

COUNTERACTING THREATS TO CRITICAL ENERGY INFRASTRUCTURES THROUGH SECURITY TRAINING

Rostislav RICHTER, Jitka COLLIS, David JACKSON

rostislav.richter@ioolb.izscr.cz, collis.jitka@gmail.com, david@homelandsecurity.org.uk

Abstract

The article summarizes the scope, findings and recommendations from the EC research project COUNTERACT (Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities) - specifically from the targeted study: "Counteracting Threats to Critical Energy Infrastructures through Security Training", undertaken by the Population Protection Institute (PPI), Czech Republic – a member of the Energy Cluster.

Energy security is one of the key elements of current energy policies in Europe. Sudden, short term disruptions can originate from a variety of events, political or trade disputes, natural disasters and malicious attacks. In the course of redefining its security policy, the European Union recognized the need for an improved understanding of the vulnerability of European critical infrastructures to terrorist attacks and through the Directorate-General for Energy supported the COUNTERACT project, whose objectives were to better understand the terrorism to Energy Infrastructure, collect available experience and existing best practices, identify existing gaps in knowledge, tools or policies, conduct targeted studies to close minor gaps, elaborate recommendations and focus for future research activities, and recommend best practice measures to enhance protection and improve preparedness and response.

Key words

COUNTERACT, protection of energy infrastructure, training course, energy security, protection against terrorism.

INTRODUCTION

Infrastructures serve as vital lifelines in our societies. We are reliant on the supply of energy and water, information technology and mobility functioning in a dependable manner. Large-scale failures of these systems or other important infrastructures, even for only short periods, can have serious consequences.

Whatever age we are, and whatever activities we undertake, energy plays a fundamental role in today's world. Energy policy directly affects everyone in Europe. The issues and challenges connected to this policy require action at European level; no single national government can address them successfully alone. By working in concert, European Union Member States and European industry can develop energy sectors which best meet the needs of citizens and our economy, whilst minimising damage to our environment. The European Commission's Directorate-General for Energy manages work in this area.

It is nothing more than our duty to protect Europe's assets and (infra) structures that are basic for a normal functioning, the well-being and the prosperity of the European citizen, his institutions and organizations and his relations with his partners.

Training, in this relation to the security of critical energy infrastructures not only shows some specific challenges, but also offers some opportunities. It is known that security awareness is something many organizations desperately need and at the same time also lack.

An active security awareness program can greatly reduce many risks which cannot be addressed through security software and hardware devices. In these cases, it is the human element of security that must be addressed which is what our targeted study tries to prove.

PRE-TARGETED STUDY RESEARCH

The PPI choose to concentrate on education and training for increasing resistance of energy infrastructure to terrorist threats because they strongly believe that systematic training of human factor and continued education of staff is closely connected to the increase of security of energy operators and therefore also protects energy infrastructure. And this theory was proved to be correct in a survey they did before they proposed their Targeted Study. Within the research inquiry, energy operators from 7 EU countries were approached and sent their answers.

The pre-targeted study survey attempted to find out, how the security managers of energy companies view the security topics, or more precisely, protection of energy infrastructure against terrorist attacks.

The research inquiry dealt with three topics

- Perception of terrorist attack threat
- Defining Critical Infrastructure on EU and national level and subsequent demands legal designation of jurisdictions and duties of each member involved
- Training of staff in order to raise their awareness of a possible terrorist attack and ability to deal with it

Structure of replies

The structure of replies can be seen in the table No. 1. Questioned people were asked to choose from the following answers: I strongly or partially agree or I strongly or partially disagree.

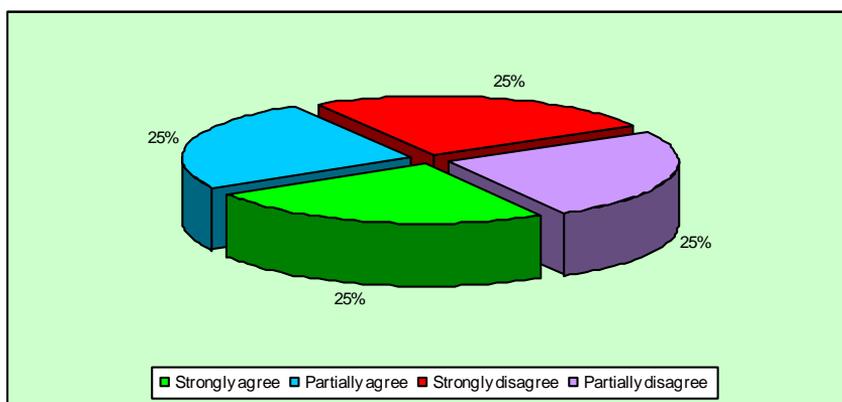


Table 1
Structure of replies

Question 1

When asked a question 1: “Do you think that education/training of selected personnel in the field of protection against terrorist attacks should be a part of companies’/organizations’ internal education and training programmes?” 92 % of respondents answered **yes** (69 % strongly agree and a 23 % partially agree). Questioned people clearly communicated, that increasing security is significantly related to human factor and that it is not just a matter of technical measures, such as monitoring and detection systems, or other elements of passive protection.

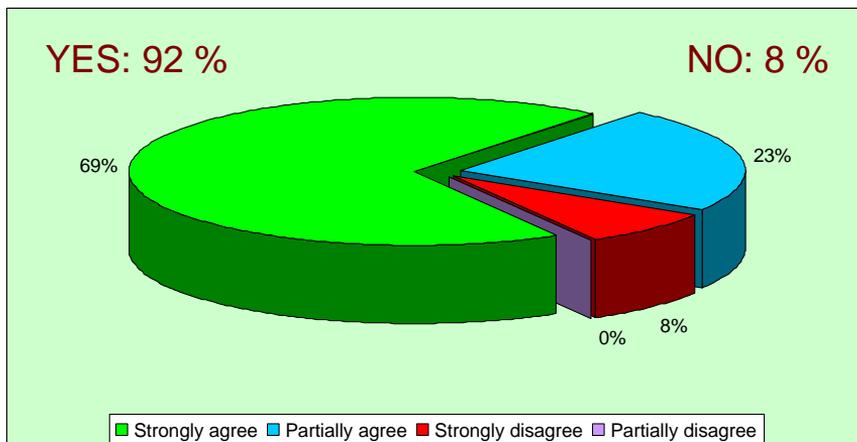


Table 2
Answers to the question No. 1

Question 2

The next question was: “Does your company/organization provide training on increasing security and awareness of terrorist threats to its employees?” In the table No. 3 we can see that only 41% (33% strongly agree and 8% partially agree) of the questioned people answered that their companies do organize some kind of training and courses concerning security and terrorism topics. If we consider the replies to the first question, where 92% of questioned people acknowledged the needfulness of such training activities, we can clearly notice an imbalance in acknowledged need to be trained and the reality. The difference is 50%.

This fact could be caused by various reasons and could be related for instance to how likely the top management thinks the terrorist attack could happen. One of the reasons however could be a small amount of external expertise and assistance in organizing such orientated course.

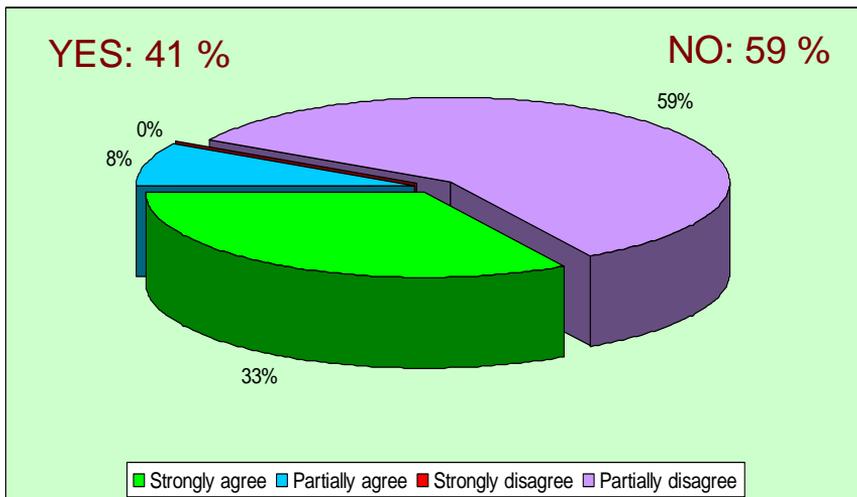


Table 3
Answers to the question No. 2

Question 3

The question: “Do you think that you get sufficient amount of offers for external training activities for your personnel in the field of detection and management of possible terrorist attacks?” was answered yes by only 33% (Table No 4) of questioned people (8% strongly agree and 25% partially agree).

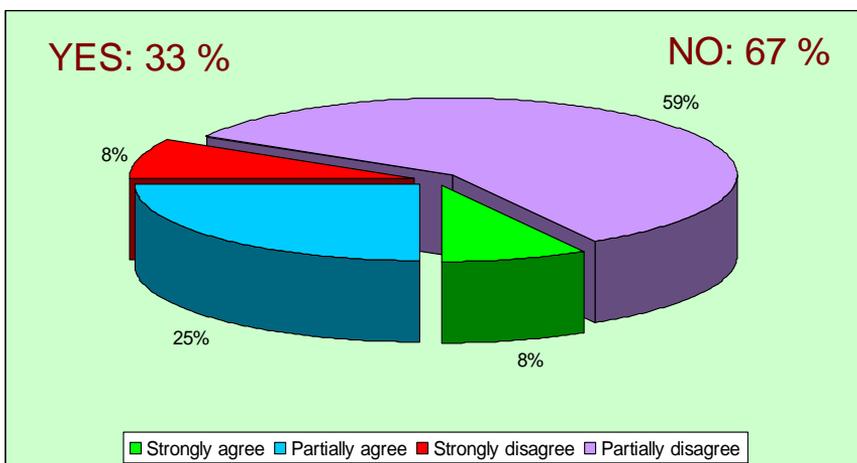


Table 4
Answers to question No. 3

And this was one of the reasons, why the PPI chose to organize the security course as a part of the targeted study. Their aim was a contribution to the strategic management.

Their vision was a guided and controlled development of intellectual potential of the staff of energy companies concerning security.

With regards to the type of a training activity, they opted for a course, because this educational method develops knowledge as well as skills; it is a combination of theory and practice.

They have concentrated on 3 spheres of action:

1. Sphere: Understanding and implementing knowledge in protecting energy infrastructure
2. Sphere: Critical thinking, creativity, independent decision making
3. Sphere: Using and evaluating information

SECURITY TRAINING COURSE FOR STRATEGIC STAFF

When creating a pilot security course it is of a vital importance to design a training programme with a clear purpose, designated target audience, and a linkage to the existing security training systems. Such a specific sectorial-based programme could only be elaborated with the full support and involvement of the lead companies within the energy sector. Indeed, it should be them who identify the training need and the training provider respond to that need with an appropriately based programme or set of training modules.

• Objectives of the pilot course

The aim of the course, which was organised in the Czech Republic by the PPI was to bring the attention of the security community within the energy industry to the following:

- An update on the threat to energy security
- An overview of key vulnerabilities within the sector
- A review of new training developments within the energy sector in the EU and USA that might have relevance to the security officials charged with this responsibility
- Instruction on how to develop security standards within the industry and how this could be linked to European Vocational Qualifications for industry personnel at several levels from basic and applied to senior managerial level
- Enhancement of networking amongst the energy operators and relevant public authorities in order to improve protection levels of the energy infrastructures
- The development of a short table-top simulation exercise to highlight security concerns
- The presentation of a 'participant handbook' - Consideration was given to the production of a course handbook this was intended for the workshop participants and reflect both lecture material provided by the training team and a selection of critical background material and relevant documents

• Targeted participants

The energy infrastructure's strategic level is – whereas this study is concerned – excluded as a specific target group.

It is understood that awareness on this level needs no further encouragement or incentive and that, also with reference to the matter of preparedness, the "tactical level" training should provide all necessary knowledge.

Security Directors/Managers from energy companies - the infrastructure's operators and security officers on a tactical level, partners from relevant public authorities – Ministry of Interior, Ministry of Industry and Trade, Fire Rescue Services, Police, University.

- **Theoretical part of the course**

The theoretical part dealt with analysis of present terrorist threats and approaches to the problems with increasing security of energy sector. Strength and weaknesses of energy infrastructure were analysed, and the speakers also talked about perception of possible terrorist threats.

It was stressed, that besides physical security planning, effort and investment should be given to train the staff in the area of risk evaluation, improve their ability to manage complex security systems and to test the equipment and security measures. There was a request highlighted to concentrate on certain threats and develop training courses with adequate modules for those types of threats. The modules could then be tested and only after that they should be implemented within the company or the whole industry. Further topics were: energy security from the supply chain point of view, requirement for public private partnerships in energy security, security checking procedures and malicious attacks against energy plant operating systems through cyber attack, planning a range of security systems and procedures in relation to typical land-based energy sector installations and identifying key requirements within a training regime.

- **Practical part: Simulation Exercise**

The second part of the course focused on a simulation exercise called “Operation Shutdown”. The exercise dealt with an imaginary terrorist attack on chosen facilities in Poland, Slovakia, Czech Republic and Hungary. The participants were divided into three groups. Each group chose its leader and a speaker. Each group also had a designated facilitator, who posed as both an advisor and somebody, who continuously released further information about activities of the terrorist group. During the work in groups, the speakers or leaders of groups reported to their facilitators. The final task was to create a report for the Government. This report had to contain three main points: account of the situation, impact on the territory of the state, and draft of measures. The participants put a lot of effort into dealing with their tasks. They were active, emotions were high, their opinions varied, but towards the end they managed to reach certain consensus of opinions. They had to reach the conclusion within a given time limit. For the final part all the participants gathered together again and their speakers presented their group reports. Their conclusions were then appraised by their facilitators.

- **Course feedback**

The course was assessed by the participants as a very successful and it fulfilled their expectations, set for these kind of training events. They valued not only the opportunity to exchange and share information about protection of energy infrastructure but also the form of active engagement in the simulation exercise. All participants appreciated the chance to meet their colleagues from other companies on such a level. Most of the participants expressed their wish to take part in similar events in the future, organized on both the national and also the European level.

Within the scope of the feedback, a new dimension called “learning factor” was covered. It consisted in not asking for the overall contribution of the course, but about how beneficial it was for the various areas, such as:

- Broadening knowledge
- Exercising skills
- Improving general outlook
- Enthusiasms for the topics

The result was satisfactory – correlation analysis showed that the questions were slightly coherent (they measured one thing), so it was worth inquiring about all 4 areas separately.

The participants had following opinions and suggestions concerning development of training activities:

1. To create a European system and individual national systems of education and training of selected staff on both EU and national levels. The aim would be:
 - to offer educational and training activities,
 - to create specialized electronic library for security managers,
 - to create educational and training modules for each type of energy operating company,
 - to define key competences for each manager (according to the level of management), selected staff and other employees within the security field.

2. Need to co-operate with the top management

It is necessary to help the managers to realize, how valuable asset it is to have well trained staff that can efficiently co-operate, share information, and develop their knowledge needed for effective functioning of the company in the field of security within today's hazardous environment.

In this respect it is necessary to pay attention to the questions concerning effective training of the staff and approaches to evaluation of efficiency of the training programmes.

Our participants expressed that with respect to the above, they would like to see an increased effort from both EU and national governments.

SUGGESTIONS: FURTHER COURSE MODULES

1 Module for key players - Seminar

In order to win over the key players a Seminar, possibly international, could be organized with the aim to provide an overview of the current terrorism threat to the European Union and its Member States and how this threat might impact on the energy sectors at the European and National levels. It should also mention the need for greater awareness, preparedness and communication throughout the European Union as regards the security of the energy production and transmission infrastructures and the contribution that a concerted, EU-wide program of security training can make to the enhancement of energy infrastructure security. This overview should be used to persuade the members of State Administrations, Security Organizations and the Energy Infrastructure top management about the need to protect their Critical Energy Infrastructure and promote security trainings in their countries.

Aimed at the senior management level, this Seminar would be expected to stimulate discussion on the common principles for a program of regionally-based security training and an implementation plan for this training program.

It would be beneficial if the following personnel participated in the Seminar: State administration officials from the relevant Ministries, relevant National Security Officers, and the CEOs or General Directors of main Electricity, Gas and Oil companies.

Speakers at the Seminar should provide the knowledge of current security threats and patterns; relevant national and international legislation and security requirements; experience with organizing similar courses in other member states; expertise in relevant aspects of energy infrastructure security, and the expertise in infrastructure security measures.

2 Module for Operational Staff

The primary goal of security awareness is to reduce loss, and this happens when good security behaviours become reflex actions for the staff. The best awareness programs motivate

the workforce by showing them that their behaviours are the most important element in preventing loss. When building a successful training course the following four steps should be specified:

- **Awareness and Training Program Design:** in this step, a companywide needs assessment would be conducted and a training strategy would be developed and approved. This strategic planning document identifies implementation tasks to be performed in support of established company security training goals.
- **Awareness and Training Material Development:** this step would focus on available training sources, scope, content, and development of training material, including solicitation of contractor assistance if needed.
- **Program Implementation:** this step would address effective communication and roll out of the awareness and training program. It should also consider options for delivery of awareness and training material (web-based, distance learning, video, on-site, etc.).
- **Post-Implementation:** this step would give guidance on keeping the program current, and on monitoring its effectiveness. Effective feedback methods should be described (surveys, focus groups, benchmarking, etc.).

It is recommended for an operator to put together a set of guidelines for building and maintaining a comprehensive awareness and training program, as part of an organization's security program. The guidance should be presented in a life-cycle approach, ranging from designing, developing, and implementing awareness and training program through post-implementation program evaluation.

In other words, if a company decides to organize security awareness courses for its operational staff, it should pay attention to how to select awareness and training topics; find sources of awareness and training material; implement awareness and training material, using a variety of methods; evaluate the effectiveness of the program; and update and improve the focus as technology and organizational priorities change.

Target groups should be all security force and selected work force on an operational level.

Aim of the course would be to enhance staff's awareness of, and preparedness for terrorist threats and their prevention and mitigation.

Program: Training session could contain the following topics:

- knowledge of current security threats and patterns and the meaning and the consequential requirements of the different security levels;
- recognition and detection of weapons, dangerous substances and devices;
- methods of physical searches of persons, personal effects, baggage and cargo; and
- leading and conducting search activities;
- recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
- techniques used to circumvent security measures;
- crowd management and control techniques;
- security-related communications;
- methodology of search activities;
- safety and best practices in specific response;
- Demo "explosives".

Studies have consistently shown that **about 80% of security incidents stem from staff behaviour**. Many of these incidents involve errors and omissions. People who have an awareness of danger signals are an organization's most valuable sensory instruments. Therefore recognizing and correctly responding to security events should be a reflex for employees. Awareness programs and activities can build this reflex behaviour.

RECOMMENDATIONS

- The aim of the education and training is to support awareness and preparedness of all stakeholders with responsibilities in the protection of Europe's critical energy infrastructures.
- Educating and training of the selected personnel is considered by EU energy operators as an integral part of increasing protection of Energy CI.
- Execution of the training course has proved that success of a course depends on:
 - Well-balanced usage of theory and practice,
 - Interactive approach, i.e. the course has to be dynamic and interactive,
 - Adequate levels of flexibility, i.e. the actual needs of participants are responded to during the course. Feedback is a fundamental building stone. The lecturer performs as a coach, who shares new pieces of knowledge, leads discussions, solves individual needs of participants, and provides new views of the situations and their present solutions.
- Until now, in the field of education and training within protection of energy CI, there has not been a network in Europe for sharing experience across borders and between public and private organisations. With regards to this matter it is recommended to found, under the authority of EC an Energy Critical Infrastructure Security Educational and Training Network (ECISETN) and to draw up a project for that purpose.

The members of the network would contribute by delivering a professional non-binding exchange of information on the security education and training of energy infrastructure, considering primarily electricity, oil and gas. Experience and best practice would be compared and discussed.

The ECISETN would arrange seminars, lectures, round table discussions, and optional field trips approximately 2 - 4 times a year.
- In line with the Article 8 (Commission support for ECIs) of COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection we would also suggest to create an analysis of education and training in the field of protection energy CI in selected both EU and non EU member states and use this analysis:
 - for providing an access to tested educational and training procedures and methodics,
 - for exchanging information,
 - as a background material for the review of COUNCIL DIRECTIVE 2008/114/EC (Article 11 – Review).
- Targeted Study Recommendation: create national systems of education and training in the field of protection of energy CI with the aim of:
 - Offer a range of educational and training,
 - Create a specialized electronic library for security managers,
 - Develop educational and training modules for individual types of energy companies,
 - Develop key competences for individual managerial levels, selected staff and other personnel in the field of protection energy infrastructure.
- Member states of EU should, in public private partnership, designate a responsible authority to guard the effectiveness and quality of local training and exercise.
- Education and training should be provided by or through a recognized security organization (RSO). Conditions to be fulfilled by a RSO:
 - expertise in relevant aspects of energy infrastructure security;

- an appropriate knowledge of energy operations, including knowledge of infrastructure and terminal design and construction;
- an appropriate knowledge of other security relevant operations potentially affecting energy infrastructure security;
- the capability to assess the likely energy infrastructure security risks;
- the ability to maintain and improve the energy infrastructure's security expertise of its personnel;
- the ability to monitor the continuing trustworthiness of its personnel;
- knowledge of relevant national and international legislation and security requirements;
- knowledge of current security threats and patterns;
- the ability to recognize and detect weapons, dangerous substances and devices;
- the ability to recognize, on a non-discriminatory basis, characteristics and behavioral patterns of persons who are likely to threaten energy infrastructure security.

SUMMARY

Social background of a terrorist threat has negative effects on psychological state of employees. By organizing educational and training activities focused on increasing ability of protection against terrorist attack, the employee have opportunity to deepen their professional role, boost their mental strength and believe that they are not only passive potential object of terrorist attack.

Education and training therefore does not only contribute to the improvement of knowledge and skills, but it also helps to increase psychological preparedness and resistance and also helps the staff to interiorize themselves with the mission of their company.

Each educational field develops with different dynamics. However, three developmental periods can be defined for each of them: pre-pragmatic, paradigmatic and revolution stage. Recognition of education and training focused on increasing protection of energy infrastructure against terrorist attacks is among many top managers and representatives of state administration still in pre-paradigmatic stage. In these contexts it is necessary to make every possible effort to change the situation, change the thinking and aim at appreciation of adequate meaning of educational and training process and its contribution to the increase of security.

This article was created within the project "Security of citizens – Crisis Management" (VF20112015018).