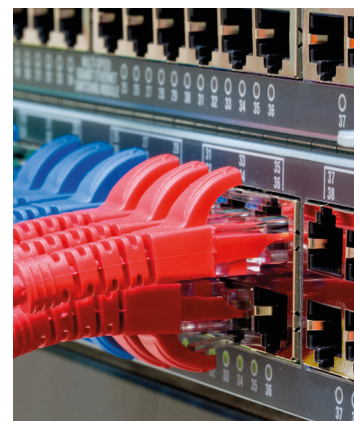



Good Practices Guide
on Non-Nuclear Critical Energy
Infrastructure Protection (NNCEIP)
from Terrorist Attacks
Focusing on Threats Emanating
from Cyberspace





The Guide raises awareness of the significance of non-nuclear critical energy infrastructure and the extent to which it is threatened by cyber-related terrorist attacks and other types of potential threats. It identifies key policy issues and challenges and presents good practices as possible solutions for government policy makers, state authorities in charge of critical infrastructure protection, owners and operators as well as other stakeholders.

Introduction

Protecting critical energy infrastructure from terrorist attacks is an issue particularly relevant for the OSCE, whose 57 participating States and 11 Partners for Co-operation include some of the largest producers and consumers of energy as well as many strategic transit countries. The importance of energy security and energy infrastructure cannot be overstated. Since critical energy infrastructure contains the fuel that keeps the global economy moving and our societies working, our dependency on such infrastructure makes it an ideal target for terrorists.

The Guide raises awareness of the significance of non-nuclear critical energy infrastructure and the extent to which it is threatened by cyber-related terrorist attacks and other types of potential threats. It identifies key policy issues and challenges and presents good practices as possible solutions.

The Guide encourages the adoption of appropriate policies and institutional arrangements to ensure cyber security of non-nuclear critical energy infrastructure, based on a co-operative, integrated (all hazard) and risk-based approach. It promotes national and international co-operation and information exchange between public agencies and owners and operators of this infrastructure to face the threat of cyber-attacks.

Target audience

The Good Practices Guide serves as a reference document containing key information for

- government policy makers,
- state authorities in charge of critical infrastructure protection,
- owners and operators of non-nuclear critical energy infrastructure and
- other stakeholders in the OSCE area.

Content

This guide describes the significance of non-nuclear critical energy infrastructure (NNCEI) for countries and energy consumers and identifies threats to that infrastructure, focusing on cyber-related terrorist attacks. It highlights methodological issues that need to be taken into account for the protection of non-nuclear critical energy infrastructure and offers suggestions for good practices to mitigate potential vulnerabilities.

Based on the findings, a number of recommended good practices for all countries and companies operating non-nuclear critical energy infrastructure include:

1. Raising awareness of the significance of non-nuclear critical energy infrastructure and the extent to which it is threatened by cyber-related terrorist attacks, as well as other types of potential threats;
2. Promoting national and international cooperation between public agencies and owners and operators of non-nuclear critical energy infrastructure to face the threat of cyber attacks;
3. Facilitating information exchange between public agencies and the operators of non-nuclear critical energy infrastructure regarding ways of dealing with the threat of cyber attacks; and
4. Using existing national and international forums and, if appropriate, creating standardized national and international forums and frameworks for addressing cyber-related terrorist attacks on non-nuclear critical energy infrastructure to consider co-ordinated measures, such as raising awareness, outreach and partnering with industry, and where appropriate, implementing adequate regulations.

Although the aim of good practices presented here is to assist countries with identifying and countering threats to cyber-related terrorist attacks, these measures may be adapted, extended and/or applied to other threats and other sectors. This possibility is taken into account throughout the guide.

The Guide includes the following chapters:

1. Executive Summary
2. Cyber-related Terrorist Attacks on Non-Nuclear Critical Energy Infrastructure
3. Good Practices in Information and Communication Technology (ICT) Risk Management Frameworks to Address Cyber-related Terrorist Risks.
4. Good Practices In ICT-related Security Measures to Address Cyber-related Terrorist Risks.
5. Good Practices in Critical Infrastructure Protection within the OSCE.
6. Suggestions for Future OSCE Roles to Advance Cyber Security in Non-Nuclear Critical Energy Infrastructure.

Each chapter offers a “Summary and Recommendations” and the Guide gives a list of suggested reading.

Accessing the Good Practices Guide on NNCEIP

E-copies are available in pdf format online:

<http://www.osce.org/atu>

The Guide will be available also in Russian soon.

The Organization for Security and Co-operation in Europe works for stability, prosperity and democracy in 57 States through political dialogue about shared values and through practical work that makes a lasting difference