Avoiding Surveillance Abroad

Product of the Research & Information Support Center (RISC)

Targeting Recognition

Any person traveling abroad on business should be aware of the fact that they could be targeted by an intelligence agency, security service, or even a competitor if they are knowledgeable of, or carrying, sensitive or proprietary information. In the course of doing business abroad, there are certain indicators that should be recognized as potential hazards and indicative of unwarranted interest in your activities. These situations should be closely scrutinized and avoided if at all possible. A few of the most common scenarios that have been used by intelligence/security services and have led to successful targeting and acquisition of information are listed below:

- Repeated contacts with a local or third-country national not involved in your business interests or the purpose of your visit, but who, as a result of invitations to social or business functions, appears at each function. This individual's demeanor may indicate more than just a passing interest in you and your business activities.

- A close personal social relationship with a foreign national of a hostile host government is often unavoidable for business reasons. In these instances, be cautious and do not allow the relationship to develop any further than the strictly professional level.

- Be suspicious of any accidental encounter with an unknown local national who strikes up a conversation and wants to:

    - Practice English or other language.
    - Talk about your country of origin or your employment.
    - Buy you a drink because they have taken a liking to you.
    - Talk to you about politics.
    - Use other excuses to begin a "friendly" relationship.

If any of the above or anything else occurs that just does not ring true, allow yourself to be suspicious, and exercise prudence and good judgment.

Surveillance Recognition

The subject of surveillance is extremely important to anyone conducting business abroad. Surveillance could be indicative of targeting for reasons other than interest by a foreign intelligence or security service. Terrorists and criminals also use surveillance for operational preparation prior to committing other terrorist or criminal acts. It should be noted, however, that the normal business traveler, who only spends a few days in each city and has a low profile, is not generally a viable target for terrorists. The real terrorist threat to a traveler is that of being at the wrong place at the wrong time, and becoming an inadvertent victim of a terrorist act.

Surveillance is an assessment of vulnerabilities in an attempt to determine any information available, from any source, about you or your activities, such as lifestyle or behavior that can be used against you. If the intended target recognizes that s/he is under surveillance, preventive measures can be taken that will hopefully deter further interest. As an example, if the surveillant(s) realizes they have been spotted, then the assumption must be that the operation has been compromised, and that the police have been notified or other preventive measures have been taken. On the other hand, if a traveler is being scrutinized by a foreign intelligence or security agency, the surveillance may well continue.

Surveillance takes many forms, from static (such as an observer physically or electronically watching or monitoring your activities in your hotel room or office) to mobile (where the individual being watched is actually followed either on foot or by vehicle).

There is only one way to recognize surveillance: remain alert to your surroundings. As a traveler, you probably will not be at any one location long enough to know what the norm is, and this puts you at a disadvantage. You will not realize that the person sitting in the car across the street is a stranger and should not be there, whereas a resident may immediately become suspicious.

Be observant and trust your instincts. If something doesn't feel right, chances are it's not. Report your suspicions or any information to the security manager of your organization in case something does occur. If there is any question about what actions should be taken, and guidance is not available from your security office, contact your embassy or consulate and they will advise you as to what you should do and whether or not the information should be

reported to the local authorities. However, the most important thing you should do is ensure your demeanor remains professional and everything you do is above board and not subject to compromise.

If you have reason to believe that you are under surveillance, here is what you should NOT do:

- DO NOT try to slip away or lose the followers. Doing this will probably alert them and gave a false impression that you are just a business traveler or tourist.

- In your hotel, assume that the room and telephone are being monitored. DO NOT try to play investigator and start looking for electronic listening devices. This again could send the wrong signals to a surveillant. Just make sure that you do not say or do anything in your hotel room that you would not want to see posted on the Internet.

Response to Targeting

If you have any reason to believe that you are targeted by an intelligence or security service, there is really only one course of action to follow: report your suspicions to your security office or embassy/consulate, and follow their guidance.