threats Emanating
from Cyberspace



- **Cyber-related Terrorist Attacks on Non-Nuclear Critical Energy Infrastructure**
- **Good Practices in ICT Risk Management Frameworks to Address Cyber-related Terrorist Risks**
- **Good Practices In ICT-related Security Measures to Address Cyber-related Terrorist Risks**
- **Good Practices in CIP within the OSCE**
- **Suggestions for Future OSCE Roles to Advance Cyber Security in Non-Nuclear Critical Energy Infrastructure**

Table of Contents

Foreword	7
Acknowledgements	8
Executive Summary	11
Cyber-related Terrorist Attacks on Non-Nuclear Critical Energy Infrastructure	15
2.1 Critical Infrastructure	16
2.2 Non-Nuclear Critical Energy Infrastructure	19
2.3 Cyber-related Terrorist Threats to Non-Nuclear Critical Energy Infrastructure	22
2.4 Potential IT-based Terrorist Attacks on Non-Nuclear Critical Energy Infrastructure	26
2.5 Summary and Recommendations	28
Good Practices in ICT Risk Management Frameworks to Address Cyber-related Terrorist Risks	31
3.1 Role and Relevance of ICT in the Energy Sector	32
3.2 Potential Vulnerabilities in ICT	35
3.3 ICT-related Risk Management Frameworks for Non-Nuclear Critical Energy Infrastructure	37
3.3.1 Principles of Risk Management	37
3.3.2 Main Elements of the ISO/IEC 27000 series	40
3.3.3 Risk Management Approaches for Energy Infrastructure	40
3.4 Summary and Recommendations	43
Good Practices in ICT-related Security Measures to Address Cyber-related Terrorist Risks	47
4.1 Addressing ICT-related Standards	48
4.2 Creating National Cyber Security Strategies	50
4.2.1 EU Nations	51
4.2.2 Non-EU Nations	53
4.2.3 Policy Recommendations for Cyber Security	54
4.2.4 Policy Recommendations for "Smart Grid" Cyber Security	55
4.3 Implementing a Risk-based Security Management Framework	55

Conclusion

Solution

PPP public private partnership

“Partnership of State Authorities, Civil Society and the Business Community in Combating Terrorism”

Oriented

Mr. Thomas Wuchte

OSCE/Anti-Terrorism Issues

Head on Anti-Terrorism Issues

Wallnerstrasse 6

1010 Vienna, Austria

Tel.: +431514366710

Mail: Thomas.Wuchte@osce.org