Critical Infrastructure Protection: new dimension of the security policy of Ukraine

Dmytro Biriukov
Head of Sector,
Energy and Technological Security Department, NISS
Critical Infrastructure Protection as a policy issue

CIP is an issue of:
• Economic (business continuity and far beyond)
• Foreign affairs
• Social stability
• Law enforcement
• Environmental security
• Technology
• …

considered on:
• corporation,
• professional society,
• general society,
• …
• national,
• and international levels.

When implementing measures (legislative, organizational, low enforcement, technological, engineering etc)

When discussing CI related issues
Critical Infrastructure Protection – essential points

- To ensure CI security and resilience under legislative norms of the peacetime
- Analyze, estimate and mitigate threats keeping in mind national security
- Involve all stakeholders to build balance of interests (“state – society– business”)

- Although we consider 10 sectors of CI as a priority sectors, the energy sector is of utmost significance

There is a lack of comprehensive mechanism to prevent and manage crisis situations related to CI functions in Ukraine
### CIP in Ukraine – fragmented system

**Primary criterion**

<table>
<thead>
<tr>
<th>Enterprises that are of strategic importance to the economy and national security</th>
<th>Objects that have to be obligatory protected on the basis of contracts by the State Guard Service</th>
<th>Facilities that are included in the State register of potentially dangerous objects and Objects of high danger</th>
<th>Objects that have to be protected and defensed during emergency situations and the special period</th>
<th>Objects that belong to categories of civil protection</th>
<th>Oil and gas industry facilities of highest importance / Energy facilities of highest importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic and social value, significance for defense industry</td>
<td>composed from categories a,c,g,h (on previous page)</td>
<td>Presence of hazardous materials, explosives, etc.</td>
<td>Preparation of territories for emergencies and defense</td>
<td>Preparation of territories for defense</td>
<td>Control points, large capacities of fuel storage</td>
</tr>
</tbody>
</table>

**Primary risks**

<table>
<thead>
<tr>
<th>Loss of control over the strategic enterprise (technologies)</th>
<th>Intrusion, sabotage, heist, hijacking</th>
<th>Depreciation of production assets, equipment failures</th>
<th>Inoperability</th>
<th>Inoperability</th>
<th>Intrusion, sabotage, terrorist attack</th>
</tr>
</thead>
</table>

**Primary protection measures**

| Restrictions on privatization | Physical protection | Technological safety inspections | Inspections | Inspections | Physical protection, technological safety inspections |
Toward implementation of CIP in Ukraine

Strategic Vision

Strategic aims of state policy regarding CIP

CIP Objectives

CIP System Development Principles

CIP system functions

Correction of the tasks for CIP subjects

A. Comprehensive improvement of the CIP legal framework

- requires
- completely determined by

C. Strengthening the cooperation among CIP subjects

- requires

B. Strengthening the guard of the objects of critical infrastructure particularly in energy and transport

- based on

F. Development of international cooperation in CIP field

- based on

D. Development and implementation of information exchange mechanisms ... and protection of sensitive information in CIP field

- based on

E. Prevention of industrial accidents and quick and adequate response, localization and minimization of their consequences

- requires
Last year activities

**Legislative proposals**
- draft of the Law on basics for ensuring cyber security (№2126a on 19.06.2015, withdrawn on 02.02.2016), draft of the Law on changes to ... (№2661 on 17.04.2015, being rejected and than withdrawn on 04.06.2015).

**Examining most suitable organizational structures**
- Cabinet of Ministers reestablished State Emergency Commission in Jan 2015

**Performing efforts to identify CI**
- Cabinet of Ministers in Jan 2015 ordered ministries to identify transport facilities, critical infrastructure and public places that require priority protection in a complicated security situation including terrorist threats.
- State Service for Special Communications and Information Protection (3SCIP) was requested to develop Procedure of CII identification and CII list, as well as assessment of the cyber security of state information resources

**Strengthening crisis management**
- The Main Situation Centre was reestablished in the Office of NSDC in Jan 2015
- Ministry of Defense developed Conception of the Development of Situation Centres Network and implementation plan.
Recently approved strategic documents

[1] Security and Defense Sector Development Conception


- Counter-Terrorism
- Civil Protection
- Counter-Intelligence
- Cyber Security
- Physical Protection

CIP

[1] State Service for Emergencies to participate in (a) CIP legislation improvement, (b) ensuring operation of CI under emergency and special period

[1] Security Service counterintelligence protection of CI

[2] Security Service: (a) CII counter-intelligence and (b) investigation

[1] 3SCIP: (a) control functions, (b) ensuring cyber security on CII, (c) conducting audit of CII

[2] defines CII

3SCIP:(a) formation and implementation of state policy, (b) audit of CII

National Bank: requirements for bank sector CII.

[1] to increase capacity of National Guard
EU Directive 2008/114/EC

on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

• constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection

• concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology sector

The primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures
EU Directive 2008/114/EC

Operator security plans (‘OSPs’) or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection and prioritisation of counter measures and procedures should be in place in all designated ECIs.

Security Liaison Officers should be identified for all designated ECIs in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities.

- It is up to each Member State to decide on the most appropriate form of action with regard to
  the establishment of OSPs.
  the designation of Security Liaison Officers.
(14) … Each Member State should collect information concerning ECIs located within its territory. The Commission should receive generic information from the Member States concerning risks, threats and vulnerabilities in sectors where ECIs were identified …

(16) Owners/operators of ECIs should be given access primarily through relevant Member State authorities to best practices and methodologies concerning critical infrastructure protection.

(17) Effective protection of ECIs requires communication, coordination, and cooperation at national and Community level. This is best achieved through the nomination of European critical infrastructure protection contact points (‘ECIP contact points’) in each Member State, who should coordinate European critical infrastructure protection issues internally, as well as with other Member States and the Commission.
<table>
<thead>
<tr>
<th>Strengths</th>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation of NATO and EU recognized approach</td>
<td>Acceleration of the establishment of CIP system in Ukraine</td>
</tr>
<tr>
<td>Demonstration of “good will”</td>
<td>To attract attention on CIP related problems (incl. transport sector)</td>
</tr>
<tr>
<td>Implementation of Energy and Transport CI identification</td>
<td>Involvement in CIP assessment on the EU level</td>
</tr>
<tr>
<td></td>
<td>Wider participation in EU projects</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Weaknesses</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation of the Directive 2008/144 won’t provide any direct instruments from EU for Ukraine to strengthen CIP</td>
<td>Risk related to Ukrainian CI could be overestimated that may result unfounded claims to strengthen security measures</td>
</tr>
<tr>
<td>Separate agreements are needed to access CIWIN, etc.</td>
<td>The reluctance of operators to take additional responsibilities and resistance to legislative proposals</td>
</tr>
<tr>
<td></td>
<td>Leak of sensitive/confidential information</td>
</tr>
</tbody>
</table>
Conclusions

• On this stage we should initialize development of CIP system.

• This could be done by conducting NSDC meeting on CIP issue and approving decision of the NSDC.

• NSDC decision could assign authorities responsible for primary actions to develop CIP system.

• These actions could include drafting of the special law to implement CIP into Ukrainian legislation, specify basics of public-private partnership, define procedure for CIP system development.
Thank you for your kind attention!

I have shared my modest findings, now please don’t hesitate to ask any questions and share your opinions.

Dmytro Biriukov
Head of Sector

Critical Infrastructure and Technological Security Sector, Energy and Technological Security Department, NISS
Tel./fax +38 044 2447936
dmytro.biriukov@niss.gov.ua