willingness to blow themselves up in suicide attacks.[12] Indeed, on account of the failings of the nationalist insurgent projects of the 1990s, they seem to have none of the specific political goals of groups such as the LIFG. Rather, given the strict confines in which they can operate, these individuals appear bent upon destruction in some vain promise that they will achieve paradise.

Although the appearance of such militants is most pronounced in countries such as Morocco or Algeria, Libya has not been immune. Reports have emerged in recent years about young men blowing themselves up to evade capture by the security services. Qadhafi's son, Saif al-Islam, confirmed how in June 2007 three young militants exploded themselves in a house in Derna and in the same year clashes were reported between militants and members of the police in Benghazi. There are also many Libyans who joined the jihad in Iraq, and there are countless stories of martyrdom celebrations being held in Libya by the families of those who have died in Iraq.

For these militants, the LIFG's revisions are unlikely to have a significant impact. It is true that the LIFG are regarded as heroes by some parts of the population; the fact that they fought in Afghanistan and have suffered in Libyan prisons gives them a degree of credibility. Yet by striking a deal with the regime, many will accuse them of being co-opted by the state. Perhaps more importantly, given the low education levels of many of these young radicals, they will have a difficult time understanding such a scholarly document as the revisions.

Moreover, the majority of today's Libyan militants and volunteers for the Iraqi jihad have come from the country's eastern regions—an area that provided the bulk of support for the LIFG when it was in its prime and an area that has traditionally had an antagonistic relationship to the center. As such, it would appear that while it is impossible to pinpoint exactly what drives someone to militancy, there are a number of underlying grievances related to internal regional factors in Libya that have yet to be resolved. As a result, while the issue of militancy in Libya should not be overplayed, it is certainly a problem that is likely to persist for the foreseeable future.

In conclusion, the LIFG revisions are a positive step for both the group itself and for the Libyan authorities. Yet they are unlikely to have any real impact on militancy in the region and beyond.

Alison Pargeter is a Senior Research Associate at the Centre of International Studies at the University of Cambridge. She is currently running a project on radicalization in North Africa that is funded by the UK's Economic and Social Research Council. She has published widely on issues of political Islam and radicalization. Her book, The New Frontiers of Jihad: Radical Islam in Europe, *was published by I.B. Tauris in 2008 and her forthcoming book on the Muslim Brotherhood is due to be published by Saqi Books in 2010.*

12 For example, data provided to the author in 2007 and 2008 by local human rights groups in North Africa regarding those arrested on terrorism charges reveal that the vast majority have extremely poor education levels with many only educated to primary school level. Although many of the LIFG rank-and-file were also poorly educated, the group also comprised graduates and those who had received an Islamic education in Saudi Arabia or elsewhere.

Rethinking Strategies to Secure U.S. Critical Infrastructure

By Charles Faddis

THERE IS AN ALMOST endless list of potential terrorist targets in the United States. The most concerning of these targets, however, are those loosely classified as critical infrastructure. There are a large number of such sites, and the potential impact of a successful attack on many of them would be catastrophic. An attack on the rail system in the Northeast Corridor, if effectively carried out, would kill hundreds if not thousands and cripple the transportation sector in a key region of the United States. Commuters would be stranded. Freight would not move. Economic costs would amount to the billions of dollars. Nuclear power plants scattered across the country are another concern due to the horrible effects of a disaster. Moreover, the United States is dotted with major chemical facilities, which are, in effect, giant prepositioned weapons of mass destruction. Railroads carry thousands of railcars jammed with similar types of chemicals. As warned by the Department of Homeland Security, a single rail car filled with chlorine has the capacity to kill 17,500 people.[1]

To prevent attacks on these targets and avoid the loss of life on an almost unimaginable scale, it is imperative that further defenses be instituted to frustrate terrorist attack plans. To accomplish this, however, it is first necessary to understand the nature of the threat and the way in which the enemy fights. Attacks planned by Islamist terrorists may involve limited physical surveillance, and the enemy will likely be prepared to die to carry out the mission successfully. Faced with this type of enemy, many of the United States' current security measures are not sufficient to counter this threat.

This article argues that more attention should focus on physical security such as explosives detection dogs or hard barriers to critical infrastructure. It explains why current security measures

1 David Howe, "Planning Scenarios," The Homeland Security Council, July 2004.

are not sufficient, and then suggests some steps for moving forward.

Current Security Policies Not Sufficient

In the 2004 Madrid and 2005 London terrorist attacks, terrorists boarded trains carrying explosive devices concealed in backpacks and bags. The terrorists themselves spoke the local language, dressed in Western clothes and blended into their environment.

"The premium must be on guards, physical barriers, metal detectors, explosives detection dogs, and related measures, and less on cameras, signs and observation. Against an enemy that relies more on shock, violence and surprise than it does on sophistication or finesse, it is essential to employ similarly tough defensive measures."

They did nothing to attract attention. In Madrid, they left the bags and exited the trains. In London, they chose to detonate the bags themselves and commit suicide.

Despite this, in the United States many of the security measures in place seem to be predicated on an expectation of being able to detect and neutralize terrorists in the run-up to an attack. One example of this is a security program initiated by a major rail system in the United States that allows uniformed and off-duty plainclothes law enforcement to ride trains free of charge as a deterrent to potential terrorists. The implementation of this measure is a perfect illustration of the lack of understanding of terrorist methodology that characterizes much of what passes for security today. What would a police officer in a uniform or in plainclothes sitting behind a suicide bomber—who would not be distinguishable from other passengers—do to stop such an attack? The officer would find out there was a bomb on board when every other passenger did: when it detonated.

Moreover, detecting a terrorist during the planning phase is also extremely difficult. There is much discussion in law enforcement and homeland security circles about the terrorist attack cycle and the necessity to detect and neutralize terrorists while they are preparing for an operation. While these detection practices are necessary and important, they gloss over the difficulty of detecting a terrorist involved in pre-attack surveillance and also greatly over-emphasize the amount of preparation that is likely to occur.

A rank amateur with aspirations to martyr himself may board a train in such a manner and behave in such a way as he prepares to carry out an attack that will allow a police officer to correctly identify and apprehend him before he takes action. Yet an operative of even marginal competence will not do so. He, or she, will dress and act and speak appropriately enough to blend into the surrounding population. In the run-up to the attack, the terrorist will board the train, ride it as far as needed to gather data and then disembark and go home. An experienced terrorist will not stand and stare or take photographs where they should not or draw diagrams of a station platform while standing in view of a security camera. In short, the operative will not do anything while conducting surveillance in preparation for an attack or as he boards the train on the day of the attack that will appear out of the ordinary to an observer. For law enforcement, it is not just looking for a needle in a haystack; it is looking for a needle in a pile of identical needles.

It is also likely that the number of such pre-attack visits to any particular site will be limited. A U.S. special operations team preparing to attack a target will undertake extensive pre-attack surveillance. The team will use overhead imagery, reporting from clandestine assets and the results of surveillance conducted over a lengthy period of time by trained operators to allow for the preparation of the best possible plan of attack. Attributing that same kind of methodology to terrorist attack teams is a mistake. Certainly, terrorists want to have information on the target they are going to strike, but the level of detail they typically acquire in advance of an attack is much less than what U.S. military or intelligence teams would judge sufficient. Much of that information will derive from open sources, from casual observation and from individuals who, largely by chance, happen to have access to the target. In fact, in many cases, it is probably more accurate to say that the target is chosen at least in part by virtue of the amount of information available about it than it is to say that the target is chosen and then information is compiled on it. There may, in fact, be a certain amount of directed, "formal" surveillance of the target, but it will likely be much less extensive in both time and scope than is often assumed.

A perfect illustration is the case of the individuals arrested for planning an attack on Fort Dix in New Jersey in 2007. The preparation for those attacks consisted of a few casual visits to military installations and the compilation of what U.S. analysts would consider a very limited amount of information on the potential targets. The terrorists' ultimate selection of Fort Dix as a target was based largely on the fact that one of them already had access to the facility as a pizza delivery man.[2] Their visits

"While these detection practices are necessary and important, they gloss over the difficulty of detecting a terrorist involved in pre-attack surveillance and also greatly over-emphasize the amount of preparation that is likely to occur."

to other installations hardly qualified as anything other than drive-bys, were extremely limited in duration and would have been almost impossible to detect. In the end, they were not captured because of their actions while casing prospective targets, but because of good intelligence work and the actions of an undercover officer. The same is true in

2 "Fort Dix Plotter Spoke of Bombs on Tape," Associated Press, October 29, 2008.

the recent Najibullah Zazi case, where attacks were prevented not because of pre-attack preparations, but because intelligence reports gave forewarning that Zazi had traveled to Pakistan and been trained in an al-Qa`ida camp.[3]

Moreover, terrorists intent on attacking the United States would likely be prepared to die during their mission, which means that they will not need to case targets extensively enough to find an escape route. One example is the attack on the U.S. Consulate in Jidda, Saudi Arabia in 2004. The team of attackers mounted a furious assault on the site with the express goal of killing every American inside.[4] Nothing in the attack suggests any planning for extraction or withdrawal.[5] From the moment the attack began, the one near certainty was that every member of the assault team was going to die.

Moreover, the nature of the terrorists' objectives often obviates the necessity for extensive pre-attack surveillance. If a U.S. Special Forces team is focused on the destruction of a specific, transient target, it may require a large amount of data to plan an effective operation. Terrorists, particularly Islamic extremists, are rarely interested in mounting any such operation. They care about killing people in large numbers and spreading terror.

A case in point is the Mumbai attack of 2008. From the moment the shooting began, the attackers were intent on one goal: killing as many people as possible. When they opened fire with automatic weapons in the middle of a crowded train station, they did not know the identities of anyone they were shooting. The amount of pre-attack surveillance required to mount such an operation is minimal. The same can be said in regard to the hotel targets hit, which were chosen primarily because they catered to upscale, largely Western tourists. When the target is one that is open to the public and employs literally hundreds of individuals from the surrounding community, as is the case with many soft targets, little pre-attack surveillance is necessary.

Even attacks on major economic targets are launched with what Western analysts would consider a rather crude understanding of the target. When al-Qa`ida struck the Abqaiq oil facility in Saudi Arabia in 2006, they employed extensive resources. They used two separate vehicle borne improvised explosive devices (VBIED) and a separate assault team to overwhelm the Saudi guards. Yet when they were successful in forcing their way into the site, they ultimately detonated their devices at locations that produced nothing like the kind of damage that could have resulted had the VBIEDs been exploded a relatively short distance away.[6] The attackers simply did not understand the facility well enough to know exactly how to cripple it.

"For law enforcement, it is not just looking for a needle in a haystack; it is looking for a needle in a pile of identical needles."

Moving Forward

The enemy is fanatical, determined and creative. They will likely base attack plans on what Western analysts would consider limited information, much of it compiled through methodologies rather than extended physical surveillance. Even when the operations are relatively complex, the bulk of the information required will be gathered through means that are difficult for authorities to detect. A target may in fact be chosen not so much because it is the best possible choice, but because it is one the actors know already and to which they may have some degree of natural access. When the attack comes, however crude, it will be executed with vigor no matter what the odds.

In this context, efforts to detect pre-attack surveillance or other preparations are necessary, but likely to be of little value. What is of value, however, are measures that can physically prevent a successful attack. The premium must be on guards, physical barriers, metal detectors, explosives detection dogs, and related measures, and less on cameras, signs and observation.

This would establish a layered, integrated defense consisting of uniformed and plainclothes officers, combined with explosives detection dogs screening all passengers as they enter a train station or other mass transportation facility. Moreover, rather than focusing on security cameras at chemical plants and other critical infrastructure, these facilities should be gated and guarded, and protected by remotely activated barriers that can prevent entry of a truck carrying a bomb.

Against an enemy that relies more on shock, violence and surprise than it does on sophistication or finesse, it is essential to employ similarly tough defensive measures. Failure to move in this direction only creates a false sense of security, and leaves only hope that a terrorist attack will not occur.

Charles S. Faddis is a retired Central Intelligence Agency operations officer and the former head of the CIA's WMD terrorism unit. He spent 20 years as an operative in the Near East, South Asia and Europe and led the first CIA team into Iraq in advance of the 2003 invasion. He is the author of a recently released book on the CIA entitled Beyond Repair *and the coauthor of a book on the actions of his team inside Iraq in 2002-2003, entitled* Operation Hotel California. *His next book,* Willful Neglect, *is an examination of homeland security from an operator's perspective and will be released in early 2010. He runs his own security consulting business, Orion Strategic Services, LLC.*

3 "AP: CIA Learned of Zazi, Tipped Off FBI," CBS News, October 6, 2009; Richard Esposito, Clayton Sandell and Brian Ross, "Official: Terror Plot Suspect Admits al Qaeda Ties, May Plead Guilty," ABC News, September 18, 2009.

4 "Jeddah Consulate," Global Security, October 13, 2009.

5 Roger Harrison, Essam al-Ghalib and Hassan Adawi, "US Consulate Attacked," *Arab News*, December 7, 2004.

6 Personal interview, confidential source, Spring 2009.