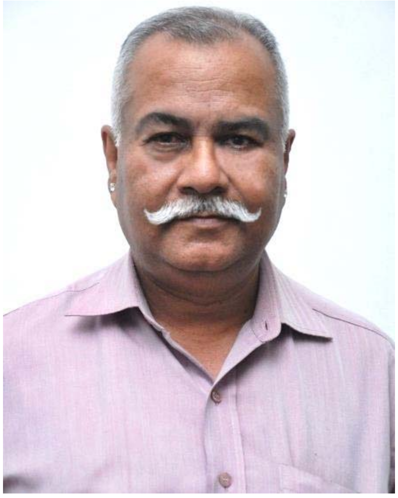
Let's professionalize the professionals…

ICISS

Newsletter: November 2016

International Council for Industrial Security & Safety Management



Happy Dipawali!

May it be safe & secure to all!!

In India the season of gaiety and festivity has already begun starting with Ganesh Puja, Durga Puja, Dusehara and id-ul-adha! Children have been anxious and exited over the year for this period only. Dipawali is round the corner!! Many families will travel to their native places leaving behind their homes locked and under the care of security personnel who have to prove themselves once again worthy of trust and confidence which such families have in them. Let all security personnel rise to this moment and discharge the duties more diligently and carefully!

However as it has often been said, security is not the duty of the security personnel alone. Everyone has to be security conscious and must discharge the basic responsibility to start living securely. In this direction, the least every one of us has to do is to secure the doors and windows while leaving the house. We keep lots of valuable items in the home and trust the security with a cheap lock! The doors sturdiness as much as heavy duty locks and bolts will add to the security of every residence.

Children need to be advised for safety precautions with fire crackers. Parental guidance is always essential and keeping first aid box is not a bad idea at all!!

Capt S B Tyagi
For ICISS

Let's professionalize the professionals…

Globalization of Terrorism

D.C. Nath, IPS (Retd.)
(Former Special Director, Intelligence Bureau)
Chief Patron, ICISSM

What to speak of an act of terrorism, the expression "terrorism" strikes terror in the hearts of the bravest of the brave. Down the ages, terrorism has indeed been the scourge of humanity! Such are the causes or factors that lead to the emergence, growth and sustenance of terrorism that the phenomenon of terrorism is unlikely to be stamped out. This is stark reality, however, unpleasant to accept. The "doomsday" may not visit the humanity through nuclear devices because of inherent deterrence of mutual destruction but weird acts of terrorism are certain to sap the life-force of those lucky to enter the 21st century. The threat posed by terrorism, rather international terrorism, is very serious and all pervasive.

Whatever are the reasons or the ground realities for terrorism, such as, socio-economic deprivation, ethno-political aspirations, ideological inspirations, suppression or oppression of weaker sections or communities, etc., the fact is that terrorism has now assumed a true transnational dimension and has all the potential and prospect of being globalised in all senses of the term. No wonder, therefore, experts say that terrorism is "widespread geographically and diverse ideologically". This low intensity activity suits many for obvious reasons. It is less expensive, boosts ego and at times helps achieve some immediate objective quickly. Frankly speaking, transnational terrorist activities are now attracting quite a few, primarily because of the feeling that resolution of internal social, economic and political problems can be achieved either by eliciting, rather easily, support (in the form of men, material and ideology) from outside or by committing some spectacular acts in some advanced countries or against some developed countries' interests. In a way, the United Nations had come to virtually accept this phenomenon when the U N General Assembly passed a resolution on October 24, 1970, that "every State had the duty to refrain from organising, assisting on participating in acts of civil strife or terrorist acts in any other State or acquiescing in organised activities within its territory directed towards commissioning of such acts." It is, of course, a different matter that such dictums have remained more on the statute books than been observed or implemented.

Terrorism has indeed become a global phenomenon with increasing and rather well-identifiable links between different terrorist groups or organisations. They use each other's areas for recruitment and training, exchange illegal weapons, engage in joint planning and ventures and also provide administrative and other logistic support. Indeed, the extent of international linkage between terrorist groups in different countries could be appreciated from the fact that the group that carried out the massacre at Lod Airport in Israel belonged to Japan, was trained in Korea, purchased arms in Italy with money support and sympathy of several Arab countries. The irony in such globalisation of terrorist activity lies in the fact that all this is often or has actually been facilitated not only by obvious support of states and governments inimical to each other, but also by technological advancement in the field of scientific research that human brains are capable of. Quite often the terrorist groups are one step ahead of the state machinery in the use of technological aids to their planning and commissioning of the act.

Though it is not intended to quote case histories in this thematic presentation, few references may help drive home the point forcefully. One has only to look at the activities of the PLO, Libyan or Iraqi terrorists in London, the attack on the synagogue in Paris, the activities of the South Mulaccans in the Netherlands, the 1986 US air strike against Libya. It is also assessed by many experts that Sudan has now practically become the safe haven for the terrorists. Politically isolated and running a disastrous economy, the military government in Khartoum, backed by Islamic leaders, would seem to believe that no one wants to get involved in the affairs of Sudan and it as such can get away with lending support to terrorists from other nations and countries. Although chauvinists from many religious sects have often been responsible for inhuman acts of terrorism down the corridors of history, resurgent Islam - may be the Pan-Islamic urge - would seem to be now rather embarrassingly involved in acts of terrorism in different parts of the world. Possibly some Islamist fundamentalists fondly or rather mistakenly believe that with the end of the cold war and the emergence of the unipolar world led by the USA, they could present themselves as an alternative to the westernised rulers in their respective countries. It is, therefore, not surprising that even Islamic countries like Egypt, Algeria, Pakistan and Saudi Arabia are all casualties of transnational or international terrorism. The Pan-Islamic Wahhabi agenda of the Taliban movement, born and nurtured by the Jamaat-e-Ulema-Islami, today threatens all the countries in the region. Neither the West Asian countries nor the Central Asian Republics or India or Pakistan nor even China (Xingiang Province) remain unaffected by the militant activities of this movement. Such is the state of affairs in Pakistan that it has virtually become, one trends to inter, the hideout by choice, for terrorists operating in the name of self-conceived cause of Islam – one such instance being the Nairobi US Embassy bombing -suspect (August 7, 1998) was arrested from Pakistan. According to Washington, their suspect Osama Bin Laden, a Saudi Arabian thrown out of the country for advocating the ouster of the Saudi Royal family, was using a base in Afghanistan to train and finance Islamist terrorist groups world-wide, targeting US interests and citizens alike. He was ultimately killed in Pakistan by USA has ultimately exposed Pakistan as protecting, sheltering and training terrorists of all the hues!

Nothing has contributed more towards the globalisation of terrorism than the illicit trade in narcotics. Notwithstanding the fact that the drug lords are primarily motivated only to earn money the quickest and cheapest way and at times the links between their operations and that of the terrorists are not that evident and require good investigation to be established, the symbiotic relationship between the two trades is no longer in doubt. The "malevolent marriage" between these two is responsible for global lawlessness in more than way. The nexus between the two is more pronounced along international borders, one providing support and the other the necessary protective cover. They, it is said, interact "synergistically" in their operations. Thus has evolved the expression "narco-terrorism," meaning in simple terms terrorism funded by narcotic trade or drug money. Narco-terrorism strikes at the social and political foundations of a country. Among many cases, the most classical example of threat from this deadly combination was Columbia's infamous drug kingpin Carols Lehder, who described drugs as the "Third World's Atomic Bomb." The threat or the danger to humanity at large from this quarter is indeed so frightening that there is welcome inter-state co-operation to work out international and multi-pronged strategies to control this menace even amongst otherwise mutually non-cohesive states or combination of states.

The twin brother of narcotic trade in providing the necessary sinews to the terrorists is the trade in illegal weapons. The so-called "arms bazaars" like those at Darra and Landi Kotal operating in some of the countries in the middle-east are meccas to international terrorists. The role of narcotics and illegal arms is perhaps best documented in a CIA study titled "Heroin in Pakistan." The study reveals how the ISI allowed Afghanistan Resistance Groups to trade in narcotics after the cut-off of US assistance. Individual ISI officers, it was learnt, were reported to have participated in the trade and terrorists pushed into India were partly, if not wholly, funded through income earned through narcotics. That activities of narcotic gangs and clandestine arms deals through covert support from different intelligence agencies were causing international concern was also clear from a U N Report of 1987, which linked international terrorism to illegal drug production and trafficking and illegal arms trade. The vast underworld, fed by hostile intelligence agencies, links criminals involved in narcotics and money-laundering and illegal arms dealers into a sinister web. Smugglers feed terrorist violence at one end and illegal arms dealers at the other. The arms-drop case at Purulia (West Bengal, India) is only suggestive of the fact that the routes for illegal arms trade criss-cross over even continents. National boundaries or international borders are of no consequence to those involved in such trades.

All these are changing the faces of terrorism and that is why perhaps the most well known student of terrorism Walter Laqueur, Chairman of the International Council at the Centre for Strategic and International Studies, USA, has said, “In its long history terrorism has appeared in many guises; today society faces not one terrorism but many terrorism.” The greatest change has been that terrorism is no longer the militants' only strategy. The past few decades have witnessed dozens of aggressive movements espousing varieties of nationalism, religious fundamentalism, fascism and even apocalyptic millenarianism, from Hindu nationalists in India to neofascists in Europe and the developing world to the Branch Dravidian cult of Waco, Texas. The earlier fascists or terrorists believed in armed or military aggression and engaged in huge arms build-up but such a strategy has become outdated. Now, mail-order catalogues tempt militants with readily available , far cheaper, unconventional as well as conventional weapons. On the question of the possibility of international terrorists of today, likely to remain operative in the 21st Century, resorting to the use of nuclear devices or biological weapons, Walter Laqueur is of the opinion that given the technical difficulties, terrorists are probably less likely to use nuclear devices than chemical weapons, and least likely to attempt to use biological weapons. “But,” Laqueur warns, “difficulties could be overcome, and the choice of unconventional weapons will in the end come down to the specialities of the terrorists and their access to deadly substances.” Terrorists are not generally likely to engage in over-kills if their traditional weapons - the submachine gun and the conventional bomb - are sufficient to continue their struggle and achieve their aims. But, despair could lead to giving up the usual armed assault and make a desperate attempt to beat the enemy, as if to prove the paradox that “only hope lies in their despair.”

Laqueur also sounds a cautious note on possible “future shock.” In the coming days, the terrorists could be individuals or like-minded people working in very small groups, on the pattern of the technology-hating Unabomber, who apparently worked alone sending out parcel bombs over two decades or the perpetrators of the 1995 bombing of the federal building in Oklahama City (USA). An individual may possess the technical competence to steal, buy, or manufacture the weapons he or she needs for a terrorist purpose and the ideology or ideologies such individuals may espouse could be more aberrant than those of usually larger groups of terrorists. A serious danger indeed!

The society today has become vulnerable, adds Walter Laqueur, to a new kind of terrorism. Advanced societies are now dependent every day on electronic storage, retrieval, analysis and transmission of information. Defence, the police, banking, trade, transportation, scientific work and a large percentage of the government's as well as private sector's transactions are on-line. That exposes enormous vital areas of national life to mischief or sabotage by any computer hacker, and concerted sabotage by some competent hacker could render a country totally non-functional at the shortest notice. Hence the threatening or emerging speculation about “infoterrorism” and “cyberwarfare.” The overall “Information Warfare” is the most dreaded form of terrorism facing the civilised society - a true model of globalisation of terrorism which would respect no national boundaries or international borders either in space or on the ground. New and intelligent methods and approaches would be called for to detect and discern the motivations and the ever-increasing skills of the terrorists threatening the mankind in the 21st century. “The salvation of mankind lies in (true) civilisation, education and humanity; it needs neither sermons nor prayer but the awakening of a feeling of human dignity in the people” as the Russian literary critic of the 19th century, Belinsky had stated.

The scribe sincerely believes that international fora such as the one organised by the International Institute For Non-Aligned Studies could provide the right platform to the thinkers – and may be even to the dreamers with visions – to plan with conviction what would be the best and workable methods to face the challenges being thrown up by the ever widening phenomenon of globalisation of terrorism and the intrinsic threats posed by terrorism to the humanity in the 21st century. What is required is will and transparency in both thoughts and action, often wanting in those who could help. It is hoped that this Seminar will draft and send a suitable message to all those concerned with the safety and security of human lives – both now and in the 21st century.

Security Executives need to be Good Salesmen!

One of the most important yet often overlooked factors in high-end, private sector protective operations is the sale. It is very difficult getting the right decision-makers to sign onto security budget – and to be willing to pay for it. One of the biggest challenges is that in most cases, the decision-makers who are in position to sign onto security program aren't security professionals. So the challenge is how to communicate – and sell – security to non-security personnel.

Having acquired over three decades of experience in this field I know there are many opportunities which Security Chief can obtain to make his case for expenditures on new security initiatives. These cover executive presentations, security board meetings, budget committee meetings and even one-on-one conversations with executives of key functions.

Make it Simple!

There's a celebrated quote attributed to Albert Einstein that goes "If you can't explain something simply, you don't understand it well enough". Most executives and stakeholders are probably familiar with this idea, and you would be wise to familiarize yourself with it too. It's OK, or even necessary, to elaborate on a subject, especially if you're asked to do so. But don't forget to start with a simple explanation before you plunge into the deep-end of things.

It's very common among security professionals to make fun of naive clients and executives who are so ignorant about their own safety and security. But try not to let this mostly harmless tendency infect the way you explain security to them. Remember, the executives and decision makers you are talking to did not get where they are by being dumb, and they're not going to appreciate you treating them as such. Security just isn't their field of expertise, it's yours.

The idea is to synthesize and summarize things into understandable terms with actionable outcomes. It's the opposite of dumbing things down.

Know your audience

This one comes up a lot. You've put together a great security presentation; detailing threat matrixes, risk mitigation strategies, hostile planning disruptions, attack contingencies, and, oops… You've lost your non-security audience about thirty seconds into it.

Always be mindful of your audience's level of understanding and/or caring in regards to security issues, and adapt the way you explain things to suit them. It's like the old basketball idea, where the responsibility for the pass falls on the player who throws the ball, not on the one who fails to catch it. Your listeners are where they are. It's your responsibility to pass the information to them at a level they can receive it.

Put things in relatable terms

Once you know who your audience is, try to translate security into relatable terms your audience is not only familiar caring about, but familiar paying for. It's not that it's particularly difficult for decision-makers to understand ideas like security risk mitigation, it's just that it's a stretch for many of them to give it the budget it requires. But put it in relatable terms for them, and explain that a risk mitigation strategy is actually a potent insurance policy (with preventive and reactive benefits), and presto, every single person in the room, from accountants to HR managers can relate to it. Speaking of insurance, suggest to your budget conscious audience (I've yet to meet one that isn't) that they can inform their insurance provider about their new security measures, and see if they can negotiate lower insurance premiums to cover the now lower risk profile – thereby actually **saving** them money.

Finally, on the slightly negative end of things (which means you should never start off with this angle), if your audience is reluctant to take action, try to explain that a lack of preventive and/or reactive security capabilities opens them up to certain legal liabilities. It's not the most cheerful subject to raise, but one that might sway the legal department to take a second look at your suggestions.

Return on investment (ROI)

You might be able to wow every decision-maker on the planet with your tactical skills and experience, but if they don't see what's in it for them, they're not likely to invest any capital in it. As you explain things, always keep your audience's interests in mind – not where you think their interests *ought* to be, but where they actually are right now. The bottom line for almost any decision-maker is '**How much will it cost me, and what's in it for me?**' It's in the second part of this question – the return on their investment – where you should really put some explanatory effort.

- Cost of Security v/s cost of having 'no security
- Cost of having 'No Security' v/s cost of having reasonable security
- Cost of having effective security

Shock & Awe: A failed tactics in Corporate World

Though this can, on occasion, lead to a sale, shock & Awe tactics aren't usually effective. It's a classic mistake that many security professionals make – trying to scare decision-makers with horrific case studies, and doom-and-gloom prophecies of what might to happen to them if they don't employ some immediate protective measure.

It's not a question of describing what you think is objectively true, but choosing an effective way to communicate things in order for your listeners to take action. As strange as it may seem, most people are not likely to take action if you try to shock and scare them. Doom-and-gloom just doesn't sell very well. You don't have to mindlessly sugar-coat everything; just find a more effective way of getting your audience to **want** to take action.

Manage expectations

Set realistic expectations for non-security audience! It's not a question of objective tactical effectiveness, but of relatable and realistic ideas to suit your specific audience. To ignore this point will not only be a disservice to your audience, but might get you booed or laughed out of the room. **"I don't know"**

Last but not least, if a question gets asked that you don't feel qualified to answer, don't be afraid to say **"I don't know"**.

Many security professionals are afraid this will make them look weak or ignorant in front of clients or prospective clients. The fact of the matter is, however, that no one knows everything, and it's actually important to admit what you don't know.

Philosophers and stoics since ancient Greek times have referred to *Socratic Ignorance* (the frank acknowledgement of what you don't know) as a true sign of wisdom. Not only is there no shame in admitting you don't know something, it can be a way to demonstrate integrity and intelligence. Don't make a big deal out of it, just admit you don't know, and offer to get back to the person with an answer later on.

Changing Scenario: Security Services in India

Digital displays changed the approach of modern man towards time and especially towards wrist watches. Hitherto, time was seen but suddenly time was being read with digital watches. So, analog watches were replaced by digital watches even when for a short time. Since the need for analog watches remained and technology transition took time, a new genre of watches, called "Digi-ana" (Digital and Analog) was brought to the market.

Similar technology driven changes were made in banking industry which greatly facilitated customers and also impacted security concerns. ATMs changed the ways banking is done! Since banks wanted to cut operational costs, they also wanted less and less customers coming to their branches for mundane banking activities such as cash withdrawal, balance inquiry or pass-book updates. ATMs were answer to all such needs and were found to be convenient, efficient and low cost. As Customers liked it, banks eagerly multiplied the number of ATM's.

Initially different group of credit cards were present, soon debit cards also joined the hustle-and-bustle and soon majority of ATM's started accepting all leading brands of credits cards and debit cards of all leading banks. At this stage since foot falls per ATM increased, increased need of cash in ATM caused security concerns. The licensing authorities, regulators and police demanded effective security measures for ATMs, causing increased administration costs. Thus 'banking-away-from banks' became expensive propositions considering 24x7 operation and security needs.

It is well studied forecast of changing trends in ATM operations that soon ATMs will remain just ATM without carrying name of any bank. All the transactions using credit / debit cards will carry transaction fees and operation and maintenance will be by some specialized agency other than the banks. Thus ATM operations will cater to varied needs of the customers and also incorporate directives of the regulator, licensor and the police.

It is further envisaged that soon in India every citizen will have only one bank account against the present freedom of holding multiple accounts in multiple banks. This migration to 'regulated bank account regime' will go long way for effective e-governance and reducing black money as well as reducing tax thefts.

In this emerging scenario; changing trends in security management will develop. Two major trends are foreseen-

- Central Command & Control Centre
- ATM Management Services.

There have been pioneering services started by few leading companies in Metro cities where under command and control centre have been established by them with the trained manpower and sufficient resources with Quick Response Teams, to take care of specific need of clients. The clients' CCTV and other alarm system are maintained and monitored, notifying the pre-identified authorities, mobilizing the resources to mitigate the alarm situation and prepare post-event reports. Since this area of specialized service has just opened-up, there are not very many players and standards are non-existent.

So far as ATM Management Services are concerned, the direction and decision of the Government will decide the shape this segment is to take. Early indications are that Central Government is seriously thinking of providing a bank account to every citizen of India linked with Aadhar and or National Citizenship Card. The citizen will have a choice for selecting a bank.

Electronic transactions will be favoured or rather encourage. Instead of going to the banks, the customer would be led to ATMs where any type of card from any bank will be acceptable. For each transaction the concerned bank will charge fees from customers, part of which will go to franchisee running / maintaining the ATMs. Thus new service segment will emerge which will offer range of services including congenial and secured environment where customer would prefer to have ATM transaction, cash transportation to feed ATMs, security of machines and the facilities and up keep and maintenance of ATMs. All the gamut of services related to ATMs will be preferred to be provides by one services provider.

Thus, it can be seen by above that soon there will be two specialized services sectors emergency in broad area of security management for which niche is already created. Some pioneer work has already been done and industries thought-leaders have already begun the initiation to shape-up this segment further.

Voice Recognition: How It Works

Our voices are unique to each person (including twins), and cannot be exactly replicated.

Voice recognition (also known as automatic speech recognition or computer speech recognition) converts spoken words to text. The term "voice recognition" is sometimes used to refer to recognition systems that must be trained to a particular speaker - as is the case for most desktop recognition software. Recognizing the speaker can simplify the task of translating speech.

Speech recognition is a broader solution which refers to technology that can recognize speech without being targeted at single speaker - such as a call centre system that can recognize arbitrary voices.

HARRY PICKED A BAD TIME TO GET LARYNGITIS

Voice recognition technology utilizes the distinctive aspects of the voice to verify the identity of individuals. Voice recognition is occasionally confused with speech recognition, a technology which translates what a user is saying (a process unrelated to authentication). Voice recognition technology, by contrast verifies identify of the individual who is speaking.

The two technologies are often bundled-

- Speech recognition is used to translate the spoken work into an account number, and
- Voice recognition verifies the vocal characteristics against those associated with this account.

Speech includes two components: a physiological component (the voice tract) and a Behavioural Component (the accent). It is almost impossible to imitate anyone's voice perfectly. Voice recognition systems can discriminate between two very similar voices, including twins. The voiceprint generated upon enrolment is characterized by the vocal tract, which is a unique physiological trait. A cold does not affect the vocal tract, so there will be no adverse effect on accuracy levels. Only extreme vocal conditions such as laryngitis will prevent the user from using the system.

During enrolment, the user is prompted to repeat a short passphrase or a sequence of numbers. Voice recognition can utilize various audio capture devices (microphones, telephones and PC microphones). The performance of voice recognition system may vary depending on the quality of the audio signal as well as variation between enrolment and verification devices, so acquisition normally takes place on a device likely to be used for future verification. To prevent the risk of unauthorized access vie tape recording, the user is asked to repeat random phrases.

During enrolment an individual is prompted to select a passphrase or to repeat a sequence of numbers. The passphrases selected should be approximately 1-1.5 seconds in length- very short passphrases lack enough identifying data, and long passwords have too much, both resulting in reduced accuracy.

Free Up Your Other Hand With Voice Recognition TV

The individual is generally prompted to repeat the passphrase or number set a handful of times, making the enrolment process somewhat longer than most other biometrics.

Each person can be uniquely identified by the sound of his or her voice. A person's Anatomy (size and shape of vocal tract) combined with learned behaviours make up His or her voice print. Latest speaker recognition systems extract features representing physical characteristics (anatomy) and behavioural characteristics (such as inflection); together these uniquely define the individual.

Traditional speaker recognition systems use 'fixed sentence' technology. A speaker utters a specific sentence to enrol and repeats the same sentence (or recorded phonemes) to authenticate. Fixed sentence technology has certain limitations such has certain limitations such as its inability to identify a speaker during a live free form conversation. In addition, there are significant security risks as the system can grant unauthorized access to fraudulent parties who simply play back a recording of the speaker saying the pass – phrase.

In 'free speech' technology the system can identify the speaker during a free form conversation in any language. It does not require any specific words or sentences to be repeated. The subject can enrol while speaking one language and later be authenticated or identified while speaking another language. Unlike fixed-sentence systems, unscrupulous users may find it extremely difficult to fool the newer automated authentication systems by playing back a recording.

To gain access, a random pass phrase generated by the system must be repeated by the user. Authorization is granted after the system determines that the correct words were spoken by the right person. On-going research has produced capabilities that can identify and authenticate speakers in any language and with free form speech. Free form speech technology offers significant advantages across numerous markets:

- Law Enforcement and Homeland Security: as a supporting technology for surveillance and intelligence gathering,
- A speaker can be identified during a free form conversation.
- IT Security: either during a live conversation or through an automated system,
- Speaker can be authenticated with or without a spoken random passphrase.
- Forensics and Intelligence: a voice print can be quickly matched against a database of
- Known persons of interest to support major investigations.
- Banking and Call Centres: determine the identity of anonymous callers and authenticate
- Customers to help prevent and solve fraud and other crimes.

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!