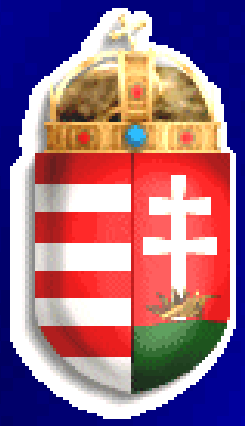


HUNGARIAN (EUROPEAN) EXPERIENCES (BEST PRACTICES) IN TRAINING AND EDUCATION ON CIP

Mihaly Recsei

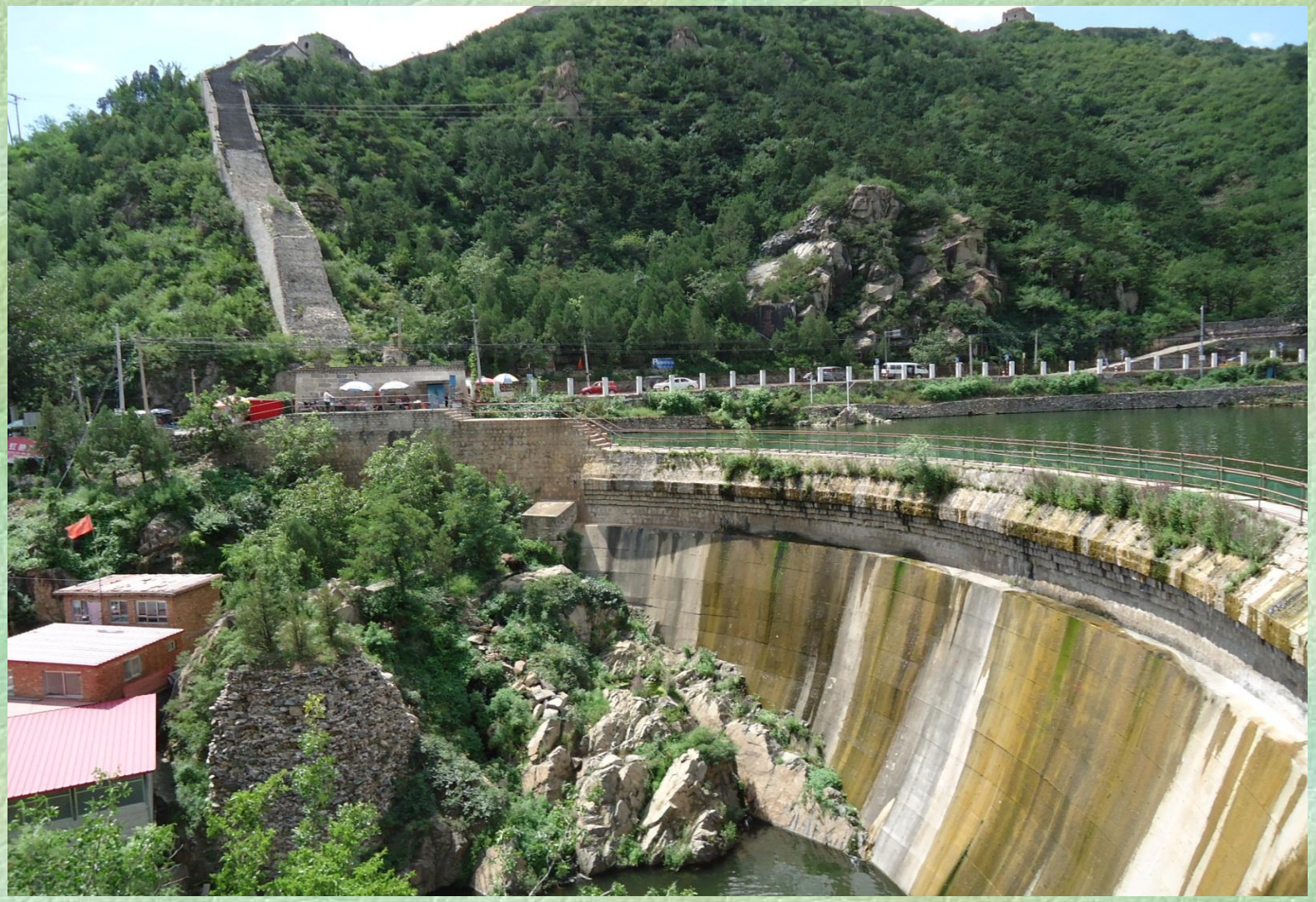
SOME DETAILS ABOUT MYSELF

- 1981-1997 CI officer in several positions within MSO;
- 1997-1998 military observer in UNIKOM;
- 1998 - 2000 head of Department for International Relations;
- 1999 - 2010 member of Hungarian delegation participating in the work of Multinational Industrial Security Working Group (MISWG);
- 2000 - 2003 head of Department of Industrial Security;
- 2003 - 2007 CI officer for colony defense at Hungarian Military Representation to NATO Allied Command Operations (ACO);
- 2005 - 2007 special agent for Allied Command Counterintelligence (ACCI) at ACO;
- 2007 - 2011 deputy head of Personnel and Industrial Security Vetting Directorate;
- 2010 - 2015 external lecturer in National University of Public Service;
- 2012 – 2014 security expert in Hungarian Embassy, China.

Agenda Items

1) EU legal background of CIP
2) EU definition of CIP and introduction of some CIP related organisations
3) Multinational Industrial Security Working Group
4) Power ranking of critical infrastructure sectors
5) Secutity awareness and training of CIP
6) Education specialities and methods of CIP

Critical Infrastructure combined with Great Wall

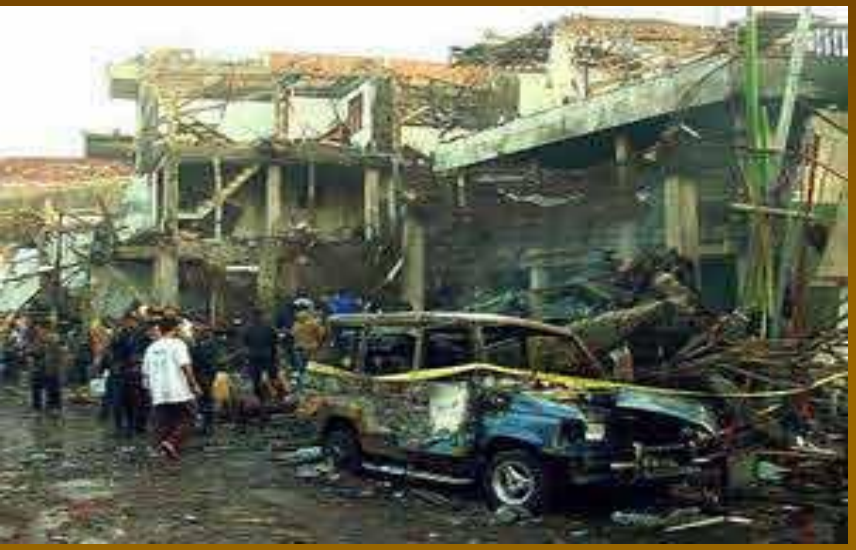


CRTITCAL INFRASTRUCTURE PROTECTION FROM ALL KIND OF THREATS

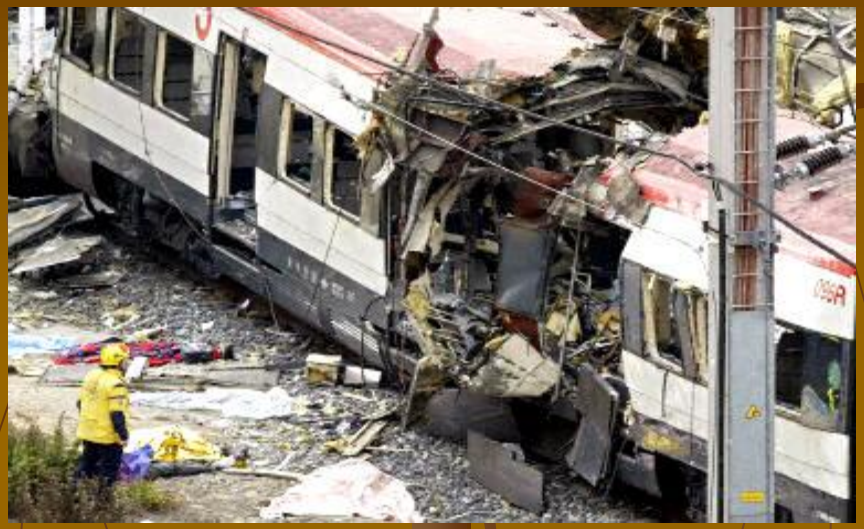
1. Global security challenges summary

Redefinition of Power

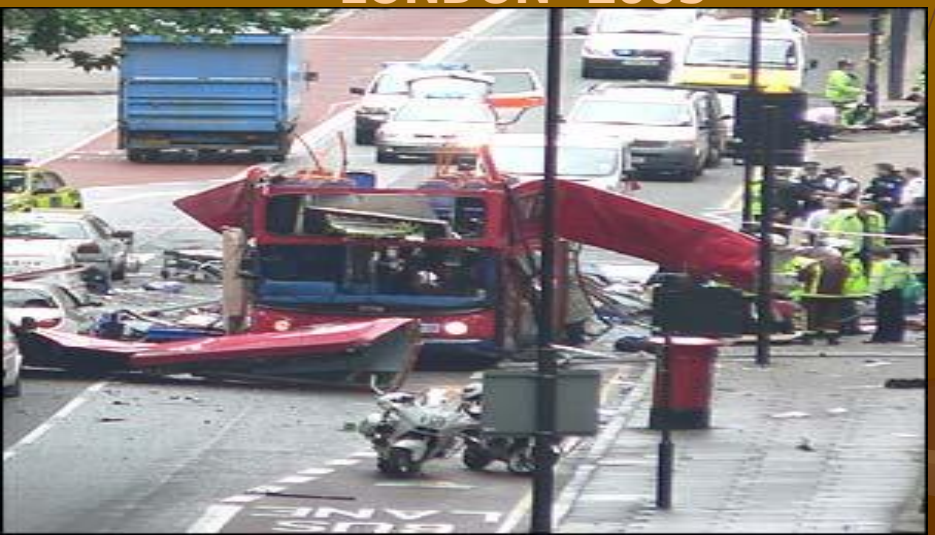
BALI - 2002



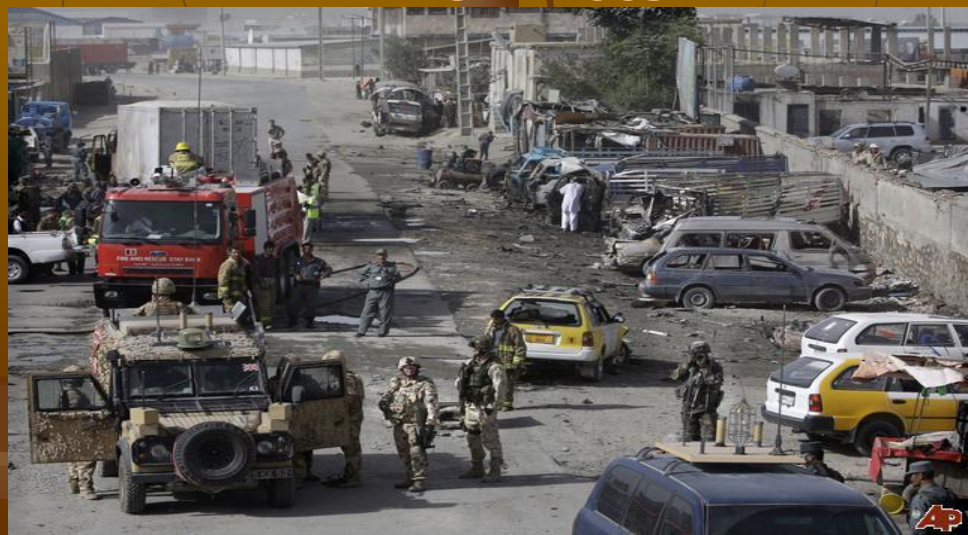
MADRID - 2004



LONDON -2005



KABUL - 2009



THE INTERNATIONAL COOPERATION OF HUNGARY

- Security Agreement with NATO on 5 July 1994.
- Security Agreement with WEU on 1 October 1996.
- Hungary became a NATO member state on 12 March 1999, at the same time we joined to the “Information Security “ agreement of the alliance.
- Security Agreement with EU on 20 March 2003.
- EU membership on 1 May 2004.
- Series of bilateral agreements in protection of classified information were concluded with NATO, EU member nations, with a part of PfP countries and additionally with other nations.

EU LEGAL BACKGROUND OF CIP

- EU COM (2006) 786 (final) document on European Program of Critical Infrastructure Protection;
- Green Paper on European Programme for CIP (COM /2005/576 final);
- Council Directive 2008/114/EC on the Identification European Critical Infrastructure, and Improvement their Protection;
- Council Decision 2001/264/EC Adopting the Council's Security Regulations;
- Commission Decisions 2001/844/EC, ECSC, EURATOM on Security of Classified Information;
- Council Directive 2014/87/EURATOM the Nuclear Safety of Nuclear Installations;

EUROPEAN PROGRAMME FOR CIP

Based on EU COM (2006) 786 (final) document:

- Common Action Plan;
- Critical Infrastructure Warning Information Network (CIWIN).
- CIP Expert Groups on EU level;
- Support for member states concerning national critical infrastructures;
- Contingency planning, external dimensions.

CIP Contact Group was created in order to serve as the strategic coordination and cooperation platform with CIP Contact Points of EU member countries.

CIP RELATED ORGANISATIONS

Society for Risk Analysis – Europe (founded in 1981) aims to bring together individuals and organisations interested in risk assessment, risk management and risk communication in Europe. It developes new methodologies for risk analysis and risk management. Their official journals are „Risk Analysis" and „Risk Research".

The Commission of a Critical Infrastructure Warning Information Network (CIWIN) aims to exchange and discuss CIP related information, good practices in order to mitigate risk across all EU Member States. It provides the platform for the exchange of best practices and rapid alerts in a secure manner.

European Nuclear Education Network (ENEN), located in Paris. Ukraine is the member of this network.

SECURITY LIAISON OFFICER

- *Based on Council Directive 2008/114/EC* Security Liaison Officers have to be acredited to all critical infrastructure facilities. Their main document is Operator Security Plan. Annual report is obligatory about actual threat assessment.
- Each EU member state has European Critical Infrastructure Contact Point (in Hungary it is in the Ministry of Interior).
- In MISWG countries there are FSOs in positions based on the confirmation of NSA/DSA throughout the government structure. FSOs are delegated to all facilities, held FSCs, too;
- All Hungarian critical infrasructure facilities have FSCs, vetted personnel, appointed FSOs, Security Liaison Officers, security risk assessments, and readiness plans.

MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP (MISWG)

34 member states: All NATO members except Iceland, additionally Sweden, Finland and Austria (EU), finally Switzerland, Australia, Israel, and New Zealand.

This forum was established in 1985 as non-governmental, non-NATO structure, originally to standardize security procedures for arms programs. MISWG has passed 23 basic documents, that may compose the foundation of the industrial security manuals of the member countries.

Hungary joined to MISWG in 1999. Three new documents were initiated and created by me: 1. Role of the FSOs, accepted in 2003. 2. Table of contents of Industrial Security Manual. 3. Facility Security Questionnaire template (FSQ), both accepted in 2011.

SOME OF THE MISWG DOCUMENTS

- Role of the Facility Security Officer.
- Facility and Personnel Security Clearance Information Sheet (opportunity for mutual data base checks);
- Programme/project security instruction (PSI);
- Arrangements for international hand carriage of classified documents, equipment and/or components;
- International visit procedures;
- Contract security clauses;
- FSQ template;
- Guidelines for assessing protection and control of classified information in a Multinational non-NATO Co-operative Defence Program.

MISWG MEETING

8-10 june 1999 in Bergen

MISWG Meeting in Tallinn, Estonia 2007

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM

- COE-DAT (Ankara) started its work in 28/06/2005, as an advisory body to Allied Command Transformation (ACT) based on terrorism related issues.
- COE-DAT's mission is to provied key decision makers with realistic solutions to terrorism and counterterrorism challanges. This transformation is focused on NATO's three declared core tasks of collecting deffence, crisis management and cooperative security.
- COE-DAT within its capacity supports the PfP countries' preparation as well.
- COE-DAT provides defence against terrorism focusing to education, training and excercises for experts.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM

COE-DAT organises and conducts the following activities:

- Courses, seminars, conferences and workshops;
- Concept and working development workshops;
- Lesson learnt evaluation and analysis;
- Academic researches and projects;
- Produce „Defence Againts Terrorism” related publications.

Expert speakers are from both the military and civilian spheres. Since 2007 COE-DAT provided 18 Mobile Education Trainings, one of them was held in 2011 in Ukraine;

In May 2016 a conference was held about critical infrastructure protection activities against terrorist threats.

CRITICAL INFRASTRUCTURE PROTECTION

Critical infrastructure: an asset, system or part thereof located in member states which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the distruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions. (EC directive 2008/114). *Hungary use this definition.*

Critical infrastructure protection (CIP): the ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction (EU).

Critical infrastructure protection 2: actions taken to prevent, remidiate, or mitigate the risk resulting from vulnerabilities of critical infrastructure assets.

CRITICAL INFRASTRUCTURE SECTORS

Power ranking statistics based on **24 nations:**

1. Energy (15 first place); 1.
2. Information and communication (4 first and 9 second place); 2.
3. Banking and finance (2 first, 5 second, 4 third place); 6.
4. Water (2 second, 4 third, 4 fourth place); 3.
5. Health (1 first, 4 fourth, 7 fifth place); 5.
6. Transport (1 first, 3 second, 4 third, 3 fourth, 5 fifth place); 9.
7. Food (1 second, 3 third, 1 forth, 5 fifth place); 4.
8. Public sector (1 first, 1 second, 1 third, 3 fourth place). 7.

Average number of critical infrastructure sectors are 9-10/country.

EU has11 sectors (power ranking of EU can be seen by red).

CIP EVENT CYCLE

Six phases of CIP Event Cycle (based on US DoD):

1. Analysis and assessment (occurs before an event).
2. Remediation (occurs before an event).
3. Indications and warnings (occurs before and/or during an event).
4. Mitigation (occurs both before and during an event).
5. Incident response (occurs after an event).
6. Reconstruction (occurs after an event).

The six phases of the DoD CIP life circle build on one another to create a framework for a comprehensive solution for infrastructure assurance.

SECURITY AWARENESS

Determined level of understanding of key issues, and what to do when face with them.

Aim of security awareness program: to understand current and future threats and vulnerabilities; to deliver right messages to the right people and at the right time; to increase reporting spirit, to promote risk management, lesson learnt process.

Some of the security awareness strategies:

- Formal and informal briefings, debriefings;
- Eye-catching security awareness bulletins, posters and flyers;
- News letters based on LOGON;
- Online computer-based tutorials in order to encourage asking;
- Imporvement of security controll and feedback.

Note: There are 130 nuclear reactors in operation in 14 EU countries. Safe operation of nuclear installations requires high level security awareness of the staff.

EDUCATION OF CIP

- CIP involves key security principles, general definitions, other common knowledges, which are valid for all sectors, so the combined education is allowed to be organised for all critical infrastructure personnel.
- Each critical infrastructure sector has its own specialities, some of them require PSCs. Due to it preferable to organise sector specific separate education courses for experts and personnel, based on need-to-know principle.

During the education among others have to describe or identify:

- The mission, the characteristic and partners of the given sector;
- Common security vulnerabilities;
- Consequences of sector failures;
- Elements of risk management;
- Potential terrorist threats and targets;

EDUCATION OF CIP

- Terrorist surveillance objectives and methodologies;
- Indicators of surveillance, and other suspicious activities;
- The elements of risk management model, involving strategy for reducing risk;
- General categories of protective measures;
- The purpose and elements of Operator Security Plan, Emergency Action Plan, Recovery Plan and Continuity Plan;
- The process of reporting incidents;
- Potential risks to workplace security, potential workplace violence indicators;
- Planned measures for improving workplace security;
- Types of special excercises.

SOME TRAINING TYPES OF CIP

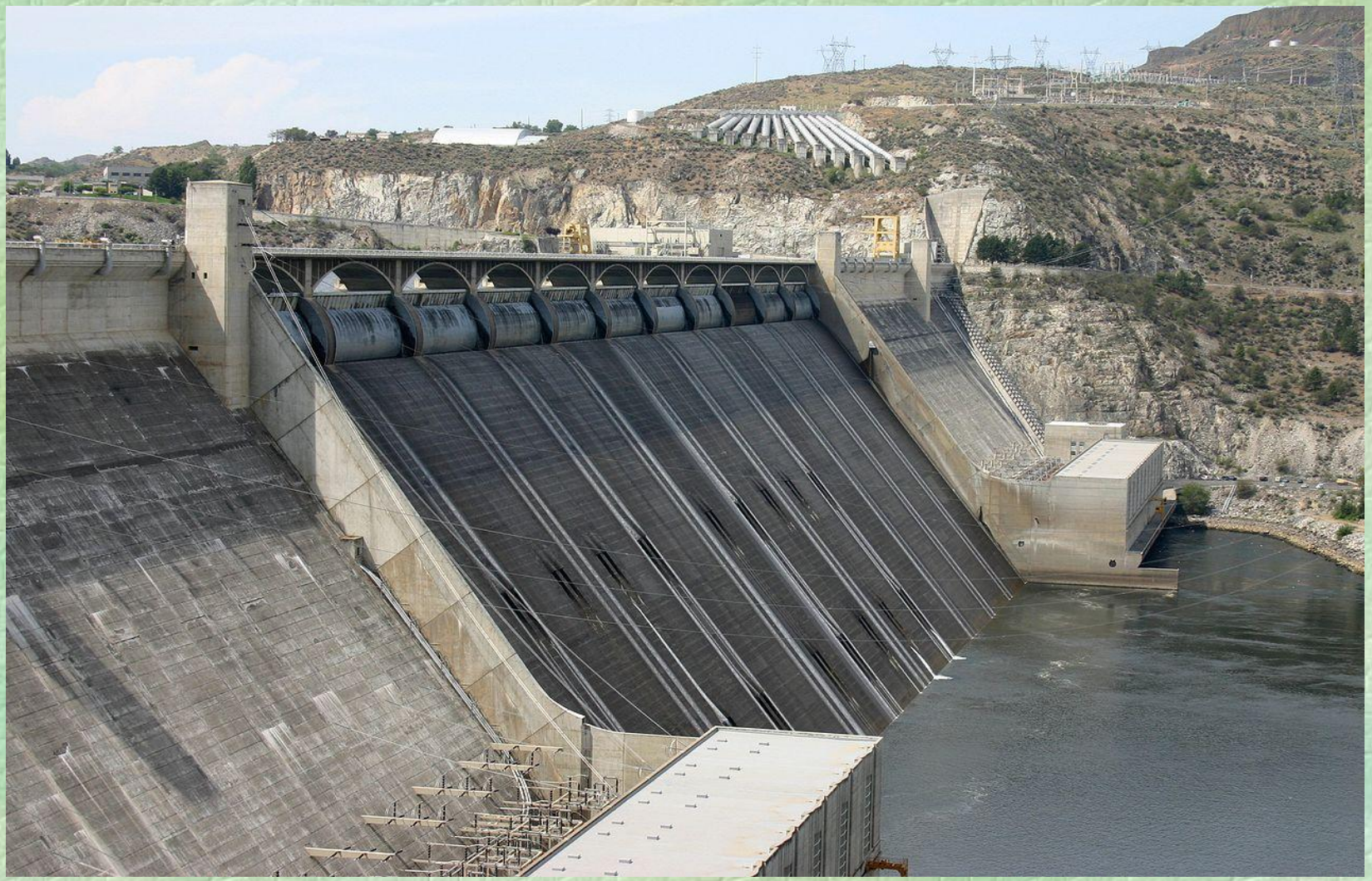
The current training program includes mainly practical knowledge for those officials, who have already passed initial training, based on protection of sensitive and/or classified information. It is raising the qualification and the security awareness of the personnel of critical infrastructure facilities.

- Incident response: it improves reaction skills, professionalism and cooperation ability of employees.
- Brain storming: evaluation of strongest and weakest links of CIP security system, protecting the given object. It develops problem-solving skills, creativity and security awarenes of personnel.
- Case studies: by analysing real CIP related situations it can develop analytical and problem-solving skills, and also build a strong sense of teamwork.
- Role-playing: excellent training technique for improving many interpersonal skills.

METHODOLOGY FOR EDUCATION AND TRAINING OF CIP IN HUNGARY

- Participation in the work of such international organisations, which are dealing with CIP education, trainings and exercises;
- Participation of experts to official, government sponsored trainings, conferences, workshops, which involve best practices, lesson learnt topics. Use their new knowledge during CIP education or training;
- Guidences on developing and implementing effective security programmes, clear requirements and strict internal checks;
- Clearly define CIP roles and responsibilities;
- Annual reinforcement of previous education and training;
- Increasing the security awareness of personnel by spread of sector specific flyers;
- WEB-based security awareness training, providing by Internet programs. Effective use of network analysis and research methods.

GRAND COULEE DAM (USA)



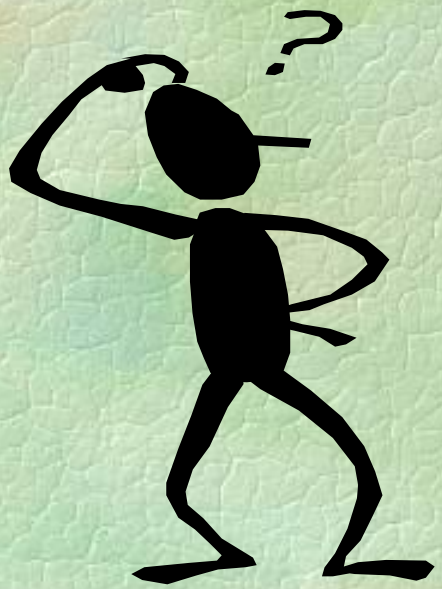
QUESTIONS?

QUESTIONS?

QUESTIONS?

QUESTIONS?

QUESTIONS?



QUESTIONS?

QUESTIONS?

QUESTIONS?

QUESTIONS?

QUESTIONS?

QUESTIONS?

QUESTIONS?

QUESTIONS?