Protective Information & Intelligence (Concepts, methods, tactics)

Insight

Information/intelligence is a **"Progressive Force"** in the business **"Battlefield"**.
The vision of information/intelligence is at our fingertips, at any given time or place, which both induces and slows down processes. It is the dream of each and every businessman and organization, whether public or institutional.

Everything begins when information/intelligence falls into the right or wrong hands, and thus influences the process of decision making.

Information/intelligence of this kind can lead to the **rise** or **fall** of corporations and organizations, may hinder business transactions, or alternatively, may give a critical advantage to the opposition and competition.

The **Nightmare** of any leader/manager/owner is the threat of **infiltration** of competitors from outside into one's inner-circles and into the home environment – discussions, decisions, professional secrets, conversations, phone calls (linear, cellular, fax), bids, computer, vehicle and relations with home & family.

The major and immediate advantage in the competitive intelligence world is the placement of prevalent, tight security of information/intelligence ones business or organization, able to identify and nullify the numerous and varying threats of which we are unaware in our everyday routine, thereby preventing tremendous damage to ones business, organization and to oneself as a manager/owner, on the personal level.

Critical information/intelligence is worth a lot. Companies, institutions and organizations invest vast sums in two parallel channels:

- Keeping existing information/intelligence from leaking out, thus preventing a significant advantage to the opposition
- **Obtaining** information/intelligence in order to gain an advantage over the competition/ opposition, according to the universal saying:

"The best defense is offense"

OUR PROACTIVE CONCEPT

Security in terms of protection and collection of information/intelligence can be defined as an array of protection circles. At the core of this array is a combination of procedures, skills and advanced technologies. The outer circles must account for all aspects of physical security, including entry control, communications control and infrastructure (linear, data, cellular), computer systems and network infrastructure, departmentalization, employee control, guest control, internal and external maintenance control as well as issues such as organizational awareness and employment of tools for gathering information.

The ability to recognize and define imminent threats to the assets one is protecting, and to decide on an appropriate operational response is essential.

PROFESSIONAL EXPERIENCE

True professional experience in the field of information/intelligence protection is both rare and unique. Our professional experience has been accumulated through years of service in various branches of the Israeli security establishment.

This session will provide an overview of intelligence gathering and countermeasures, which covers strategic and tactical intelligence as the Israeli intelligence specialist from the civil and law enforcement communities understands it, as well as the broad issues involved with competitive intelligence and countermeasures.

SYLLABUS

Operative intelligence gathering methods

Module - “HUMINT - The Human Side of Intelligence”

This module will focus on the human factor in the collection of intelligence. It will cover both open and clandestine sources of information.

- Open sources of information include newspapers, magazines, commercial news clipping services, court transcripts and filings, libraries, and public records.
- Clandestine sources will analyze the history and current status of undercover agents, their recruitment, training, management, evaluation and control.
- Before the gained information can be put to work for the organization’s relevant departments, verification is necessary to ascertain its accuracy.
- Undercover activity: Building and adapting a cover, protection against undercover operators.
- Operative actions: Covert searches + information gathering from target +obtaining documents
- Recruitment and “running” of operatives: Finding, recruiting, and “running” the candidate.
- How to prevent mishaps, pre-hiring checks.
- Planting an operative: How it is done?

Module - Surveillance

In this module the student will get acquainted with the techniques of physical and technical surveillance, for the purpose of obtaining information and/or evidence while conducting an investigation. The student will learn the difference between covert vs. overt surveillance and the means by which they are carried out depending upon the situation.

The module will cover the various methods used in the field as well as the applications of modern technology to expand the field agent's reach.

- Covert vs. overt surveillance
- Types of surveillance
- Preparation
- Observation - day/night, quiet/crowded area, urban/suburban area
- Surveillance on foot and per vehicle
- Stationary surveillance and observation posts
- Operational disguises and make-up
- Communication - overt/covert, concealed on person or in vehicle, familiarity with equipment and its operation
- Surveillance technology
- Identification - by picture or description
- Report writing

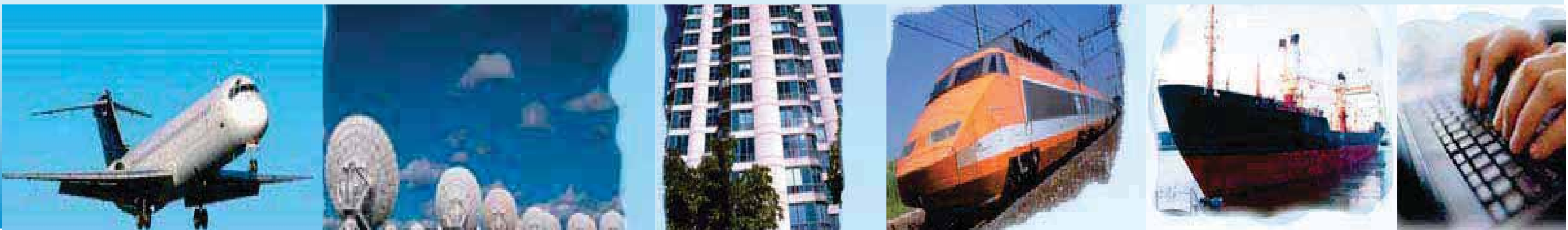
Module – Technical surveillance equipment & electronic countermeasures

In this module, different surveillance methods will be reviewed, including mechanical, electronic, visual and optical attacks. Mechanical attacks comprise everything from tape recording to physical capture of the information through oral or written form. Visual and optical attacks perhaps present the most common, least suspected form of intelligence collection.

- Various countermeasures to RF and wave transmitters, including infrared, laser and air techniques for intelligence collection.
- Detection, through systematic methods of conducting a physical search, electronic countermeasures and nullification including a practical understanding of how to conduct electronic sweeps to detect radio transmitters.
- How to conduct a physical search.
- Nullification of all surveillance methods.

Module – Phone line tapping countermeasures

1. Basic electricity and measurement, transmitters, overt and clandestine, telephone analyzers, and non-linear junction detectors.
2. Electronic switching systems, central office procedures, telephone testing, line tapping and tracing.
3. Telephone system design, security practices, and devices like scramblers.
4. Effective methods of nullification and all methods of telephonic intercepts.



Module - Covert video technology and sting operations

This module will teach the student basic theory, application and the technology available for covert video surveillance.

- Equipment, from light source to final monitoring, recording and printing for legal documentation.
- Developments in video technology miniaturization and remote transmission, video motion detectors, VCRs and frame storage devices.
- The practical application of video surveillance in retail stores as well as open-air surveillance.
- "Sting operations": how they are set up, site selection, security operatives, video camera selection and operation, identification of suspects, evidence preservation and documentation. (While the course is focused on criminal surveillance for the law enforcement community, there are numerous private security applications of sting operations).

Module - Electronic tracking technology

- Tracking theory and its application in an urban environment, field-tracking problems, placement of transmitters, and re-acquisition of lost signals.
- New technologies and their potential use in the security field such as satellite communication networks. Such technologies have potential use for tracking everything from stolen property to kidnap victims.

Module - Computer intelligence collection and security - Cyber security

Intelligence collection by computer is a rapidly expanding technology and service that is readily available to a growing number of private investigators, security officers and law enforcement investigators.

This module will cover many databases that can be accessed by computer, including: personal and business records, assets location and local address searches.

- The essentials of computer security, including security software programs, operational security systems, protection of hardware devices, protection of software and data, transmission security, audit trails and standard practice procedures for computer systems.

Module – Surveillance detection – concepts, methods and tactics
Module – Social engineering
Module – Information gathering methods & means
Module – Questioning, overt- covert, interrogation
Module – Information Protection methods & means

Module – Internal security

This module will cover issues including personnel, document and physical security.

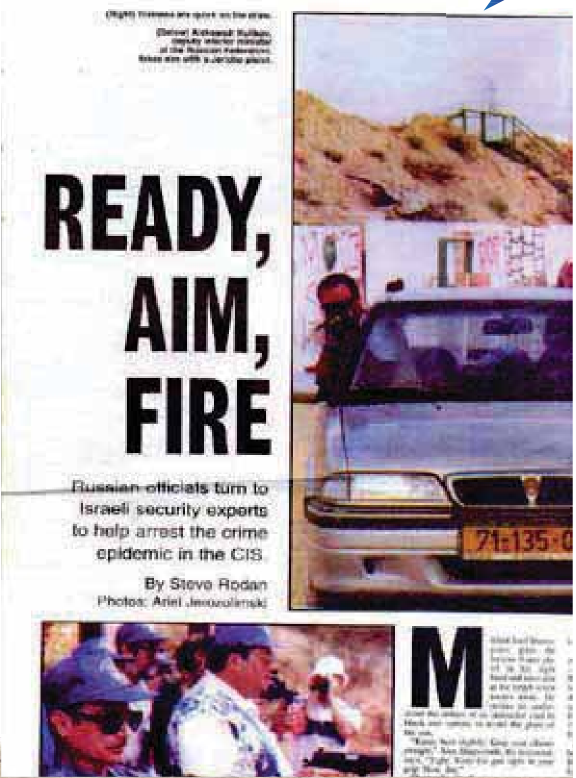
- Personnel security refers to the policies and procedures intended to determine that an individual is not currently a security risk, and are not likely to become one. A personnel security program is intended to prevent criminal activities by employees, espionage attempts by external intelligence forces and unintentional acts by employees that could lead to a compromising situation.
- Document security, classification management, reproduction, disposal and transmission of sensitive or classified documents.
- Physical security includes issues like access control, security patrols, personnel identification and visitor control, as well as methods of detecting unauthorized intrusion or activity, alarm systems and facility clearances.

Module – Simulative drills and practice of information, Data and knowledge planning (field exercises)

Very Important Issues

- Intelligence & Information
- Deception & Concealment
- Deterrence
- Secrecy & Confidentiality

Simulation drills and practices (field exercises)



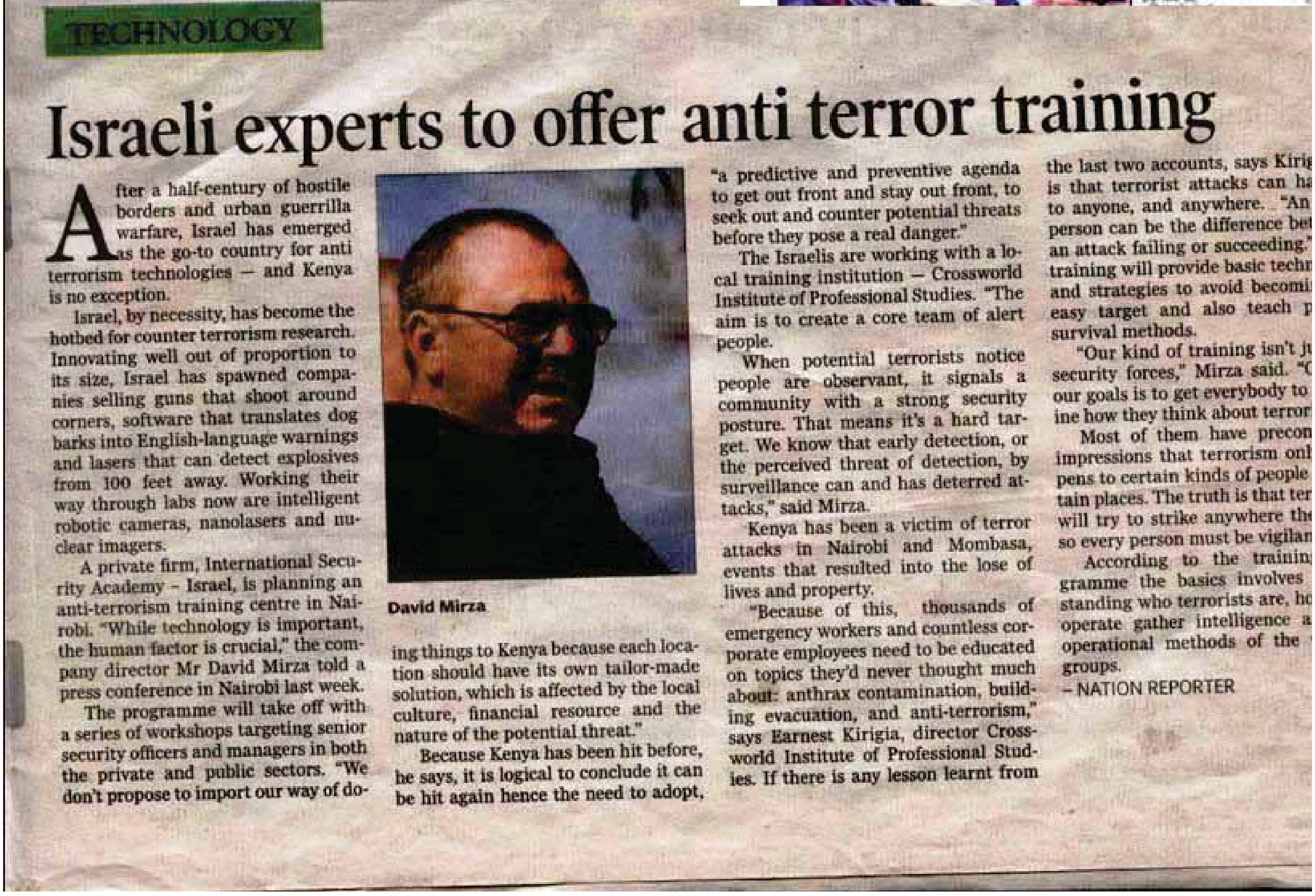
READY, AIM, FIRE

Russian officials turn to Israeli security experts to help arrest the crime epidemic in the CIS.

By Steve Rodan

Photos: Ariel Jerozolimski

M [illegible]



TECHNOLOGY

Israeli experts to offer anti terror training

After a half-century of hostile borders and urban guerrilla warfare, Israel has emerged as the go-to country for anti terrorism technologies — and Kenya is no exception.

Israel, by necessity, has become the hotbed for counter terrorism research. Innovating well out of proportion to its size, Israel has spawned companies selling guns that shoot around corners, software that translates dog barks into English-language warnings and lasers that can detect explosives from 100 feet away. Working their way through labs now are intelligent robotic cameras, nanolasers and nuclear imagers.

A private firm, International Security Academy - Israel, is planning an anti-terrorism training centre in Nairobi. "While technology is important, the human factor is crucial," the company director Mr David Mirza told a press conference in Nairobi last week.

The programme will take off with a series of workshops targeting senior security officers and managers in both the private and public sectors. "We don't propose to import our way of doing things to Kenya because each location should have its own tailor-made solution, which is affected by the local culture, financial resource and the nature of the potential threat."

David Mirza

Because Kenya has been hit before, he says, it is logical to conclude it can be hit again hence the need to adopt, "a predictive and preventive agenda to get out front and stay out front, to seek out and counter potential threats before they pose a real danger."

The Israelis are working with a local training institution — Crossworld Institute of Professional Studies. "The aim is to create a core team of alert people.

When potential terrorists notice people are observant, it signals a community with a strong security posture. That means it's a hard target. We know that early detection, or the perceived threat of detection, by surveillance can and has deterred attacks," said Mirza.

Kenya has been a victim of terror attacks in Nairobi and Mombasa, events that resulted into the lose of lives and property.

"Because of this, thousands of emergency workers and countless corporate employees need to be educated on topics they'd never thought much about: anthrax contamination, building evacuation, and anti-terrorism," says Earnest Kirigia, director Crossworld Institute of Professional Studies. If there is any lesson learnt from the last two accounts, says Kirig is that terrorist attacks can ha to anyone, and anywhere. "An person can be the difference be an attack failing or succeeding." training will provide basic techn and strategies to avoid becomi easy target and also teach p survival methods.

"Our kind of training isn't ju security forces," Mirza said. "C our goals is to get everybody to ine how they think about terror

Most of them have precon impressions that terrorism onl pens to certain kinds of people tain places. The truth is that ter will try to strike anywhere th so every person must be vigilan

According to the trainin gramme the basics involves standing who terrorists are, ho operate gather intelligence a operational methods of the groups.

– NATION REPORTER

SECURITY MANAGEMENT & LEADERSHIP INSTITUTE
I.S.A
ISRAEL
1987

I.S.A INTERNATIONAL SECURITY ACADEMY

THREAT ASSESSMENT, SECURITY, PROTECTION PLANNING & OPERATION

№

Homeland Security
Protection Management
If You want to be considered the Best
You should train with the Best!

Assessment Planning, Operation & Management

Syllabus

Module - The Private Security Industry and its role in the struggle against violent crime & Terrorism.

Module - The "Adversary"

- Familiarization with potential adversaries
- Adversary motives
- Adversary objectives
- Adversary modus operandi

Module - What is terrorism?

Understanding Terror from Within: Applying Anthropological Knowledge to Challenge Security Threats"

Module - Arab/Islamic Terrorism

Familiarization with Arab/Islamic culture, radical Islam, religion, manners and language, Sunni VS Shiite

Module - The potential Terrorists

- Types of terrorism
- Motives
- Objectives
- The terrorism modus operandi
- Suicide terrorism

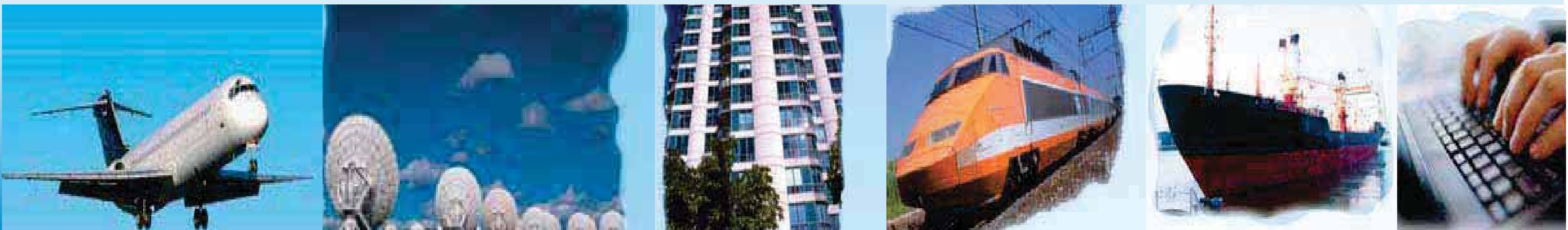
Module - International Crime & Terrorism

- Types of International Terrorists
- Types of International crime organzations
- Narco-terrorism, Anarchist, Left-Winged, Right-Winged, Militia Movement, Nationalist, Communist, *State-Sponsored Terrorism
- Case Studies

Module – Threat assessment, Protection assessment and protection planning

The Protection Array

- The goals of the security array
- The level of security
- Parameters for ascertaining Security Level
- The Protective effort depends upon:
- Security Situations
- Methods of Security
- Security Actions



Module - VIP protection concepts, methods & tactics

Module - Sensitive installation's protection

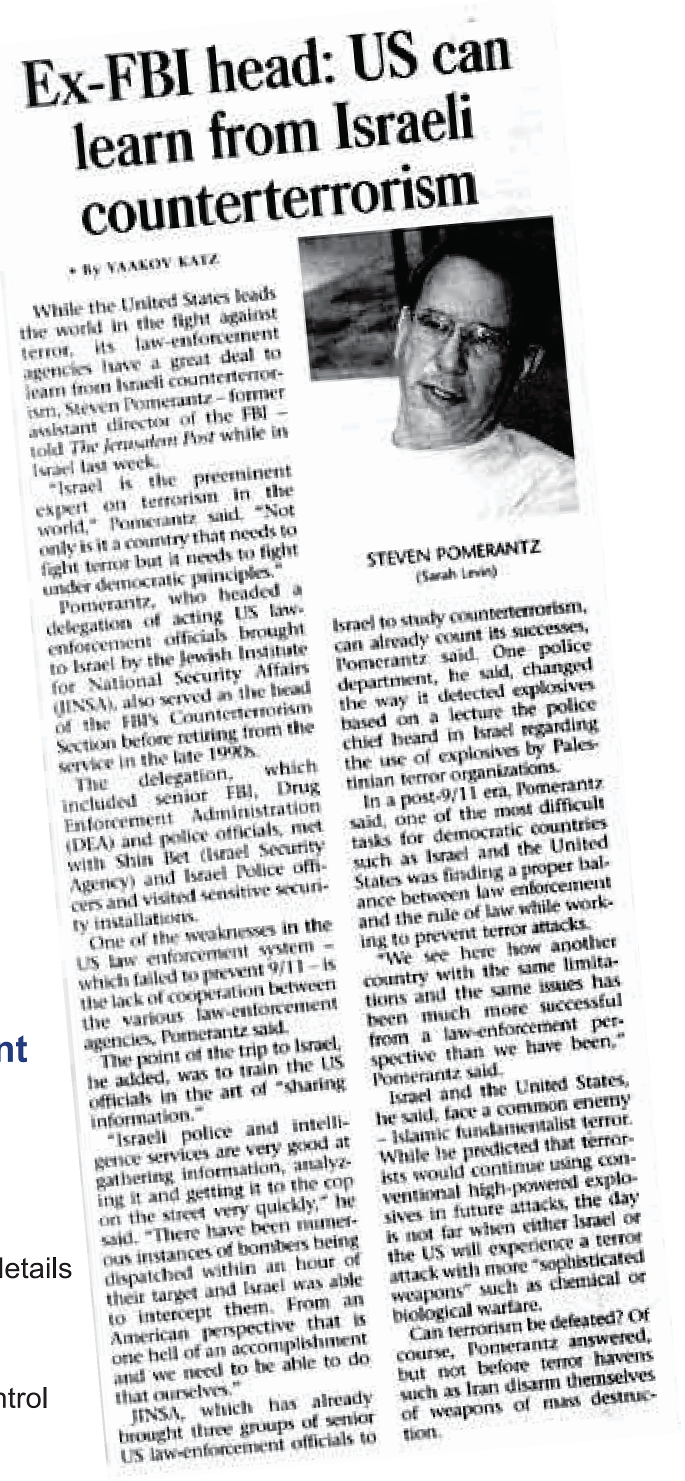
- Fixed installation
- Residence
- Points regarding apartment
- Plans and drawings needed
- Private Home
- Temporary Installation
- Venue file
- Security survey
- Risk analysis
- Vulnerability assessment

Module - Physical Protection

- Methods of Security
- Physical protection
- Physical protection circles
- Security system's structure
- Warning, detection & deterrence
- Delay & entry prevention
- Response array
- Communication system
- Control & Supervision, How to do it?
- Physical Means
- Routine Procedure

Module - Special events protection planning & operational management

- Types of Events
- Characteristics of Events
- Security tasks during an event
- The event security plan
- Coordination Meeting Preparations, stages, details
- Operations
- Emergency situations
- Emergency situations evacuation & crowd control



Ex-FBI head: US can learn from Israeli counterterrorism

• By YAAKOV KATZ

STEVEN POMERANTZ
(Sarah Levin)

While the United States leads the world in the fight against terror, its law-enforcement agencies have a great deal to learn from Israeli counterterrorism, Steven Pomerantz – former assistant director of the FBI – told *The Jerusalem Post* while in Israel last week.

"Israel is the preeminent expert on terrorism in the world," Pomerantz said. "Not only is it a country that needs to fight terror but it needs to fight under democratic principles."

Pomerantz, who headed a delegation of acting US law-enforcement officials brought to Israel by the Jewish Institute for National Security Affairs (JINSA), also served as the head of the FBI's Counterterrorism Section before retiring from the service in the late 1990s.

The delegation, which included senior FBI, Drug Enforcement Administration (DEA) and police officials, met with Shin Bet (Israel Security Agency) and Israel Police officers and visited sensitive security installations.

One of the weaknesses in the US law enforcement system – which failed to prevent 9/11 – is the lack of cooperation between the various law-enforcement agencies, Pomerantz said.

The point of the trip to Israel, he added, was to train the US officials in the art of "sharing information."

"Israeli police and intelligence services are very good at gathering information, analyzing it and getting it to the cop on the street very quickly," he said. "There have been numerous instances of bombers being dispatched within an hour of their target and Israel was able to intercept them. From an American perspective that is one hell of an accomplishment and we need to be able to do that ourselves."

JINSA, which has already brought three groups of senior US law-enforcement officials to Israel to study counterterrorism, can already count its successes, Pomerantz said. One police department, he said, changed the way it detected explosives based on a lecture the police chief heard in Israel regarding the use of explosives by Palestinian terror organizations.

In a post-9/11 era, Pomerantz said, one of the most difficult tasks for democratic countries such as Israel and the United States was finding a proper balance between law enforcement and the rule of law while working to prevent terror attacks.

"We see here how another country with the same limitations and the same issues has been much more successful from a law-enforcement perspective than we have been," Pomerantz said.

Israel and the United States, he said, face a common enemy – Islamic fundamentalist terror. While he predicted that terrorists would continue using conventional high-powered explosives in future attacks, the day is not far when either Israel or the US will experience a terror attack with more "sophisticated weapons" such as chemical or biological warfare.

Can terrorism be defeated? Of course, Pomerantz answered, but not before terror havens such as Iran disarm themselves of weapons of mass destruction.

Module - Aviation Security

Module - Chemical, Biological, Radiological, Nuclear security

Module - Protection Plan & Operation Order

Module - Managerial subjects

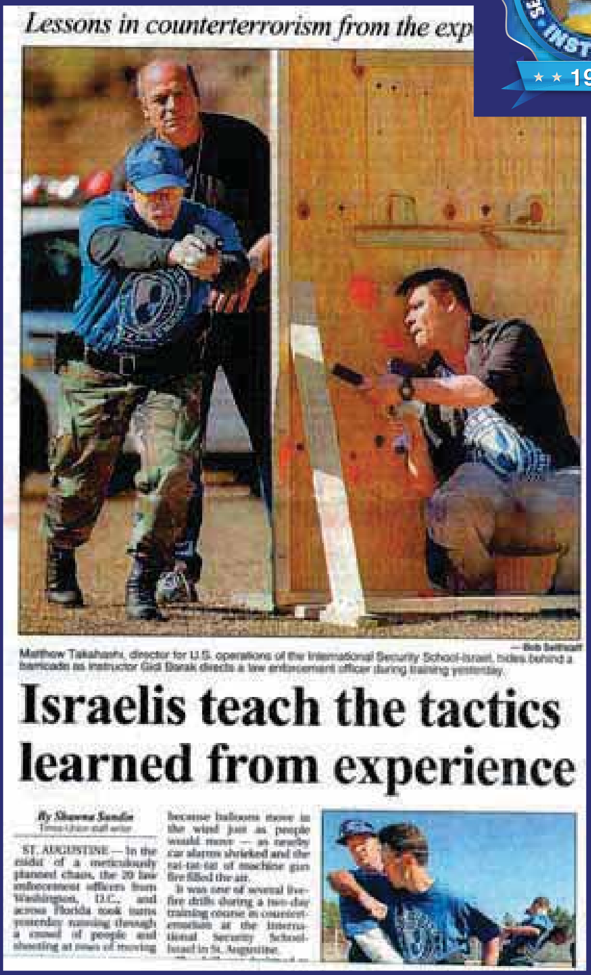
- Tactical thinking
- Information & intelligence gathering
- Information security-basic principles
- Targeted analysis-residence, office
- Operational analysis-“Scene of action”
- Risk assessment and situation analysis
- Coordination meeting
- Security of groups, conferences and delegations
- Planning the protective effort
- The operation plan
- The operational deployment
- Decoy and deception
- Information security
- Procedures - routine & emergency
- Coping with high stress situations-methods
- Briefing and debriefing

The command post-control - Communication

- Operations center/room/car/helicopter/ Equipment
- General requirements
- Operation orders
- Operational duties

Module – Practical acquaintance with:

- Israeli Tactical Response Methods
- Israeli unarmed combat method (Krav Maga)
- Israeli Instruction Methods for Protection Personnel
- Instruction & Education
- Drills Planning
- Types of drills
- Tabletop drills
- Surprise reaction drills
- Pre-planned drill (simulation)
- Control & supervision



Lessons in counterterrorism from the exp

— Bob Self/staff

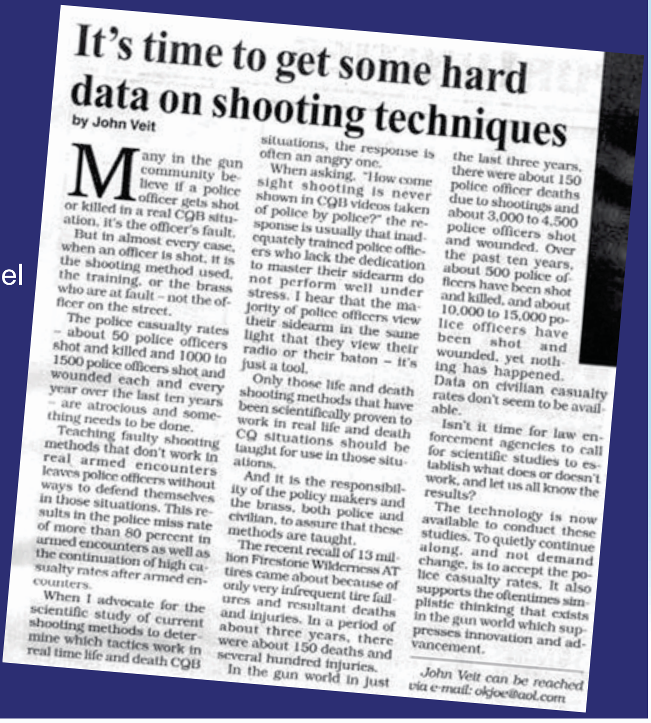
Matthew Takahashi, director for U.S. operations of the International Security School-Israel, hides behind a barricade as instructor Gidi Barak directs a law enforcement officer during training yesterday.

Israelis teach the tactics learned from experience

By Shawna Sundin
Times-Union staff writer

ST. AUGUSTINE — In the midst of a meticulously planned chaos, the 20 law enforcement officers from Washington, D.C., and across Florida took turns yesterday running through a crowd of people and shooting at rows of moving because balloons move in the wind just as people would move — as nearby car alarms shrieked and the rat-tat-tat of machine gun fire filled the air.

It was one of several live-fire drills during a two-day training course in counterterrorism at the International Security School-Israel in St. Augustine.



It’s time to get some hard data on shooting techniques

by John Veit

Many in the gun community believe if a police officer gets shot or killed in a real CQB situation, it's the officer's fault.

But in almost every case, when an officer is shot, it is the shooting method used, the training, or the brass who are at fault – not the officer on the street.

The police casualty rates – about 50 police officers shot and killed and 1000 to 1500 police officers shot and wounded each and every year over the last ten years – are atrocious and something needs to be done.

Teaching faulty shooting methods that don't work in real armed encounters leaves police officers without ways to defend themselves in those situations. This results in the police miss rate of more than 80 percent in armed encounters as well as the continuation of high casualty rates after armed encounters.

When I advocate for the scientific study of current shooting methods to determine which tactics work in real time life and death CQB situations, the response is often an angry one.

When asking, "How come sight shooting is never shown in CQB videos taken of police by police?" the response is usually that inadequately trained police officers who lack the dedication to master their sidearm do not perform well under stress. I hear that the majority of police officers view their sidearm in the same light that they view their radio or their baton – it's just a tool.

Only those life and death shooting methods that have been scientifically proven to work in real life and death CQ situations should be taught for use in those situations.

And it is the responsibility of the policy makers and the brass, both police and civilian, to assure that these methods are taught.

The recent recall of 13 million Firestone Wilderness AT tires came about because of only very infrequent tire failures and resultant deaths and injuries. In a period of about three years, there were about 150 deaths and several hundred injuries.

In the gun world in just the last three years, there were about 150 police officer deaths due to shootings and about 3,000 to 4,500 police officers shot and wounded. Over the past ten years, about 500 police officers have been shot and killed, and about 10,000 to 15,000 police officers have been shot and wounded, yet nothing has happened. Data on civilian casualty rates don't seem to be available.

Isn't it time for law enforcement agencies to call for scientific studies to establish what does or doesn't work, and let us all know the results?

The technology is now available to conduct these studies. To quietly continue along, and not demand change, is to accept the police casualty rates. It also supports the oftentimes simplistic thinking that exists in the gun world which suppresses innovation and advancement.

John Veit can be reached via e-mail: okjoe@aol.com

Module - Leadership/ Management

Practical workshop intended for Managers who operate Protection operatives involve in High Risk tasks.

- Basic theories of management/ Leadership.
- Principles of management/. Leadership
- Management and leadership (types of managers and types of leaders).
- Basic concepts of management and organization.
- Methods and techniques for recruitment of employees: interview, admittance exam, practical exam.
- Recruitment, classification and absorption of employees: dividing human resources according to suitable abilities and required skills for the job, suiting the employee to his job/task according to his abilities and the demands.
- Instruction: Planning in advance.
- Instruction methods and techniques (advanced level).
- Managerial effectiveness (result test).
- Motivating employees.
- Decision making.

Module - Simulation exercises and practice of preparation of assessment planning of protection arrays of the various security sectors

- Practical workshop intended for Managers who operate Protection operatives.
- Basic theories and principles of management/leadership.
- Basic concepts of management and organization.
- Methods for recruitment of employees: interview, admittance exam, practical exam.
- Recruitment, classification and absorption of employees: dividing human resources according to suitable abilities and required skills for the job, suiting the employee to his job/task according to his abilities and the demands.
- Instruction: planning in advance.
- Instruction methods and techniques (advanced level).
- Managerial effectiveness (result test).
- Motivating employees.
- Decision-making
- Modesty and Leadership abilities