International Council For Industrial Security & Safety Management

Newsletter: November 2012

Let's professionalize the professionals...

http://www.wix.com/sbtyagi/iciss

Better Security Sense...

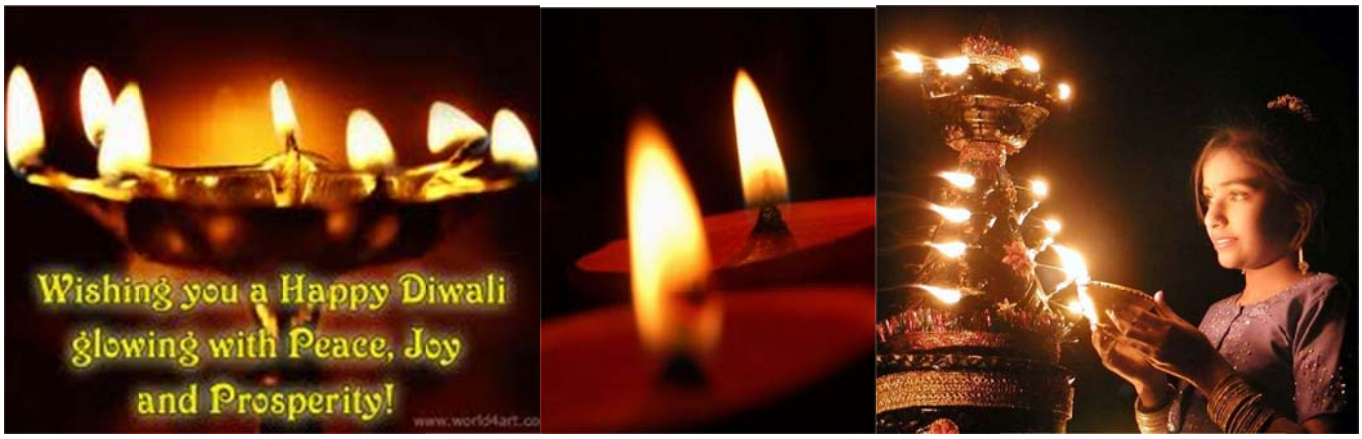
The most essential quality, which we have but ignored, is the power of observation.

We see but we don't observe. Observation is not just seeing thing but understanding the implications of what we see. So effective observation of what goes on around us is a very important requirement for better security sense. Wherever you are, be it at home or outside in a public place look around and try and see through things rather than just see them.

Try and gauge the need for a thing to be present at a particular place, for a person to be standing at a particular place. Don't ignore anything that seems unusual. Pry harder and you will come out with surprising results. Make observation a habit.

'Festival of Lights' celebrated in India with fervor is round the corner! Its message has universal appeal and application – victory of light over darkness, victory of good over bad! Let there be light to lead all on virtuous path!

Capt S B Tyagi
For ICISS



Private Security Guard: Use of licensed weapons while on duty

Capt SB Tyagi, COAS'CC**, FISM, CSC

There is lack of consensus in Man-guarding industry and the Users regarding the arms licensing requirements and conditions in the Private Security Agencies Regulation (PSAR) Act 2005. While the Act does not recognize armed guarding services as a distinct category of service, the increasing demand for armed security is leading to unregulated and random employment of individuals as private security guards who hold personal licenses. Ironically, while the PSAR has nothing defined, the Arms Act, 1959, only allows individual applicants to hold arms licenses. As a result, private security agencies have been compelled to employ people who hold Arms License in individual capacity.

About this prevailing situation **Capt Arvind Mahajan**, **Senior VP at Reliance Infra (**http://in.linkedin.com/pub/arvind-mahajan/30/208/b16**)** questions –

> "The weapon that a guard carries, strictly speaking is for HIS PERSONAL PROTECTION. It is by default that the installation (where such a guard carrying his personal weapon, meant for his personal protection), gets armed protection. But, can we as Principal Employer ask vendor agencies to provide us Armed Guard?"

To this **Col. Satendra Kumar CPO, CPO (I), G. M. (Training) at G4S Security Services** (http://in.linkedin.com/pub/satendra-kumar-cpo-cpo-i/16/88b/57b) says –

> "Yes anyone with valid license can use his weapon in self- defense but onus of proving that use of weapon was in Self Defense lies with the person using it. Now next question is what is self-defense? If a suspected criminal is without any weapon and only trespasses on a private property can the ASG use his weapon? You be rest assured criminal with intent of committing a crime will never come with a double or single barrel gun visible from miles! He will come with a concealed weapon and use it at point blank. There are very ifs and buts and unless law specifies legal authority it is difficult to bail out an ASG if he uses weapon. Surely no client will come in his support even when he has used weapon to save client's life!"

For issues relating to security guards using weapons while on duty, we need to understand the scope of Right to private defense as defined in section 96 & 97 of Indian Penal Code, which provides that -

- Nothing is an offence which is done in the exercise of private defense [There are some restrictions in the Sec 99]
- Every person has a right to defend his own body and the body of any other person, against any offence affecting the human body.
- Every person have a right to defend the property whether movable or immovable, of himself or of any other person, against any act which is an offence falling under the definition of theft, robbery, mischief or criminal trespass, or which is an attempt to commit theft, robbery, mischief or criminal trespass.

Thus we know that as a law abiding citizen any security guard who is on duty with his licensed weapon can use his weapon in exercise of his right to 'private defense, even when his employer doesn't order him to do so or even when scope of his employment or jurisdiction of duty does not provide so. In fact it is not only expected of him, but is also his duty as law-abiding citizen to use the licensed weapon while preventing attempt or commitment of crime. We also further need to study the scope of grant of arms' licenses under Indian Arms Act, which in very clear terms is for the purpose of 'private defense'.

About armed security guards there is reference in PSAR Act 2005 in Section 2, Subsection (a) which says that –

> "Armored car service" means the service provided by deployment of armed guards along with armored car…"

Further, Section2, Subsection (h) says that –

> "Private security guard" means a person providing private security with or without arms to another person or property or both and includes a supervisor."

Surprisingly there is no reference of armed security guards or the definition in PSAR Rules 2006. Thus we have to understand the scope of duties and validity of using licensed arms under Arms Act 1959 and also understand 'Right to Private Defense' as defined in Indian Penal Code (Section 96 onwards) especially on 'use of force'.

Under the Arms Act 1959, the arms licenses are issued but no specific purposes are enumerated for obtaining the licenses. It is only inferred that the arms under licenses are to be used in exercise of 'Right to Private Defense' (ROPD) or for 'sports' or special reasons such as cinematography. Hunting is not permitted anymore and thus only sport left is marksmanship. Good news is that Arms Act 1959 does provide in its Section 40 the protection of action taken in good faith. It says that, "No suit, prosecution or other legal proceeding shall lie against any person for anything which is in good faith done or intended to be done under this Act."

At this point **Arvind Mahajan, Sr. VP at Reliance Infra** is in quandary and he says -

> "Knowing fully well that the Armed Guard has the weapon for his personal protection -- Is it right to call him an Armed Guard? (I am not going into ROPD provisions - whether he fires or not, that's immaterial). But, Can I deploy him as an Armed Guard? How do I differentiate his duties from the unarmed Guard?

His predicament goes further,

> "How does one justify that an Armed Guard needs to be paid extra? Aren't we by default admitting that he is being deployed for providing Armed Protection, which as per Arms Act he is not supposed to provide? The individual got an Arms License, because he convinced the authorities of threat to his life, and NOT for performing an Armed Guard duty."

There were times when organizations or the companies used to get Arms Licensees under retainer ship basis (Section 13 of Arms Rules 1962), under which the licenses were issued on the name of the company and the arms were to be used by notified persons of the organization or the companies. These licenses were found to be cumbersome to obtain and had inherent

difficulties for the actual license holder in some case a busy director or the rich owner of a factories since there was Section 33 of Arms Act 1959 which held them responsible for action by the retainers of the licenses.
The Section 33 of Arms Act says, "

> "Offences by companies.-(1) Whenever an offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge of, or was responsible to the company for the conduct of, the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly."

Maj. Dhiman Bose, VP of TigerSwan India (http://in.linkedin.com/pub/dhiman-bose/22/456/739**)** has valuable recommendations for security agencies which they must follow –

- Ask all the personnel with arms to have their license to be entered in the local police jurisdiction - now this takes time and the police station carries out a verification of their license from the jurisdiction and the issue of license place. It needs leg work and money to get the process done.

- Once the gun entry is made in the nearest police station the individual with his weapon is summoned by the Local Arms DEPT.(POLICE HQ) where the same is cross checked, that the license is genuine and the All India permit is true,-- liaison acts by the security agency is must.

- Once these two things are in place the person can display his weapon when standing guard. A register is kept by the organization regarding the duty/ shift. The roving police/ beat constables do come and check this against the gun number and license.

Thus armed security guard is a guard who performs his duties while carrying his licensed weapon, for which he might be paid extra. Neither his employer nor his principle employer will have any legal control over his decision to use his weapon nor can these be contractual obligation. He would be well within his legal right to refuse use of his weapon on the orders of his employer / principle employer. It will be his and only his decisions to use or not to use his licensed weapon in any given circumstances.

The need to amend the Arms Act, 1959 has been long since felt and time to press for amendment in the Act has come! My understanding of the Arms Act and the PSAR Act as of now is that the arms licenses are issued for exercising right to private defense of self or other person and that of property of self or other person. When to use the weapon and how to use is purely at the discretion and wisdom of the holder of the weapons and of the license. No third party can give the holder of the weapon / license on how and when to use the firearms. Arms' licenses and weapons as of now cannot be used for earning livelihood. Indian law doesn't provide for 'guns-on-hire'. The security agencies having 'armed security guards on hire' can be easily treated by police officers as 'mercenaries armies' since law doesn't provide for such usages.

I would therefore like to summarize that the PSAR Act 2009 has been hastily drafted and leaves much to desire! I often said in the presence of past Joint Secretary (Police Modernization), Ministry of Home Affairs, who is the official directly concerned with the PSAR Act that "this Act has been apparently written by the police officer to retain police control over the act and it

appears to be so superfluous that even the broad headings are not explained properly!" Interestingly even when PSAR Act 2005 provides for lot many things, it nowhere clarifies whether security guards are to be treated as skilled, semi-skilled or non-skilled workers. The Labor Department's gazette notifications on minimum wages mentioned the categories of 'watch and ward duties' besides other but do not have 'security guard', 'armed security guard' as categories. Unfortunate part here is that even 'Watch and Ward' services are duties are not defined in any Act or the Order!

Emerging Security Trends

The nature of world-wide espionage is currently experiencing a dramatic shift.

A recent analysis of trends suggests the need to redefine the problem and to develop new strategies to combat growing threats to national security from economic intelligence gathering and corporate espionage.

If left unchecked, analysts estimate losses could grow an additional 50% by the year the next year.

A New National Security Perspective

The rapid pace of change in the post-Cold War era demands a new definition of national security issues. The development of the European Community, break-up of the Soviet Union, economic and political shifts within the former Warsaw Pact nations, the reunification of Germany, and the brisk economic growth of Pacific Rim countries have led to a new world of opportunity and threat.

The challenge to the intelligence community is to discern and disrupt economic espionage directed towards national companies and interests. A fundamental shift in our understanding and protection of the nation's secrets will require:

- Redefining the concept of national security secrets and moving beyond protection of the defense industry to assisting the entire private sector in combating corporate espionage.
- More explicitly connecting the impact of industrial espionage on the national economy to national security issues.
- Broadening the role of personnel security in non-defense industries, including a new perspective on "clearances," training, and threat awareness.

- Providing more information to the corporate community from the intelligence community regarding espionage threats, source countries, and targets and means.
- Aggressively prosecuting those involved in illegal economic and competitive intelligence.

Emerging Espionage Targets

Every industry and every country has important economic resources which must be protected. Generally, the focus of economic espionage activities can be broken down into two broad categories.

The first is formulae, processes, components, structure, characteristics, and applications of new technologies. Examples include:

- Fifth generation computer architecture; new computer chip designs, conductivity, and biochip research; and software development.
- Biotechnology.
- Supercomputing and superconductivity.
- Holographic and laser research, applications, and modeling.
- Optics and fiber optics technology.
- Aerospace technologies.
- Medical technologies, including pharmaceuticals.
- Advanced communications technologies and processes.
- Advances in satellite usage and space technologies and applications.
- Electromechanical products and technologies.
- Chemical process technology and research.
- Integrated circuit technologies.

The second category is factors associated with the marketing, production, and security of new technologies. Examples include:

- Pricing information.
- Marketing research on demand and consumer profiles.
- Products needed for compatibility and applicability.
- Production timetables and product release dates.
- Production quantities.
- Market targets and schedules and overseas marketing plans.
- Security equipment, sensors, and processes.
- Electronic banking equipment, interfaces, and protocols.
- Technology-upgrade schedules and planned changes in technology.
- Software developments, especially those enhancing new technologies, networking, and technological integration.

Two Vulnerable Targets: Computers and Intellectual Property

Computers provide both a target and a tool for industrial espionage. The new information highways provided by network systems (like Internet, Milnet, and Bitnet) and other advances like Electronic Data Exchange (EDI) and SWIFT (Society for World International Financial

Transactions) also can mean increased access for illegitimate purposes. Computer-related crimes can be broken down into four main categories.

Computers as Targets: This relates to unlawful accessing of computers to gain information or to damage programs or hardware. A wide array of crimes fall into this category including: theft of intellectual property or marketing information, blackmail, sabotage of files, accessing and/or changing government records, techno-vandalism (causing internal damage to computer systems) and techno-trespass (violating the privacy of computer files).

- **Computers as Crime Instruments:** Computer processes used as instruments of crime. Examples include: ATM fraud, rounding off monetary entries, credit card fraud, and fraudulent computer transactions, and telecommunications fraud.
- **Incidental Criminal Computer Use:** Computers used to increase the efficiency of traditional crimes, for example: money laundering, off-shore banking, pedophile information exchanges, organized crime record keeping, murder (through changing information in hospital records or other control systems), and bookmaking.
- **Crimes Associated With Computer Prevalence:** The advent of microcomputers has opened new crime and espionage targets. These include: software piracy/counterfeiting, copyright violations, counterfeit and black market computer equipment and programs.

Another growing target of economic / industrial espionage is intellectual property. It consists of concepts, ideas, planning documents, designs, formulae, and other materials intended for products or services which have commercial value and represent original thought or work. It may be clearly protected (with copyrights, trade-marks, patents, or as trade secrets) or less well defined (in the case of non-protected research, incomplete new concepts or ideas, and public domain information which has been individually modified or refined).

Intellectual property is increasingly sought through industrial espionage because it can reflect a valuable investment involving lengthy research and development efforts. Moreover, it is often stored on computer media which are them-selves an increasing target of espionage.

Methods of Espionage

In addition to unlawful computer access, many of the traditional methods employed in national security and industrial espionage will continue to be prominent. Among the many means of obtaining information are:

- Open sources (Right to Information Act requests, published government documents and bidding specifications, opened bids and technical journals).
- Consultants or outsourcing contractors from targeted firms who provide "inside information" to competitors.
- "Moles" working inside a particular industry or company with access to desired information.
- Computer hacking and data transmission interruption.
- Compromising employees through blackmail, set ups, corruption, and bribery.

- The use of student researchers and interns to gain access to research.
- Surveillance of corporate employees.
- Intercepting communications through faxes, telephones, etc.
- Burglary.
- Gaining access to records through janitorial or service personnel.
- New technologies and techniques adapted as detection devices or espionage countermeasures.

Motivations for Espionage

In general, the primary motivation for engaging in espionage is monetary. However, several factors have emerged in recent years that may make it easier for employees or others to participate in economic espionage. As espionage activity has shifted away from a focus on national security, the profitability of spying has increased. In addition, economic espionage (especially when information is divulged to traditional national allies) is less morally repulsive than betraying a national security secret and does not incur the same threat of punishment.

Employers should watch for a number of key characteristics that may indicate a security risk. Security threats may include employees who:

- Are generally unhappy on the job, or unhappy with the location of their assignment.
- Believe they have been overlooked for promotion, salary increases, or commendations and rewards.
- Feel their contributions to the company are ignored and uncompensated.
- Are facing personal financial difficulties.
- Have personal problems.

Prevention

There are a number of measures that employers can take to reduce industrial espionage. The most crucial of these are related to effective personnel policies and procedures.

Selection: Employees should be recruited and screened on the basis of their knowledge, competence, loyalty, and psychological and social stability.

Training: Employee training should include information about security threats and procedures.

Surveillance: Maintaining control over and limiting access to sensitive information will reduce potential losses.

Supervision: Attentive supervisors can both identify security violations as well as intervene before problems occur by remaining alert to warning signals.

Accountability: Ensuring that employees follow procedures, perform efficiently, and adhere to organizational values will help maintain personnel integrity.

Target Hardening: Measures should be taken to protect crucial information and to improve security in order to reduce temptation.

Positive Work Environment: Increasing employees' sense of worth within the organization can increase their sense of obligation and loyalty, thereby decreasing the possibility of espionage.

Realistic Sanctions: Employees must have a realistic sense that security violations will be identified and severely punished.

Positive Rewards: To balance the threat of discipline, positive contributions to the organization must be reinforced and rewarded.

Reinforcement of Ethics and Values: The organization must strengthen its employees' sense of moral obligation through a statement of organizational values, reinforcement of ethical standards, and high standards of professionalism.

Imagine a world where License Plate Recognition (LPR) technology and advances in city-wide video surveillance make it possible to spot suspects and criminals so quickly and comprehensively that law enforcement is able to apprehend them virtually at will, with little to no struggle involved. There would be no shots fired, no high-speed chases, or other high-risk activity.

Let's take one scenario as an example. LPR cameras mounted at the entrance of a tunnel capture the license plate number of a suspect as his vehicle heads to a major metropolitan area. Another video surveillance camera is focused on the car. Working in tandem, the license plate number is indexed to video footage previously taken of the car, after which an operator confirms it is the one in question.

An alarm is immediately sent to law enforcement officials who right away zone in on the vehicle with other strategically placed video surveillance cameras. The cameras track the vehicle as it makes its way through the tunnel.

As the car enters the city and nears an intersection, it is watched by law enforcement officials in various locations, as these are network cameras easily accessed from remote locations. The cameras are also part of a municipal network that connects various departments, including the traffic department responsible for the computerized network of stoplights throughout the city. As the car gets closer to the intersection, an official from central command turns the light from green to red.

The light continues to stay red, which quickly creates gridlock in the already crowded urban area. This gives various undercover officers time to approach the vehicle from various angles. Before the suspects are able to realize how it happened, they are surrounded by officers with guns drawn, and have no way out. They are quickly arrested and taken into custody.

Because of these advances in LPR and video surveillance technology, a high-speed chase that could have potentially injured or killed bystanders, other drivers, or the officers and suspects, was avoided and the suspects were apprehended without a struggle.

This is not a farfetched scenario. It's actually happening right now in various metropolitan centers throughout the world. In what follows, we will explore recent innovations in LPR and video surveillance technology that allow law enforcement divisions to fight crime and ensure public safety much more effectively than could have been imagined just a few short years ago.

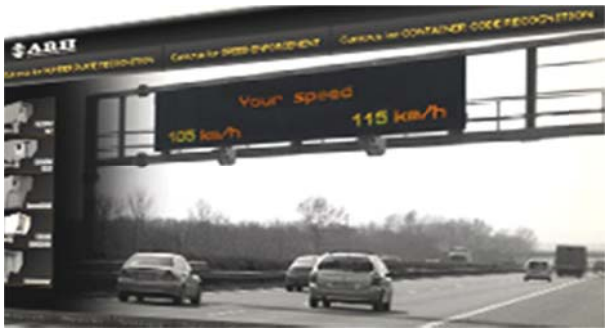
Advances in Video Surveillance Technology

Video surveillance cameras and management systems have come a long way from the early days of CCTV when grainy, analog images and limited functionality was the rule of the day. Digital (IP) technology now offers a host of advantages, including open multi-vendor architectures supporting cameras with clearer picture quality, a variety of flexible network architecture options, including wireless camera connectivity, enhanced scalability and failover and redundancy options. More so, innovative features in advanced video surveillance systems have helped cities attain objectives they never before deemed possible. Essentially, truly advanced systems allow multiple independent systems from numerous organizations to be managed as if they were a single unified system, regardless of geographic boundaries.

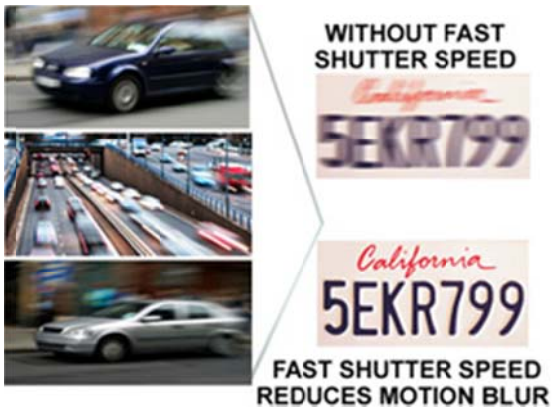
Similarly, developments in video analytics have also added a layer of intelligence that make these cameras and systems much more effective crime fighting tools, so that instead of just viewing scenes, the cameras look for abandoned objects on the roadway, loitering or virtual fencing near critical infrastructures, and can instantly alert law enforcement when a suspicious activity is spotted. These network cameras can typically be easily accessed from laptops, cell phones and other devices which not only cut down on the need for traditional surveillance techniques, but also improve overall communication and collaboration within the municipality while sharing infrastructure costs between various departments.

IP video surveillance is definitely more and more the wave of the future, just as digital advances have taken over so much of the rest of the technological landscape. However, for those who wish to maintain all or part of their CCTV systems in place, the good news is that they can do so, and at the same time, benefit from digital advances via encoders to gradually migrate their existing investments to the digital age.

Advances in License Plate Recognition LPR Technology



Challenges arise when it comes to reading license plates at various speeds and in various environmental conditions (i.e., day, night, rain, fog, etc.). This is a case where not just any CCTV camera and OCR (optical character recognition) technology will do. External infra-red lighting, high shutter speed progressive scan camera, and chromatically corrected lenses are some of the features necessary for the license plate image to be clear, of sufficient quality and well contrasted at any speed or time of day and night for it to be read perfectly by an LPR engine.



For law enforcement and national security agencies the good news is that not only is such LPR technology available, but accuracy in capturing license plates is very high. One advanced LPR system in particular can attain more than 93-percent accuracy, or 99 percent when considering OCR equivalents. Along with that, the ability to link video feeds and LPR, and view both in one single unified software interface is a serious step forward that is already benefiting law enforcement officials throughout

the world. Being able to index video footage and instantly link it to a license plate number is not just a convenience, but as seen from our previous example with the car full of suspects entering a city, can be essential to pro-active enforcement.

The One-Two Punch for Municipalities: Advanced Video Surveillance and LPR Technology

Most city departments, including police, fire, water, gas and electric, transportation etc. are more and more tied-in to one another. In the United States, as in many countries, the goal is not just interagency cooperation at the federal level, but the ability for cities to quickly marshal their defenses in the event of an emergency situation, and more importantly to use modern technology advances to try to be more pro-active in addressing public safety. On a more day-to-day level, with cities struggling for sources of revenue because of difficult economic times, it is important that such technology also benefit cities' financial bottom lines as well.

All this is possible now because of highly intelligent video surveillance and advanced LPR technology. Dispatch centers can instantly know through video cameras placed on highways and streets whether an ambulance should be sent to an accident scene. Law enforcement officers can observe criminal gang-related or illegal drug-selling activity in a neighborhood and do so un-detected by suspects. LPR technology can be used in both fixed applications for surveillance or traffic management or in mobile applications where LPR cameras are mounted on the vehicle to spot wanted criminals, scofflaw vehicles or vehicles without proper parking permits or parked overtime. In a day and age in which every dollar a city spends is scrutinized more closely, the ability to do more with less is a constant theme. The ability of video surveillance and LPR technologies to work in tandem so that, for example, a license plate is matched to previous video footage of a suspect's car, reduces the amount of hours that might have been spent on such a task if this level of integration with new technologies did not exist.

For budget-conscious municipalities, the benefits of advanced video surveillance and LPR techniques have also been extended to mass transit. This includes controlling traffic through automated tolling, as well as monitoring traffic density, volume, and flow. Besides cutting down on gridlock, the cameras can also be used to check for speeding violations by calculating a vehicle's time spent traveling between two points.

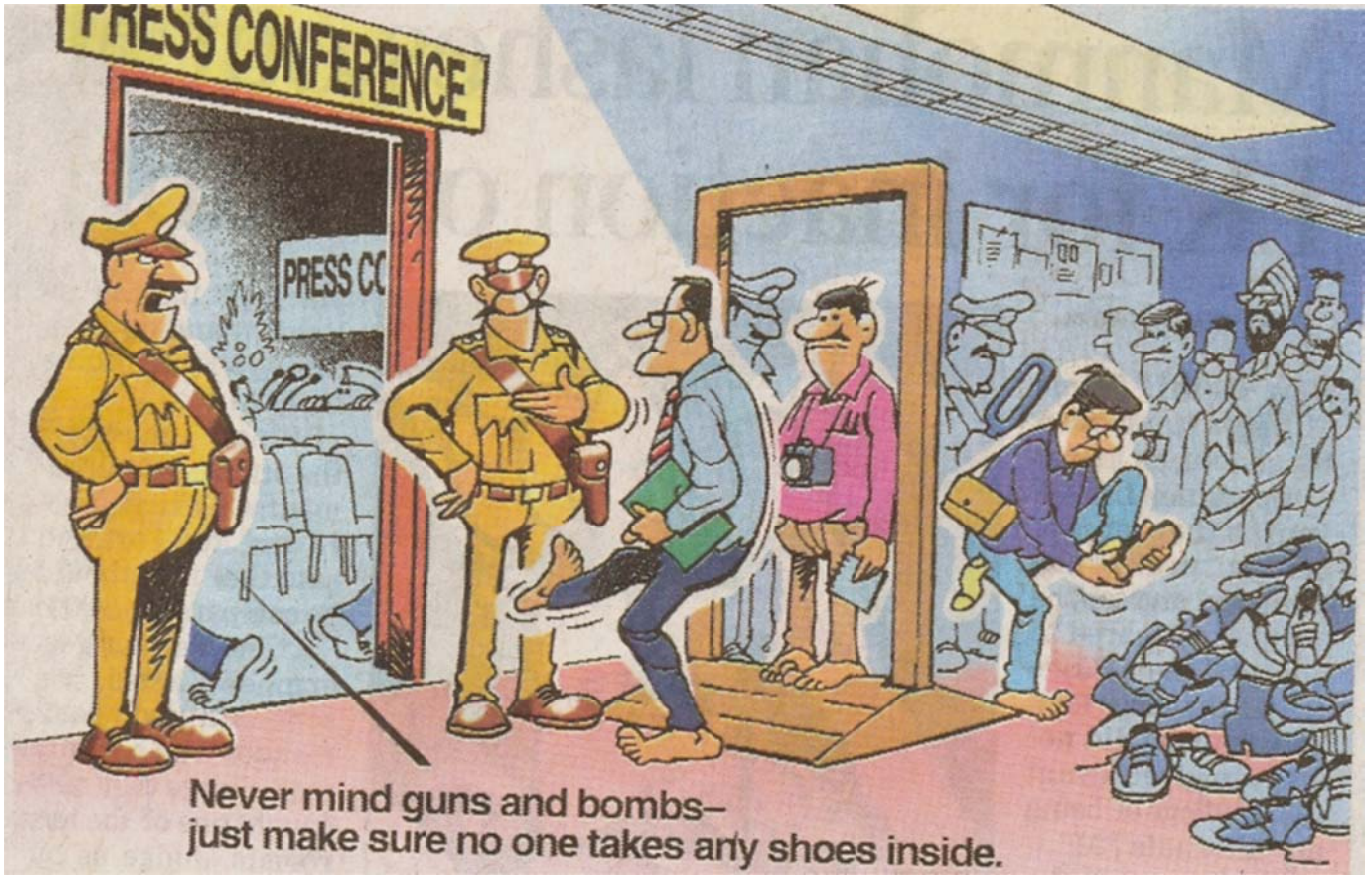
The Road Ahead

As the populations of major cities of the world continue to grow, traffic issues typically get worse, not better. Along with such population growth, crime often increases, particularly in times of economic distress. At the same time, governments worldwide – at the federal, state and local levels – are facing even greater budgetary constraints than usual.

With all this in mind, the need for automation and greater intelligence in reference to security technology should become even more paramount. Fortunately, the innovations that have taken place in city-wide video surveillance and LPR in recent years have not only increased the automation factor, but increased intelligence and functionality. These technologies have now become even greater crime fighting partners for law enforcement, as well as have helped to reduce total cost of ownership for cities. As the technology gets even smarter over time, such benefits can only be expected to increase.

Reference: http://www.securitymagazine.com/Articles/Online_Exclusives/BNP_GUID_9-5-2006_A_10000000000000919930

In lighter veins



Suggestions & feedback may be sent to us on e-mail: sbtyagi1958@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!