Let's professionalize the professionals…

International Council for Industrial Security & Safety Management

ICISS

Newsletter: April 2016

CONTENTS

CONTENTS

Let's professionalize the professionals...

Post Brussels: Paradigm Shift in Aviation Security

Even if it means rewriting of the security drill at airports, it is warranted although this could lead to long queues and avoidable rush, besides affecting flight schedules. One needs to balance the safety requirements with smooth movement of passenger traffic through airports etc. Adding long queues on account of any "unreasonable" security checks would only end up inconveniencing the passengers. However inconvenience is not greater than human lives!

There are three types of security systems at airports globally. The most stringent is "concourse plan" under which passenger and baggage screening happens before entering terminals.

The second is "security hold area" plan under which passengers are screened after check-in and before being allowed to go to the boarding gate area. This is the most commonly used system both globally and in India.

The third is "boarding gate" plan where passengers are screened just before boarding plane. "A security system is chosen depending on the threat perception of a place. India has a very high threat perception yet why we allow anyone to take anything inside terminal buildings without screening beats me," said a security establishment insider.

The response to a terror attack anywhere in the world has to be reasonable. After every aviation related terrorist act, special alert and standard operating norms associated with it are considered as the right response. A review of the security drill every time an airport is attacked in any part of the world, would be ridiculous. The heightened security drill at airports covers measures such as random checking of luggage at entrance to airports, deployment of more quick reaction teams, stricter frisking and a second round of checking of hand baggage at boarding gates.

Kolkata's police commissionarate and airport security are a worried lot after one member of state assembly was arrested from the airport with a firearm. The firearm could only be detected after he put his luggage on the baggage scanner. Ideally, the firearm should have been detected earlier. Even when this was not a technical breach as the gun was found immediately at the first possible detection point.

The Authorities and security agencies need to consider and decide clearly as to whether they are securing the flights or the people in and around airports. As of now, the focus appears to be on flights only!

Capt S B Tyagi
For International Council of SS

All the Facets of Airport Security

Terrorism has been a problem for airlines and air travelers since the 1970s, when hijackings and bombings became the method of choice for subversive, militant organizations around the world. Although security at airports has always been tight, the 9/11 attacks woke many people up to a harsh reality -- it wasn't tight enough.

According to the Department of Homeland Security, 730 million people travel on passenger jets every year, while more than 700 million pieces of their baggage are screened- for explosives and other dangerous items.

Imagine for a second that you are a terrorist who wants to blow up or hijack a plane. You know that once you get inside the airport, you will have to pass through metal detectors, bomb-sniffing dogs, and possibly a search of your clothes and luggage. How could you bypass all of those security measures? You could climb a fence or drive a truck to a sensitive area of the airport. With the security agencies focus on securing the security hold areas, the terminals and the concourses, the runway-side of the airports are often neglected. Climbing the walls undetected is easy, and, thereafter remaining undetected while moving towards the terminal side is easy. It must be admitted that anyone approaching the aircrafts undetected is very difficult. But when target is not the flights but the people – any people, the task of potential terrorists is very easy.

First Line of Defence:

For this reason, the first line of defense in airport security is the most obvious: fences, barriers and walls. Tall fences that would be difficult to climb enclose the entire airport property. Security patrols regularly scan the perimeter in case someone tries to cut through the fence. Especially sensitive areas, like fuel depots or the terminals and baggage handling facilities are even more secure, with more fences and security checkpoints.

Another risk is that someone could drive a truck or car containing a bomb up to the airport terminal entrance and just blow up the airport itself. Airports have taken several steps to prevent this. Large concrete barriers, designed to block vehicles up to the size of large moving trucks, can be deployed if a threat is detected. Loading zones, where people once parked their cars to get their baggage in or out of the trunk, are now kept clear of traffic. No one is allowed to park close to the terminal.

One critical security measure utilized by several regional and international airports is the use of fiber optic perimeter intrusion detection systems. These security systems allow airport security to locate and detect any intrusion on the airport perimeter, ensuring real-time, immediate intrusion notification that allows security personnel to assess the threat and track movement and engage necessary security procedures.

Secure the People, Flights will be secured:

When flight security is the focus then the stringent screening right from the times people enter the airport must start. This ensures that not only the people are screened their belongings and luggage are also screened at fist level of checking which also becomes first level of screening and intervention. There is no point if someone enters with a printed copy of a ticket and remains inside the airport areas prior to conventional security checking after obtaining the boarding passes. This means that still a very large area is accessible to any terrorist and large crowd is his potential target.

A recent development is the controversial use of backscatter X-rays to detect hidden weapons and explosives on passengers. These devices, which use Compton scattering, requires that the passenger stand close to a flat panel and produce a high resolution image. A technology released in Israel in early 2008 allows passengers to pass through metal detectors without removing their shoes, a process required as walk-though gate detectors are not reliable in detecting metal in shoes or on the lower body extremities.

Alternately, the passengers step fully shoed onto a device which scans in under 1.2 seconds for objects as small as a razor blade. In some countries, specially trained individuals may engage passengers in a conversation to detect threats rather than solely relying on equipment to find threats. The art and science of 'people profiling' has very encouraging results and is found better then technologies.

Trusted Traveler Program - Secure Flights:

Throughout the world, there have been a few dozen airports that have instituted a version of a "trusted traveler program". Proponents argue that security screening can be made more efficient by

detecting the people that are threats, and then searching them. They argue that searching trusted, verified individuals should not take the amount of time it does. Critics argue that such programs decrease security by providing an easier path to carry contraband through.

Secure Flight is a risk-based passenger prescreening program that enhances security by identifying low and high-risk passengers before they arrive at the airport by matching their names against trusted traveler lists and watch lists. To protect privacy, the 'Secure Flight program' collects the minimum amount of personal information, such as full name, date of birth, and gender, necessary to conduct effective matching. Read the Privacy Impact Assessment and the System of Records Notice for information about the program's rigorous privacy protections. Personal data is collected, used, distributed, stored and disposed of according to stringent guidelines.

Started by "Transports Security Administration, USA" the Secure Flight transmits the screening instructions back to the airlines to identify low-risk passengers eligible for TSA Pre✓®; individuals on the Selectee List who are designated for enhanced screening; and those who will receive standard screening. Secure Flight also prevents individuals on the No Fly List and Centers for Disease Control and Prevention 'Do Not Board List' from boarding an aircraft. The Travel Redress Program provides resolution for travel-related screening or inspection issues.

Photo ID is not enough:

Simply taking a look at a photo ID isn't enough, however. The high-tech buzzword in airport security today is biometrics. Biometrics essentially means checking fingerprints, retinal scans, and facial patterns using complex computer systems to determine if someone is who they say they are - or if they match a list of people the government has determined might be potential terrorists.

A new system called CAPPS II could help accomplish some of this. Short for Computer Assisted Passenger Prescreening System, CAPPS II will require more personal information from travelers when they book their flights, which will lead to a risk assessment of no risk, unknown risk, elevated risk, or high risk. Passengers considered risky will be further screened. Although the system has been delayed and isn't in place yet, the Department of Homeland Security (DHS), USA, predicts that CAPPS II will make check-in faster for the average traveler.

Passengers may have noticed the public address system at an airport replaying an automated message telling you not to leave your bags unattended. And you've probably noticed that check-in attendants are asking some questions that sound a little odd:

- Has your luggage been in your possession at all times?
- Has anyone given you anything or asked you to carry on or check any items for them?

These are very important questions. A tactic used on occasion by terrorists is to hide a bomb inside an unsuspecting person's luggage. Another tactic is to give something, maybe a toy or stuffed animal, to someone who is about to board a plane. That innocent-seeming object may actually be a bomb or other harmful device.

Brussels Attacks: Will We Ever Learn our Lessons

Pramila

Pramila has been studying the changing trends in industrial crimes and the malpractices corporates engage for over a decade. She has migrated from the field of education to Corporate Laws even after post-graduate degrees of MA (Hindi) and B.Ed.

After her LL.B; she has been mostly involved in studying, projecting and forecasting the trends in corporate ethics, malpractices and competitive intelligence. Due diligence and background screening is other fields of her expertize.

Not only Daesh (ISIS) supporters have been cheering the terror attacks in Brussels, they've also resorted to polling a terrible question – "What will be the color of the Eiffel Tower in the next attacks?" The winner – London, United Kingdom! Clearly, both Paris and Brussels attacks could be avoided if the correct policies were adopted. Nonetheless, there are many 0facts about the Brussels Attacks which show the unlearned lessons by security forces, the justice delivery systems and the gross apathy by the establishments of the Governments.

Before the bombings, several Islamist terrorist attacks had originated from Belgium, and a number of counter-terrorist operations had been carried out there. In May 2014, a gunman with ties to the Syrian Civil War attacked the Jewish Museum of Belgium in Brussels, killing four people. In January 2015, anti-terrorist operations against a group thought to be planning a second Charlie Hebdo shooting had included raids in Brussels and Zaventem. The operation resulted in the deaths of two suspects. In August 2015, a suspected terrorist shot and stabbed passengers aboard a high-speed train on its way from Amsterdam to Paris via Brussels, before he was subdued by passengers.

The perpetrators involved in the November 2015 attacks in Paris were based in Molenbeek, and Brussels was locked down for five days to allow the police to search for suspects. On 18 March 2016, Salah Abdeslam, a suspected accomplice in those attacks, was captured after two anti-terrorist raids in Molenbeek that killed another suspect and injured two others. During interrogation, Abdeslam was presented with photographs of the Bakraoui siblings, who would later be suspected of committing the attacks in Brussels three days later. Belgian investigators believe that Abdeslam's arrest may have hastened the Brussels bombings.

Clear Writings on the Walls….

According to the Belgian Interior Minister, Jan Jambon, who spoke after the bombings, authorities knew of preparations for an extremist act in Europe, but they underestimated the scale of the attack. Unlike other radicalized Daesh adherents, who started as petty criminals, the men had a history of committing more serious crimes. Belgium has more nationals fighting for jihadist forces as a proportion of its population than any other Western European country, with an estimated 440 Belgians having left for Syria and Iraq as of January 2015. Due to Belgium's weak security apparatus and competing intelligence agencies, it has become a hub of jihadist-recruiting and terrorist activity.

Koenraad Elst says, "We in Belgium felt it was only a matter of time before such a thing would happen though the actual event came as a shock". He further says that the militants of Daesh, the self-styled caliphate, are acutely aware of Islamic history, and that contains one reason, dim to us but very vivid to them. ISIS statements about the attacks identify the victims as "crusaders", and Belgium is indeed strongly identified with the crusades. The First Crusade was led by the proto-Belgian earl Godfrey of Bouillon, who became the first king of Jerusalem in 1099; his equestrian statue adorns the highest place in Brussels, next to the Royal Palace. The Crusader elite corps of the Knights Templar had a tactical alliance with the Assassins, a Shia militia dedicated to fighting the (Sunni) Caliphate. Today, the neo-caliphate (Daesh or IS) is continuing that thousand-year-old struggle against both Shia and Crusaders.

The Criminal Backgrounds of all the Perpetrators…

Ibrahim and Khalid El Bakraoui

The Bakraoui brothers were born in Brussels and raised in Laken, a residential district in northwestern Brussels. Their father, a retired butcher and devout Muslim, emigrated from Morocco; their mother was described as "conservative and reclusive". The brothers were known to the Belgian authorities. They were believed to have rented an apartment that housed some of the assailants involved in the November 2015 Paris attacks and supplied ammunition for them. Ibrahim

died in one of the suicide bombings at Brussels Airport, while Khalid died in the suicide bombing at the metro station. Both of them had evaded capture during a police raid in Brussels on 15 March 2016.

Ibrahim

He was involved in the attempted robbery of a currency exchange office in January 2010, where he shot at police with a Kalashnikov rifle while providing a lookout for his accomplices. One police officer was shot in the leg but survived. Ibrahim was sentenced to 10 years in prison, but was released on parole in 2014 under the condition that he will not leave the country for longer than a month. He failed to abide by the conditions of parole and was sought again by the authorities. According to the authorities in Turkey, they arrested Ibrahim as a "suspected terrorist" in June 2015 and deported him to Europe. Belgian authorities were informed of the detention and deportation, but they apparently ignored the warnings, and the Netherlands released Ibrahim after failing to establish any link to terrorism.

Khalid

Khalid was one of three men involved in a bank robbery on 27 October 2009, in which they kidnapped an employee and forced her to drive them to her workplace in Brussels and deactivate the alarm. They made off with €41,000. About two weeks later, Khalid stole a vehicle and was later found with it and a number of other stolen vehicles in a warehouse. Khalid was also arrested in 2011 for the possession of Kalashnikov rifles. In September 2011, he was convicted of the carjacking, the weapons possession, and the 2009 bank robbery, being sentenced to five years in prison. Following his release, Khalid was arrested upon meeting with a former criminal accomplice in May 2015, which violated a term of his parole. Interpol issued a warrant for his arrest in August 2015. Two further arrest warrants were issued for Khalid on 11 December 2015, one international and one European. Both were issued by a Paris judge investigating the November 2015 Paris attacks, because Khalid rented the Charleroi house where fingerprints of Abdelhamid Abaaoud, the mastermind of those attacks, as well as an involved suicide bomber, Bilal Hadfi, were found. On 16 March 2016, the Federal Bureau of Investigation informed Dutch authorities that he was wanted for "terrorism, extremism and recruitment".

Najim Laachraoui

Najim Laachraoui (also known under his cover name, Soufiane Kayal; was confirmed to be one of the two suicide bombers at the airport on 23 March. He was born in Morocco but raised in the Schaerbeek neighborhood of Brussels, where he studied electromechanical engineering at a local Catholic high school. He reportedly travelled to Syria in February 2013, resulting in the mayor of Schaerbeek declaring that Laachraoui had been removed from the voting rolls in 2015, but being "powerless to do more." Like the Bakraoui brothers, he evaded capture during the police raids on 15 and 18 March 2016 which captured Salah Abdeslam. Laachraoui is believed to be an accomplice of

Abdeslam's, with whom he travelled across Europe under the false identity of Soufiane Kayal. Laachraoui is also believed to have made the suicide vests used in the Paris attacks.

The Path on Which Daesh Will March On...

After the Brussels Attacks, intelligence officials from Europe and Iraq reveal that at least 400 trained fighters have been sent to attack Europe, deploying interlocking terror cells like the ones that struck Brussels and Paris. The mission and order: to choose the time, place and method for maximum carnage.

At any rate, in a realistic assessment, Brussels had it coming. Belgium's Home Minister had warned last week that the latest catch of a terrorist did not mean that the terror threat had died down. He was proved right sooner than he expected".

After the Brussels Attacks, intelligence officials from Europe and Iraq reveal that at least 400 trained fighters have been sent to attack Europe, deploying interlocking terror cells like the ones that struck Brussels and Paris. The mission and order: to choose the time, place and method for maximum carnage.

Before being killed in a police raid, the ringleader of the November 13 Paris attacks claimed he had entered Europe in a multinational group of 90 fighters, who scattered "more or less everywhere." And the objective appears to no longer limit to be killing as many people as possible but also to have as many terror operations as possible.

The world of violent jihadism is a competitive one, and IS's greatest rival has always been al-Qaeda. Their antagonism has many roots, some going back decades, to the war in Afghanistan, but it is today expressed both as literal war in Syria, where they fight for territory, and as a broader but more abstract war of ideology, over which group can rightfully claim the mantle of jihadism's global vanguard..

Daesh, (ISIS itself hates the name Daesh - not just because it downgrades its claim to being the "Caliphate", but also because "Daesh" sounds similar to the Arabic word "dahes", which is translated as "someone who sows discord") was probably always going to lose its "caliphate." The group simply does not have the resources or capability to run a mini state for long. It is surrounded by enemies who are far more powerful and bent on its destruction.

For the past year, we've been watching the ISIS mini state crumbling right before our eyes. As that happens, the group's leadership seems to have concluded that its best response, in simple strategic terms, is to coordinate large-scale terrorist attacks abroad: 100 people in Ankara, a Russian airliner over Egypt, 43 people in Beirut, the Paris attack.

"If an extremist group that has seized territory starts to lose it, it will be highly incentivized to turn to terrorist operations that allow for maximizing effects at a lower cost," Clint Watts, another terrorism expert, wrote in War on the Rocks shortly after Paris.

Daesh is all but certain to continue losing ground in Iraq and Syria, and its efforts to establish new "caliphates" seems doomed as well. It survives, ideologically and militarily, on momentum, and that momentum will inevitably shift into more large-scale attacks against civilians, including in Europe.

Wi-Fi offered free in public places poses a major security risk

A researcher armed with a mere $100 (about Rs 6,400) device recently walked into the Bengaluru airport and confirmed fears of security risk associated with offering free Wi-Fi at public places. He easily hacked into the computers of hundreds of users who had connected to the airport's complimentary WiFi. And while he was at it, he also accessed the users' WhatsApp conversations, credit card numbers and encrypted user names and passwords for good measure.

This casts a dark shadow over the government's plan to offer free WiFi in 2,500 cities and towns across the country. Among other users, thousands of senior level executives including CEOs of companies may be sharing confidential information such as business plans without being aware of it. Some of them may even be the target of corporate espionage, cyber security experts said.

According to Shubho Halder, chief scientist at mobile security firm Appknox, who conducted the exercise at Bengaluru airport, most airports and free WiFi hotspots in India are a hacker's paradise owing to lack of proactive security. Halder, who said he had also found security holes in products from Apple, Microsoft and Google, added that he found users accessing their corporate emails and banking applications at the free WiFi zones and he managed to get all such details in a jiffy.

WiFi offered free in public places poses a major security risk "While these airports use a lot of security tools, they usually do not track what the users are doing with the WiFi connection which lets hackers use fake WiFi hotspots to gather tons of information from unsuspecting victims," Halder told ET. Halder used WiFi Pineapple, a portable device which acts as a router and creates fake WiFi hotspots that appear to be authentic — such as Free_airport_WiFi, Free_cafe_WiFi, etc. Once the user connects to this network, he or she is able to access the internet as usual without realising that somebody else is accessing all the information.

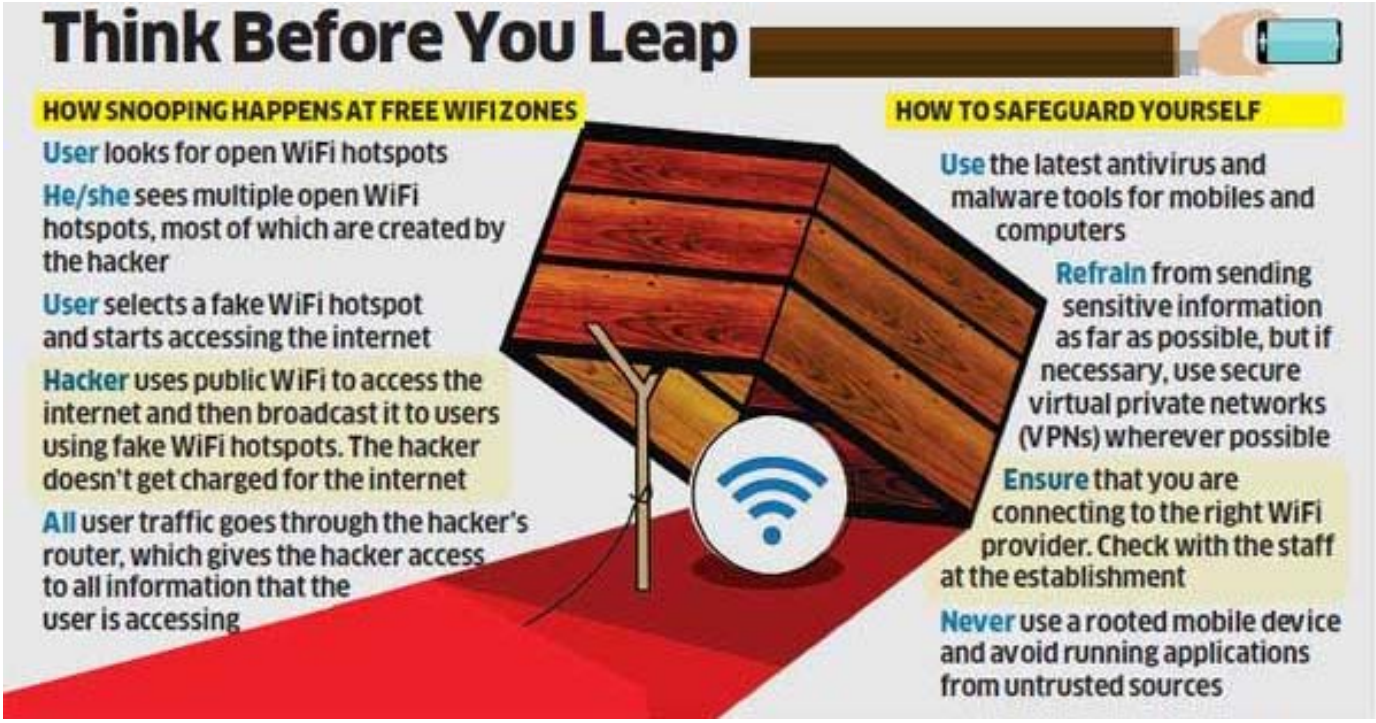
WiFi Pineapple can be carried by hackers around offices of large companies, coffee shops, malls, etc and create massive repositories of usernames, passwords, WhatsApp conversations, and credit card and banking data.

"Hackers are not just randomly collecting data at airports and cafes. We've seen cases where hackers are going after specific targets to steal business plans as part of corporate espionage and then sell it to competitors, which could be in India or overseas," said Jayaraman Kesavardhanan, founder and CEO of K7 Computing. According to American networking equipment maker Cisco

Systems, which is working with the government on many public WiFi projects, the company has the tools to identify such fake Wi-Fi hotspots and even locate the user who is trying to do this but smart hackers can get their way around it. "If a hacker uses a 3G or 4G router to offer a fake WiFi hotspot, there is no way to detect or stop it. The only thing that can be done is to tell users not to use any WiFi hotspot that doesn't ask for SMS verification," said Pravin Srinivasan, lead-security architecture sales, Cisco India SAARC.

In many cases, while the public hotspot providers have tools to prevent such misuse they often don't activate it, Srinivasan said, adding, "The tools can only tell you what's happening. It is ultimately up to the security teams of the public WiFi providers to monitor and take action." While there are ways to fix security bugs, there is no way for users to tell if they are the target of snooping. "We should consider public Wi-Fi as raw internet," said Sajan Paul, director-systems engineering, India SAARC at Juniper Networks.

"At an average end-user level, it is very difficult to detect such scenarios. However, one must understand that anything that goes into the Internet is subject to snooping and other forms of attacks. The user should be vigilant while accessing and sending sensitive data over such mediums."



According to Symantec Corporation, deployment of security tools is not enough to deal with the menace of snooping in free WiFi zones. "Individual security products cannot help companies handle such a situation," said Tarun Kaura, director-technology sales, India at Symantec.

Read more at:
http://economictimes.indiatimes.com/articleshow/47350035.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

'Divyachakshu' (divine eye): Through Barrier Imaging Radar

In what can prove to be a great aid for the Indian forces in dealing with hostage situations, India's premier government R&D body DRDO has developed radar that can look through a wall.

The Through Barrier Imaging Radar, named Divyachakshu' (divine eye), has been developed by defence Research and Development Organization's (DRDO) Electronics & Radar Development Establishment (LRDE) based in Bangalore and is going through development trials now.

"The radar can produce images from the other side of the barrier up to a distance of 20 meters. It catches the thermal signatures and movements in a room can be clearly seen," a scientist working on the project told IANS on condition of anonymity.

The radar tracks heat on the other side of the wall and gives real time thermal image, which can disclose the movement, number of people and other important information about the situation on the other side of the barrier.(ALSO READ: India test-fires indigenously developed interceptor missile).

"In a hostage situation, the radar can help give an idea about the number of people inside the room and their movement," the scientists said.

According to experts, the nature of movements can help in locating the terrorists and differentiating them from the hostage. The development of the radar was triggered by the Mumbai terror attack of November 2008, where terrorists took hostages at several locations, including hotel Taj Mahal, Oberoi Trident and Nariman House. The device will also prove useful in situations such as the recent attacks in Gurdaspur, Punjab, where terrorists entered the Dina Nagar police station, or the Pathankot airbase and two of the terrorists went on to hide in a building. The project was started in 2010 and the development trials are expected to conclude by the year end.

"We are looking at the Army, the BSF and paramilitary forces as the buyers," the scientist said. The Indian Army at present does not have such an equipment. Apart from the distinction of being indigenously developed, the equipment cost is low. The scientist said the device costs around Rs. 35 Lakh, while similar devices in the international market cost around Rs. 2 crore. Efforts are also on to bring down the weight of the device from present 6-7 kg. The device will also prove useful in situations such as the recent attacks in Gurdaspur, Punjab, where terrorists entered the Dina Nagar police station, or the Pathankot airbase and two of the terrorists went on to hide in a building.