ENERGY-CRITICAL INFRASTRUCTURE PROTECTION: "THE CASE OF GREECE"

Ioannis E. Anastasakis

Introduction

Certain Critical Infrastructure assets, including systems and networks, were considered vital for the normal operation of all public services, in every well organized community. In order to be controlled in an efficient way, Critical Infrastructure assets are modular separated in various Sectors[1]. For the efficient protection of Critical Infrastructure, national Authorities and private Security agents should collaborate in a well coordinated and common understanding manner. This collaboration could be sustainable by conducting common training, common exercises and above all by information sharing

Critical infrastructure sectors

In global environment, there are experts[2] on the Critical Infrastructure (CI) field, identifying CI Sectors (CIS) in a different approach, focusing mainly on cyber security, or on energy, or on Communications, or putting other priorities. For purposes of studying and better understanding, review of a national "Critical Infrastructure (CI)" constellation is very helpful. A "model" of study is that of the USA because CI is a well organized and properly documented field. In USA public services, there are sixteen (16) distinctive "critical Infrastructure" Sectors[3], as follows:

First Sector covers "Chemical" factories and storage facilities; Second Sector covers "Commercial

[1] . USA/Presidential Policy Directive/PPD-21 (2015)

[2] J. Lopez, R. Setola, S. Wolthusen, 2012," Critical Infrastructure Protection", Springer Link

[3] USA/DHS/www.dhs.gov/what-critical-infrastructure (2016)

Facilities",here many people gather together in the pattern of every day life; Third Sector covers "Communications"; Fourth Sector covers "Critical Manufacturing" as viable production industrial basis; Fifth Sector covers "Dams" as water emergency reservoirs, or as part of hydroelectric assets; Sixth Sector covers "Defence Industrial Base" which plays a key role in sustaining national Security contingencies in homeland or abroad; Seventh Sector covers "Emergency Services"; Eighth Sector covers "Water & Waste water Systems"; Ninth Sector covers "Financial Services"; Tenth Sector covers "Food and Agriculture"; Eleventh Sector covers "Government Facilities"; Twelfth Sector covers "Health& Care"; Thirteenth Sector covers "Homeland Security"; Fourteenth Sector covers "Nuclear Reactors", both for operational and environmental issues; Fifteen Sector covers "Transportation Systems"; and, finally sixteenth Sector covers "Energy", which includes three major resources, namely electricity, Oil and Gas.

As it is obvious, the Energy Sector is of paramount importance, because the provision of "power" is essential to supporting and sustaining the functions of all other Critical Infrastructure Sectors.

Protection of assets

Focusing on the Protection of Energy related Critical Infrastructure, namely the related assets, systems and networks, it will be proper to cover certain main points, such as Personnel, Physical protection of assets, encountering of disasters, and renewable energy.

Personnel

Initially, of high importance is the Personnel that is usually called "the human factor". The term "personnel" includes employees of any kind of function, at all levels of organizations pyramid, including administration, production, services and security. In addition, and for Security reasons, the term Personnel may describe any person appointed with an official authorization to have access to critical energy infrastructure.

The role of the "human factor", as percentage of various behaviors, is well analyzed in OSCEs related study[4] , which clearly shows the importance of the personnel factor in any critical energy infrastructure, in order to prevent accidents, sabotage, and minimize terrorist or criminal activities. In the context of selective "reasons" of the catastrophic "human Factor" effect in CIP process, one can cite the unsystematic prevention 57%, the career disappointment 69%, the inadequate internal checks 77%, and the lack of a sense of wrongdoing 93%.

Thus, proper training, Security planning, drills and exercises, inspections and periodically Security Personnel Interviews can safeguard that the "human factor" will contribute positively towards CIP.

Physical protection

The physical Protection of Critical Infrastructure is a complicated issue. Public or Private enterprises, in order to safeguard CIP they need to employ well trained Security Personnel and put procedures in place, based on a local vulnerability analysis[5] .

Knowledge and experience gained from past incidents and also from international Organizations "Security Policy papers" are very important and useful consignments. For example, NATO's Security Policy Documents[6] and related Directives[7] , which focus on "Protection Measures for NATO Personnel and Installations (assets) against Terrorist Threats", provide substantial information and guidance. On the same path, the European Union's "Industrial Security measures"[8] provide a concentrated knowledge and experience on Security Protection of Critical Infrastructure which is also applicable to energy related CIP.

Based on this, Security officers and Security Planners should take certain steps and measures towards

[4] OSCE, "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP)"

[5] George Leventakis, 2013, "system Security and Critical Infrastructure", Aegean University

[6] NATO, Protection measures … Against Terrorist Threats, C-M(2002)50

[7] Directive on Personnel Security, AC/35 D/2000 – Directive on Physical Security, AC35 D/2001

[8] European Program for CIP (EPCIP), COM(2006)786 Final

enhancing CIP on any particular asset. There is a big variety of key Infrastructure assets that Security Personnel have responsibility to protect. Vulnerability varies from asset to asset, depending on specific characteristics that need to be considered. The size (spot, length, compound etc), the Location (remote area, within city limits, etc.), the Access (offshore, on shore, mountainous area, access routes by land-sea-air, etc), the Approach (Physical or technical obstacles), are some of the characteristics that Security planers should take under consideration.

Encounter disasters

A common saying among military officers worldwide is that: "*If you want to avoid war, be prepared for war*". On the same pattern, concerning Security and Critical Infrastructure Protection, the common saying should go like: "*if you wand physical protection of assets, be prepared for disasters*".

Encountering Disasters is not an easy task. Special reaction Units, at public or private companies' level, should be established. These Units should be manned, equipped and trained in a proper manner to obtain capabilities in order to properly react and minimize disasters effect on human lives and assets. Joint training and exercises between Public and Private Units should be conducted periodically, with the purpose of achieving common understanding, professional experience and interoperability of equipments.

Sabotage and Terrorist actions primarily aim to cause extensive damage[9], therefore Security Personnel performing CIP should be proactively prepared to tackle "Asymmetric Threats" that aim to cause a "shock and terror effect".

Renewable energy installations

At this point, it is important to note that the renewable energy sub-sector, due to the local and low quantity energy production, should be considered as a second priority target because of the low "damage effect" it has on the extended society.

[9] Security Manager magazine, Nov. 2008, "European Program for CIP"

Especially in Greece as well as in Croatia, there are not large "Renewable Energy Parks", the disruption of which could cause the effect that terrorist and saboteurs would like to create. Noteworthy, the total installed capacity for Greece and Croatia is 15,1% and 6,6% respectively, with 2012 est.[10] Thus, for the purpose of economy in manpower and means, Security Planers should protect this kind of assets, as much effectively as the company can afford.

The Protection of Critical Energy Infrastructure and the readiness to encounter disasters, is not solely the responsibility of the Public or Private enterprise which runs a specific company. The supervision and collaboration of the competent National Authorities is of paramount importance.

Eastern Mediterranean hydrocarbon discoveries (Contemporary and Future Security Implications)

The discovery of oil and natural gas in the Eastern Mediterranean poses a number of distinct and localized security concerns for the future, in addition to contemporary measures. The Security Planers need to answer certain questions during the planning process.

The first question is: "*How attractive a target might be to terrorists, for both the on-shore and off-shore installations*?" The Security Plans need to cover threats from terrorism actions, hostile states, sabotage, natural disasters or any criminal action.

The second question is: "*What would be the most lucrative option for attacking/targeting on-shore and off-shore installations?*" It is important to establish an early warning system and enforce protection measures for deterrence.

The third question is: "*What security structures or organizations are necessary to deter and prevent hostile action(s) against these sites?*" An answer can be based on experience from other hydrocarbon extractions areas, like: Australia, Gulf of Mexico, Falklands, Nigeria etc. It is of high importance to mention that the National Authorities and Private Enterprises responsibilities are overlapping in most of the cases.

[10] Fact book, 2015 edition

The fourth question is: "*What effect might hydrocarbons have on the security of wider national or regional areas, like Greece, Croatia and the Balkans, including relations with other regions and stakeholders?*" An answer needs to encompass Political and Environmental implications. International Organizations[11] and key players, in collaboration with the local Authorities should give proper guidance to answer this complicated question.

Natural Disasters and especially intentionally caused mankind disasters on hydrocarbon Energy related Critical Infrastructure create huge damages, disruption of public life, human losses and severe environmental effects. It is essential for Security Planners to take measures to prevent such disasters. In an unavoidable situation, they should have plans on how to "encounter Disasters". Everybody remembers the front page press releases covering disasters, such as the oil spill in the Gulf of Mexico, in Alaska, and other areas.

Conclusion

For countries like Greece and Croatia that have a flourishing tourism industry, the kind of cited disasters can create a devastating effect on the national economy. It is important to highlight the need for common understanding of all personnel playing a key role in the protection of critical Energy Infrastructure. Even though CIP is primarily depending on National responsibility, International and Regional collaboration is key for success, and can be achieved through Information flow, sharing experience and knowledge, common training and exercise, as well as collectively response to threats and disasters.

[11] Official journal L345/75, 23-12-2008,"CIP implementation of the European Directive 2008/114 EC