In a failed attempt to capture Paris attacker Saleh Abdesalem, investigators in Belgium seized about 10 hours of video footage of the residence of an executive who worked at a nearby nuclear power facility. Belgian experts were able to say with confidence that the footage was taken by a clandestine, unmanned fixed camera hidden in a wooded area near the executive's home, but off his property.

Later investigation after the Brussels bombings determined that the surveillance had been conducted by one or both of Brussels suicide bombers, Khalid and Ibrahim Bakraoui. Some analysts believe the video footage must have been part of pre-operational surveillance for a planned attempt to place the executive under duress in a "tiger kidnapping" scenario to force him to give the terrorists access to the facility or to radioactive materials.

Stratfor, authors of this article, have no quarrel with that speculation: There are few other credible explanations for the terrorists' actions. They remain skeptical, however, that the terrorists would have succeeded in any nuclear-focused operation. We are most interested in how fixed, unmanned camouflaged video camera, deployed off the property, have been used to collect large amounts of information about the executive, his family, their movements and schedules, and their residence.

"While such operations are commonly used by law enforcement, military and intelligence teams, they appear to be new in the terrorist toolbox, something we want to draw to the attention of chief security officers.

"As we have written many times, the terrorist and criminal attack cycles always include a period of pre-operational surveillance during which hostiles collect information needed to plan an effective attack, whether it be an assassination, a kidnapping or some other hostile operation.

"We also say that of all the different forms hostile surveillance tasks, fixed surveillance is the most difficult to detect because it does not react to the target's actions. The use of unmanned cameras adds a new and more powerful dimension to fixed surveillance. Once inserted into a "hide" there is no need for a human presence to operate them. Moreover, modern battery technology has minimized servicing requirements. State of the art devices are very small, very powerful, and easily hidden in a natural environment. Access to such devices is not restricted to official use: Everything from inexpensive but powerful infrared capable game cameras to tiny

surveillance cameras are available on the open market.

"For conducting early-stage preoperational surveillance against a fixed target such as a residence, the use of technology versus human eyes-on surveillance can drastically reduce the risk of discovery by security teams. Generally, we are trained to look for people and vehicles, and telltale behaviors, not tiny, silent, skillfully camouflaged devices in a rural or outdoor setting. However, countermeasures do exist, and should be used routinely to mitigate this threat.

"Once in place and well-hidden, surveillance cameras are invisible to the casual observer. But the one thing that must not be obscured with camouflage is the lens or lenses, otherwise the device is useless. This makes it vulnerable to trained, careful scrutiny, no matter how well hidden it is. "If it can see you, you can see it" should be the operating principle. Paradoxically, devices once in place may be more vulnerable after dark than in daylight. Some of these cameras by design emit infrared light to facilitate night-time recording. An ordinary off-the-shelf night vision device (NVD) will detect infrared light, so regular scans around and near a facility with an NVD are recommended.

"Another vulnerability of fixed technical surveillance in a rural setting is the time when the device is inserted; when it is serviced (although some devices operate without servicing for as much as a month); and when it is extracted. These are the times when a human presence is required. The skills required to insert, service and extract a fixed device without being detected by alert security teams require different training from that of conventional surveillance operators, more akin to that given combat snipers.

"In Northern Ireland during the IRA insurgency, for example, British surveillance teams were divided into two types with different missions, urban and rural. The rural surveillance teams were able to accomplish astonishing things, but their successes were hard-won through intensive training and long experience. We feel safe in saying that neither terrorists nor criminal gangs at present will have skills at that level, meaning alert, situationally aware security teams have a good chance of detecting rural technical operations during insertion, servicing and recovery. Professional training in tracking skills can also be of help. As trackers say, nothing moves through the woods without leaving "sign," and humans leave most noticeable tracks of all.

"Importantly, the camera targeting the Belgian executive was placed off his property. We have long said that effective security operations pay due attention to the most outer ring of security:

off-property, an area many ignore to their peril."