ICISS

Newsletter: February 2016

International Council for Industrial Security & Safety Management

In a joint address before the media in India, at Delhi on Monday, 25th January, French President Francois Hollande focused extensively on terrorism, saying that both countries 'know the forces that hit them — Daesh (Islamic State).'

"(Islamic State) is provoking us in the worst manner possible. But they can only make us more determined," Hollande said at Hyderabad House in Delhi.

Indian Prime Minister Narendra Modi, too, made a strong reference to terrorism, saying that terror attacks have been seen recently in Paris, as well as in Pathankot. "Terrorism is the enemy of human values and humanity. The world must unite against this threat," Modi said.

The journey of terror from Paris to Pathankot is full of correlations, many common characteristics and a lack of desire to have a peaceful coexistence by certain nations and/or communities. For the security and safety professionals perils to life are biggest professional challenges to be handled in the professions and saving lives are the biggest rewards! We constantly need to upgrade our situational awareness and fine tune our responses.

With this purpose as our focus of this edition of the ICISSM Newsletter, we bring to you two articles – one is an attempt to draw parallels between Paris & Pathankot terrorists' attacks and other one is aimed to bring out the considerations for security of key-infrastructure.

With very best regards

Capt S B Tyagi

ICISS International Council For Industrial Security And Safety Management

Paris to Pathankot: Industrial Security Uptake

The Global Threat of Terrorism Targeting Oil and Gas Industries

Capt SB Tyagi, FISM, CSC, CSP

‘Energy security is among the most serious security and economic challenges, both today and in the future. As the economies of the World grow and societies develop, so does the importance of energy. And so does the importance of the infrastructures that produce and supply this energy’. This brings Oil & Gas Sector under sharp focus!

Terrorist organizations have always been interested in targeting oil and gas facilities. Striking pipelines, tankers, refineries and oil fields accomplishes two desired goals: undermining the internal stability of the regimes they are fighting, and economically weakening foreign powers with vested interests in their region. In the past decade alone, there have been scores of attacks against oil targets primarily in the Middle East, Africa and Latin America. These attacks have never received much attention and have been treated as part of the ‘industry’s risk.’

Today, a growing number of interconnected and diverse threats, mainly physical and cyber threats are challenging critical infrastructures. In that regard, terrorist threat is not a new phenomenon and critical infrastructures have long been attractive targets for terrorist groups and malicious acts. Especially, as being one of the most vulnerable sectors, Critical Energy Infrastructures have been subjected to increasing terrorist threat which is correlated with the growing political and economic instability in oil and gas producing regions. Furthermore, despite its enormous economic and political consequences, unlike other types of terrorism, energy terrorism could not attract a significant level of attention.

According to the University of Maryland's Global Terrorism Database, terrorist threats targeting oil and gas sectors have risen sharply. More precisely, during the mid-1990's, attacks on oil and installations reflected less than 2.5 of all attacks whereas in 2013, 600 out of 2600 total terror attacks targeted oil and gas sectors. In fact, a wide majority of attacks concentrates in the Middle East and North Africa.

However, from U.S to China, energy infrastructures are facing a varying level of threat (from theft to sabotage) which means that energy facilities worldwide have common vulnerabilities including inadequate controls at the borders; lack of a holistic security approach; lack of technology and lack of dedicated security forces etc.

Examining this trend more closely it can be seen that in 2003 roughly 25% of terrorist attacks were aimed at the energy sector, having jumped to 30% and 35% between 2003 and 2007 –the long-term trend revealing more attacks aimed at energy infrastructure (EI) occurring annually–. With oil accounting for nearly '40% of the world's energy and 96% of its transportation', the protection of energy infrastructure has thus become a top priority for most industrialised nations.

Threats over the Sea

There is growing evidence that terrorists find the unpoliced sea to be their preferred domain of operation. Today, over 60% of the world's oil is shipped on 3,500 tankers through a small number of 'chokepoints' – straits and channels narrow enough to be blocked, and vulnerable to piracy and terrorism. The most important chokepoints are the Strait of Hormuz, through which 13 million barrels of oil are moved daily, Bab el-Mandab, which connects the Red Sea to the Gulf of Aden and the Arabian Sea, and the Strait of Malacca, between Indonesia and Malaysia. Thirty percent of the world's trade and 80% of Japan's crude oil passes through the latter, including half of all sea shipments of oil bound for East Asia and two-thirds of global liquefied natural gas shipments.

Pipelines are terrorist's weapon of choice

Until recently, the pipeline industry has been preoccupied primarily with environmental, safety and maintenance issues. Beyond occasional cases of vandalism, the human factor was hardly perceived as a threat to the world's vast web of oil and gas pipelines, which, all told, carry roughly half of the world's oil and most of its natural gas.

Pipelines, through which about 40% of world's oil flows, are another Achilles heel! They run over thousands of miles and across some of the most volatile areas in the world. Pipelines are also very easily sabotaged. A simple explosive device can put a critical section of pipeline out of operation for weeks. This is why pipeline sabotage has become the weapon of choice of the insurgents in Iraq. An attack on major oil installation, a chokepoint or a pipeline hub would be detrimental to any country's economy and likely to affect every aspect of lives of its citizens.

Petrochemical complexes and Oil installations on the hand are highly critical, highly vulnerable and sabotage and terrorist attack is highly provable. This makes them also very attractive target with high "Terror Quotient" as damages here are likely to the lives and economy!

Security Solutions

With the threat of terrorism looming, pipeline operators in the industrialized world have taken action to prevent terrorism from harming energy infrastructure with steps that include:

- Increasing system redundancy,
- Deploying state-of-the-art surveillance equipment,
- Deploying aerial and ground patrols, and
- Fortifying pipeline systems against cyber-security breaches.
- 'Lessons learned from accidents and safety incidents have been regrettable but they are critical contributions to instil safety in the DNA and operating culture of any prudent oil and gas operator.' In other words, it could be said that in order to implement and exercise best security practices for the energy industry, lessons learned from previous incidents should be well understood.
- Numbers of best practices could be recommended for the Oil & Gas Sector -
- 'Security' should be considered and studied as an independent and distinct discipline from 'Safety' and it should be defined with clear objectives.
- Establishing proper mechanisms for 'Intelligence' and 'Information Sharing' is critical for assessing terrorism risks for a critical infrastructure. For instance, in order to eliminate insider threat and reach deeper information about their employees, companies could cooperate with state agencies in information sharing.
- A holistic and integrated security approach seems as a must in implementing corporate security policies.
- Developing alternative 'threat scenarios' with various inputs and outputs is an essential part for a company's security plans. In other words, security departments should be capable to answer 'what if' questions regarding the changing conjuncture and threat and risk levels.

Conclusion

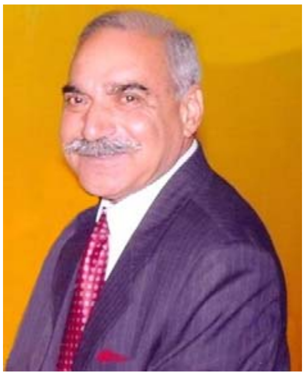
Terrorist attacks carried out by radical Islamist groups within the EU's borders are a concern and measures to prevent future catastrophic attacks must continue. However, as North Africa becomes a more significant supplier of energy to Western Europe, threats to the energy infrastructure in the region must also be considered. Attacks or threats against energy infrastructures can lead to uncertainty amongst market players and overall insecurity, thereby raising global energy costs and placing additional budgetary pressures on states and consumers. To counter this trend and the inflexibility of the current energy environment, states need to adopt a multifaceted approach.

Security of Vital Core Strategic Installations: Indian Perspective

By: Col NN Bhatia, Veteran

It is but our second nature not to learn from past mistakes, especially the ones that were grave like Kargil War, 26 /11 the last Pathankot episode that quickly followed the earlier 27 July 2015 Gurdaspur incident. In the northeast in Manipur the National Socialist Council of Nagaland – Khaplang (NSCN-K) group, ambushed the Army convoy on 4 June 2015 in which 18 soldiers were killed. Regretfully, after every such avoidable incident and loss of precious lives, scores of reams of paper are written on lessons learnt and forgotten before the next dastardly terrorist act is encountered and the vicious circle goes on & on!

Our response to terrorism, whether emanating from across our borders, or internal Left Wing Extremists & cyber terrorism need to be pro-active. Sine we are still reactive in appreciating, mobilizing and neutralizing various threats to our national security, creation of National Counter-Terrorism Centre (NCTC) is now seriously necessitated that will work under the Ministry of Home Affairs. Intimate coordination, training & sharing of real time actionable operational intelligence with the armed forces is lacking. In fact, having served both in the Army for over 32 years & nearly 8 years in the Intelligence Bureau (IB), I found both avoided each other. The plethora of agencies has created inter & intra rivalries and lack of coordination, thus, failing us in creating our pro-active and timely response even in last terrorist attack at Pathankot Indian Air Force (IAF)Base located so close to international border with Pakistan.



After retiring from the Army he joined Intelligence Bureau where for over 5 years he had undertaken Industrial Security Evaluation of large number of vital & strategic Public Sector Undertakings (PSUs) such as Aeronautics, Airports, Banks, Defence, DRDOs, Mints, Nuclear Energy, Oil, Power, Ports, Refineries etc. He also conducted numerous Industrial Security & Disaster Management Training Programs, Seminars, Workshops, and Exhibitions and has interacted with numerous Ministries, Departments & NGOs.

He was again appointed Industrial Security Consultant with MHA after 26 /11 and did numerous security audits of PSUs.

Presently he is freelance Industrial Security Consultant undertaking Industrial Security Audits, Reviews, Training & Advice in Disaster Management & handling of IEDs & Explosives.

He has vast experience in the management of the Human Resources, Training & Development, Liaison, Fire Fighting, Logistics, Equipment & Material Management, Strategic Decision Making Process, clearance of Maps & Aerial Photography (GIS), Explosives handling and Industrial Security & Disaster Management.

Five Commandments in Security Planning of Vital Installations

1. Firstly, Security should be based on threat perception & not for glamour or pomp or show**.**
2. Secondly, security should eliminate threats & crimes. White collar, cyber, internet & organised crimes occur on intrusion and misuse of detection systems.
3. Thirdly, security is neither permanent nor perfect as technologies obsolete very fast & modern day terrorists & criminals being very high tech-savvy evolve new methodologies to damage our installations. Management & security force must keep themselves abreast with fast changing technological developments to outwit criminals & terrorists in their game to harm us.
4. Fourthly, security systems should be cost effective, user friendly, in depth & easy to implement.
5. Fifthly, security systems should be periodically reviewed & audited by professionals to eliminate weaknesses & mid-course corrections. For training, development, advice & audit, experts need to be employed permanently.

Recommendations for Manning Security of Vital Installations

The National Security Management requires integrated approach & coordinated applications of the political, military, diplomatic, scientific, industrial & technological resources of the state to protect and promote national security goals and objectives. Therefore, 'Security of Vital Installations & Infrastructural Security' forms integral part of the National Security Management. Of late, multidimensional threats to national security have increased many folds from international terrorism, espionage, sabotage, subversion, internal conflicts, secessionism, communalism, strikes, emergence of white collar crimes and cyber terrorism. Technological advancements in Industrial Security have ensured access control, surveillance, detection and damage control more effective, accurate and timely.

Top Management and Security Officers cannot any more remain content with their preventive and physical security roles. They have to be proactive and upgrade their skills as terrorists and anti-national elements (ANEs) are using hi-tech equipment to destroy our vital installations. Contrary to the earlier notion that all expenditure on security was of 'no return on investment', Industrial Security has graduated from 'Guarding' or 'Watch-and-Ward' to all pervasive Asset Protection, Loss Prevention, Crime Control, Intelligence, Safety and Disaster Management!

Perimeter Security

- In the US & Israel perimeter is protected by multiple layers of concertina or chain link fences that are 8-10 feet high with 6 inches gap and poles 6 feet apart in between clipped together at intervals. Fence protection devices available are electric, electronics, electromagnetic, optic fibre cable, active infra-red, microwave intrusion alarms, seismic and sensors systems in various configurations. There are numerous miscellaneous openings like culverts, sewers, drain pipes, exhaust conduits, intake pipes, manhole covers etc. Any such opening having a cross-section area more than 96sqi or more must be protected by bars, grill works, barbed wire and alarms & vents doors with proper locking devices. 24x7 CCTV coverage and patrolling of such vulnerabilities need to be ensured.
- The CCTV System with toady's technologies which is thoughtfully installed with appropriate video analytics is force-multiplier. CCTV coverage of entire perimeter wall with correct video analytics make it a very effective tool for real time monitoring and for post-event investigations.
- While designing perimeter wall, the topography & ground configuration around the installation must be catered for. Undulating, dead ground, water channels, vegetation must be under constant surveillance & no trees, electric poles or tall buildings should be constructed within 20 meters either side of the perimeter as they hinder visibility, field of fire and also assist in scaling it. The area within the complex needs to be cleared of undergrowth and thick vegetation misused by miscreants to hide & store weapons, ammunition, explosives & stolen goods. Also, in summers, dry grass leads to fires.

Gates

Every opening in the perimeter barrier is a potential security hazard as more openings mean more deployment to protect them. Hence gates should be kept to minimum. Gates not used should be sealed, if not locked and manned.

- Area around the gates must be properly lighted with a dedicated phase of power supply & emergency lighting system.

- Sturdy construction to with stand ramming of explosive laden vehicle(s) by terrorists.
- Height of the gates should not be less than the perimeter wall.
- Anti-scaling devices should be fitted on gates to negate climbing over.
- Gates must be manned round the clock-ensure sentries in pairs in night and inclement weather. This is often not done on lesser used gates like emergency gate to economize on security manpower.
- The Security Control Room is well secured and located near the Main Gate and manned round the clock with duplicate communication, anti-sabotage checking equipment like HHMDs, DFMDs, explosive detectors, trolley mirrors with night capability, mobile ramp to check overhead carriage of trucks and buses, first aid box, loud hailer and alarm system.
- Fool proof system of issuing and collecting passes, escorting visitors, frisking and checking men and vehicles entering and exiting the installation. Access control is of paramount importance.
- CCTV monitoring console and car number plate reader with recording & play back facilities should be provided at gates.
- In larger installations there may be more than one gate and separate materials in and materials out gates that must be secured with necessary documentation.
- Manual /electronic barriers constructed to hinder free run of doubtful traffic.
- Speed breakers should be erected on either side to ensure vehicles slow down /stop while entering or exiting for thorough checking. Tyre busters in sensitive installations may also be installed.
- Security staff should be adequate with day's quick reaction team (QRT) located nearby for meeting any threat.
- Arms of guards must be secured with chains tied to belt to ward off arms snatching by the miscreants. Sentries must have whistle, baton & torch in night.
- Vapour Cloud Tracking & Detection System should be installed in sensitive, vulnerable areas to prevent fire in ATF & lubricants storage areas.

Perimeter Lighting

- Poles should be minimum 15-20 feet away from the perimeter wall with sufficient height with barbed wire rapped to prevent scaling.
- Thumb rule for lighting is that the inner areas should have 40% while area outside the perimeter should have 60% illumination so that miscreants cannot have clear view of installation from elevated structures while sentries at gates & watch towers have good night vision outside the perimeter.
- Power cables should be underground & junction boxes secured.
- Electrical equipment installed in sensitive installations should be approved by the national regulatory agency.

Access Control

Ineffective access control is perhaps the weakest link in the strategically important installations as large numbers of workers, families, contractors, vendors, AMC providers, maintenance staff and vehicles move in & out of the installation. Following need to be ensured:-

- The sensitive installation must be declared as 'Prohibited Place' under the Official Secrets Act, 1923 in India and under similar laws elsewhere and warning boards displayed to the effect in official /local language with maximum punishment for infringement mentioned to act as deterrent.

- Issue of biometric identity cards, visitor passes & visitor badges must be displayed physically.
- To ensure regular checking of identity cards & passes at the gates.
- HHMDs/ DFMDs/ Explosive Detectors need to be used for frisking of employees, labour, contractors, visitors, AMC staff & their vehicles.
- Over-head mobile ramps to check upper carriage of vehicles.
- Dog squad (sniffer & patrol) are always a welcome element of any security plan! Both handlers and animals must be trained.

Watch Towers

To enhance the physical security of the large perimeter, watch towers should be constructed laying emphasis on the following aspects:-

- Sited tactically with clear field of vision and fire with no dead ground in between. If there is dead ground or blind area it should be reinforced with barbed wire and concertina coil like obstacle system & kept under CCTV & patrolling surveillance.
- Manned 24x7-preferably in pairs in night/inclement weather and frequently visited by patrols.
- Height of the watch towers from ground should be 15-20 feet depending on the height of the perimeter wall and topography around the installation.
- Staircases of watch towers are so constructed to facilitate security guards to easily negotiate them during day and night with their arms and equipment.
- Provided protection from adverse weather conditions like heat, snow or rains. In insurgency environment they should provide sentries good field of fire, observation and protection from small arms fire and splinters.
- Have rest rooms with cots, toilet and water facilities.
- Provided duplicate communication and in mutual support of the neighbouring watch towers.
- Search lights with dedicated power supply, CCTV coverage, binoculars & night vision devices (NVDs) provided to optimize effective surveillance.
- Sentries perform 2-4 hours duty at a stretch. Beyond that is extremely tiring and not conducive to installation's security.
- Duty officer of the day and night must check the watch towers.
- Sentries manning the watch tower should never panic and inform Security Officer /Security Control Room and neighbouring watch towers if unusual development occurs.

Vehicle Parking

- After thorough anti-sabotage checking of vehicles & verification of drivers/helpers, only minimum essential vehicles be permitted parking inside the installation which should be close to the administrative block.
- Parking lots outside the perimeter should be close to manned gates with proper lighting along with toilet, rest room and canteen facilities for the drivers and helpers.
- Licences of drivers of the vehicles entering inside the complex must be checked and collected at gates and given back while vehicle exits installation. That is only feasible if one gate is only used for entry and exit and traffic is moderate.
- Ensure no vehicle is abandoned. If there is any such vehicle, police must be informed to tow it away.
- Vehicles without spark arrestors are not permitted in the vicinity of ATF stores/ refineries.

Surveillance Devices

- Day & night patrolling both within & outside the perimeter.
- Manning all watch towers normally not done to save on manpower expenditure.
- CCTV system with continuous day, night & adverse weather condition recording & play back.
- Installation of intrusion & fire alarms.
- Dog squad as discussed above.
- Cyber & communication security.
- Drones & aerial reconnaissance.
- Satellite imageries.

Security Force

Each installation must have three layered security so that if one is breached, unauthorized access is detected at the next two layers. In IAF base only Defence Security Force coupled with private security personnel were employed who are old, ill trained, physically unfit lacking motivation & zeal. There are large numbers of IAF installations, therefore, IAF need to raise their own dedicated well trained & equipped force with the state of the art weapons & equipment to protect their vital installations.

Character & Antecedent Verification of security staff is vital as lately many defence services and police personnel have been found involved in dubious activities. Men with certain character deficiencies & weaknesses for 3Ws (wine, women & wealth) are weeded out with disciplinary actions. Drugs, arms, narcotics & FICN lobbies have long compromised the police and para-military forces making the country's western and eastern borders porous. Now they are reportedly penetrating in the armed forces as incentive for making easy money are very high. What goes for security staff needs to be discreetly watched in other employees serving in sensitive installations close to borders.

Basic factors to be kept in mind while dealing with a terrorist attack

- Task of neutralizing terrorists is specialized one and undertaken only by trained military /police commando force.
- Terrorists are ruthless, well-armed and indifferent to consequences of their actions. Nothing be said or done to provoke them into violent action.
- Terrorists will be on look for targets like head of the installation or most sensitive /vulnerable equipment in the installation. So nothing should be said or done to give away to terrorists this special knowledge.
- Most of the terrorist threats are to induce fear. Therefore, while outwardly displaying fear, inwardly employees should confidence to neutralize such threats. Avoid panic and be calm. Quiet prayers and yoga help to remain calm.

Pro-active Steps (before the terrorists attack)

- Ensure trained security force & commandos are located inside the complex.
- Direct communication link from innocuous location with Security Control Room is maintained.
- Crisis Management Group (CMG) within the installation should handle all decision making tasks in a terrorist situation.
- An alternate Crisis Management Group with senior managers who normally work away from the installation may also be formed.

- Detailed physical plan of the installation with locations of vulnerable areas, buildings, doors, stairways, lifts, along with photographs would always be helpful to counter terrorist force to launch offensive against terrorists.
- With the cooperation of the police/ security forces locally located, a '**Terrorist Attack Contingency Scheme (TACS)** should be prepared.

Actions to be taken if terrorists attack

- Sound alarm and Immediately contact /inform head of the installation, nearest military unit, police, hospitals, blood banks, fire services, civil administration & adjoining installations.
- CMG immediately convened along with stand by CMG outside the plant. Only CMG should contact /brief outside security force, police and civil administration.
- Cordon installation and man traffic with own security staff till arrival of the specialised commando/ security force.
- Evacuate non-essential vehicles and personnel to prevent injury and loss of life in an orderly manner.
- Assist specialised police /military force in encircling the terrorist infested area in the installation to confine and neutralise them.
- No attempt by employees or installation's security personnel should be made to encircle terrorists. Clumsy attempts will provocative terrorists to fire and inflict avoidable causalities.

Integration of Security Technology

Integration of Security Technology in any installation under potential terrorists' threat should be cost effective and user friendly. The necessity of integrating the various sub-systems in the Central Control Room is as under:-

- Access Control Mechanism
- CCTVs with Centralized Control mechanism.
- Alarms & alarms monitoring including fire-fighting.
- Biometric ID badging.
- Perimeter or fence intrusions detection system.
- Intercom (video & sound).

CCTV system acts as **'eyes and ears'** to the security system. The role of alarms, access control & perimeter systems are to detect, restrict & control movement of people. The system integration should be done in multimedia mode using graphic user interface (GUI). Before going for integration technology, a detailed feasibility survey by electronic, IT, fire safety and security experts to design a cost effective and user-friendly system should be undertaken. Though not discussed, buildings, cyber, documents & personnel security will always be dove-tailed in the security management of vital installations.

ICISS at LinkedIn: http://www.linkedin.com/groups?gid=4413505&trk=hb_side_g
ICISS at Google Group: https://groups.google.com/forum/?fromgroups#!forum/icissm

Suggestions & feedback may be sent to us on e-mail: onlineicissm@gmail.com

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address and we will move it out from our contact list, thank you!

Forthcoming Event:

INDIA RISK SURVEY 2016

India Risk Survey is an attempt to analyse and quantify 'potentially destructive' risks to business enterprises in India. It would provide a referral to understanding the complexity of these risks across a spectrum of stakeholders, i.e., policymakers, corporate and members of the civil society. The survey would help in sensitising the Government and the corporate world about emerging risks and the danger they pose, so that a well-planned strategic policy decision could be formulated and implemented.

Your participation would help us in conducting a comprehensive study

For participation please log on to **http://irs.pinkertonindia.com**

Contact Us

Mr. Sumeet Gupta (Director)
Mr. Ankit Gupta (Sr. Asst. Director)

FICCI, Federation House, Tansen Marg
New Delhi - 110 001

Tel: +91 - 11 - 23738760-70 Ext: 212
Fax: +91-11-23320714, 23721504
Emails: sumeet.gupta@ficci.com
ankit.gupta@ficci.com

Knowledge Partner

PINKERTON®

Supported by

ICISS ASIS

Media Partner

IMR