

Foreign Travel & Counter-Intelligence Briefing



FOREIGN TRAVEL

&

COUNTER-INTELLIGENCE

BRIEFING

Foreign Travel & Counter-Intelligence Briefing

BE A SMART TRAVELER.

- Carry personal identification and any special medical information with you at all times
- Store essential medication in original containers
- Do not leave your wallet or purse unattended
- Leave your itinerary at home with a point of contact, and advise of any changes to your itinerary during your trip
- Carry international traveler's checks and always exchange currency at reputable exchanges (it is illegal to do otherwise in some countries)
- Drive carefully (you may want to apply for an international driver's license if you plan to travel extensively by car)

Foreign Travel & Counter-Intelligence Briefing

- **Observe local laws and customs.**

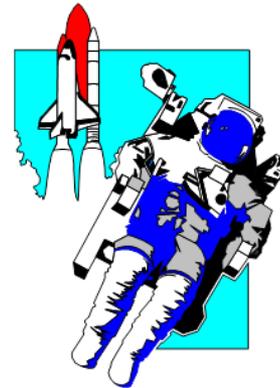
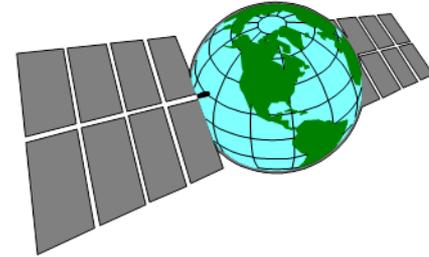
For example:

- **In Turkey, Taiwan and Spain individuals are prohibited from making derogatory comments about the government or its leaders**
- **In other countries it is unlawful to use insulting language or abusive gestures toward another person while driving**
- **Remember that you are representing the United States. Avoid political discussions, and remember that you may encounter anti-American sentiments**
- **Be patient rather than critical of local customs**

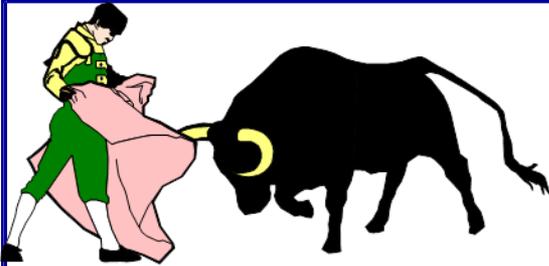
Foreign Travel & Counter-Intelligence Briefing

FACT:

- **U.S. TECHNOLOGY** is targeted by foreign nations
- It is less expensive to steal technology than it is to develop new technology
- This technology threat pertains to classified, sensitive protected, company proprietary, and other unclassified protected information

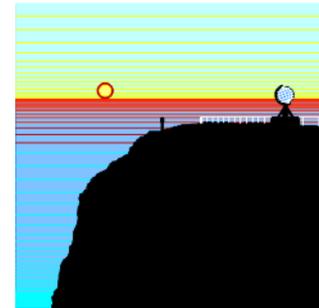
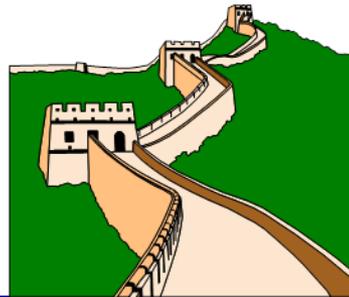
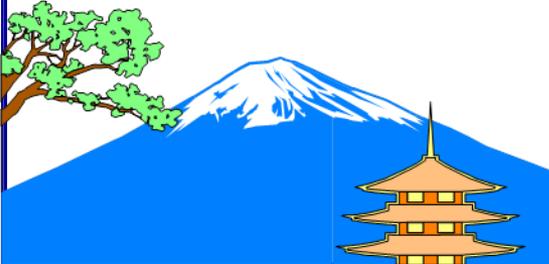


Foreign Travel & Counter-Intelligence Briefing



FACT:

- As a traveler, you are vulnerable because you may be unfamiliar with the customs, people, language, topography, laws and judicial system of that country.
- You become more dependent on strangers. This is an attractive situation for foreign agents.
- The same opportunities exist in both “friendly” and “unfriendly” countries.

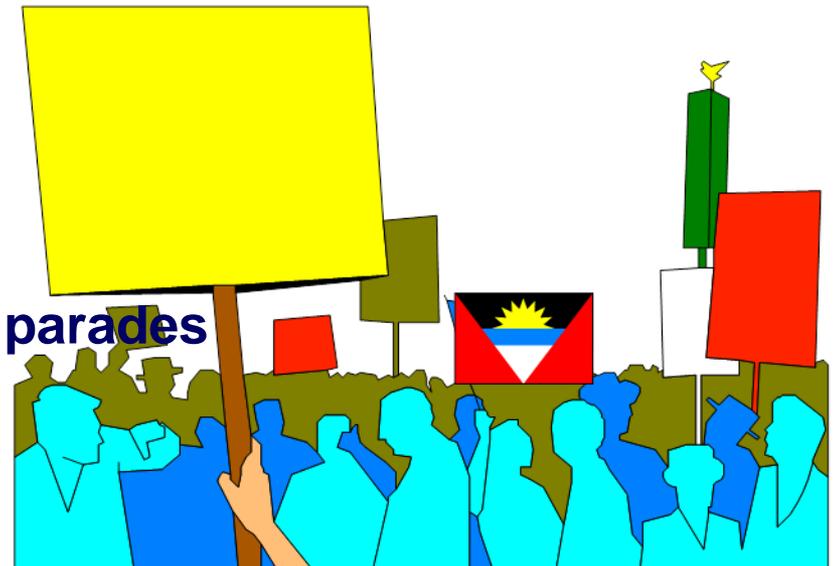


Foreign Travel & Counter-Intelligence Briefing

Do not fall into a compromising situation where outside help may be needed or threat of blackmail could surface.

EXAMPLES:

- **Involvement in Illicit currency trade**
- **Poor judgment in alcohol consumption**
- **Minor traffic violations**
- **Gambling**
- **Any immoral conduct**
- **Viewing political demonstrations or parades**



Foreign Travel & Counter-Intelligence Briefing

FOREIGN GOVERNMENT SCRUTINY OF YOU IN ANOTHER COUNTRY MAY ALSO OCCUR DUE TO:

- Your fitting the profile of a terrorist, narcotics-trafficker, or criminal.
- Involvement in black-market activity.
- Discovery by the host government of material on your person or in your luggage that is banned or strictly controlled.
- Associating with individuals the government labels as dissidents. Having language fluency, declared relatives, or organizational affiliations in the country you are visiting.

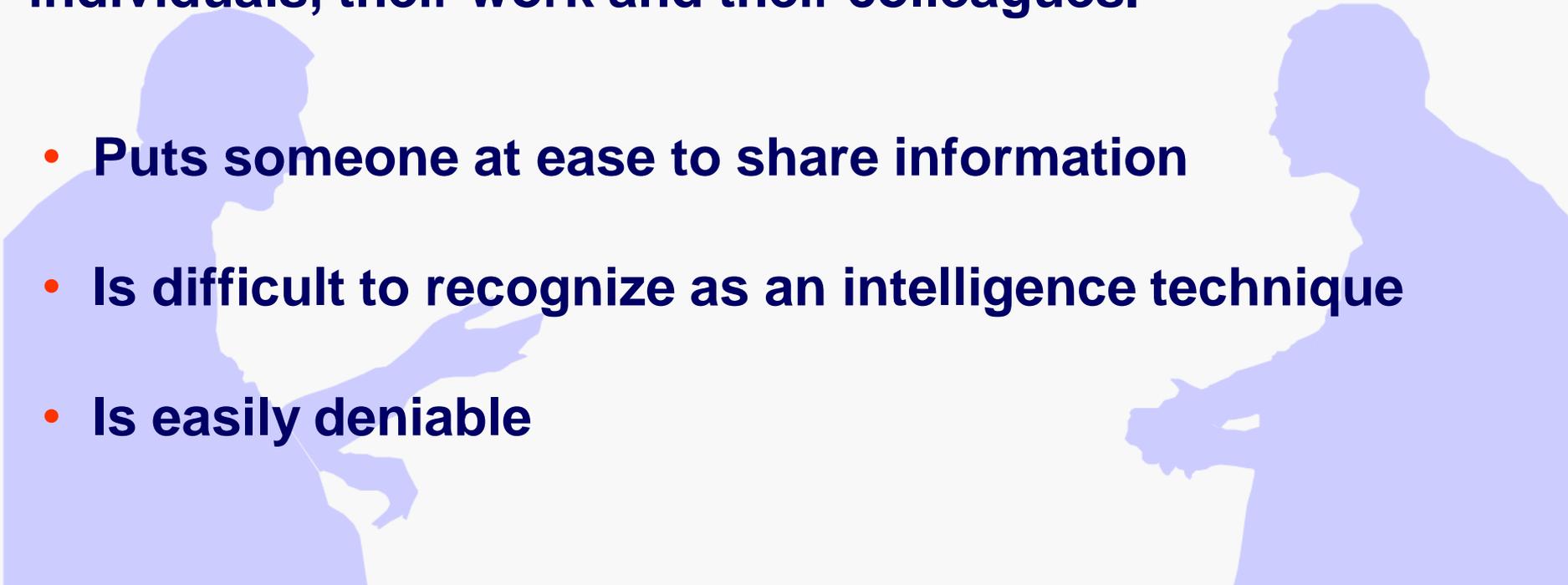


Foreign Travel & Counter-Intelligence Briefing

A COLLECTION METHOD

ELICITATION - A ploy whereby seemingly normal conversation is contrived to extract information about individuals, their work and their colleagues.

- Puts someone at ease to share information
- Is difficult to recognize as an intelligence technique
- Is easily deniable



Foreign Travel & Counter-Intelligence Briefing

- **Usually, any intelligence activities directed against you will be conducted in an unobtrusive and non-threatening fashion.**
- **Although, in some cases a foreign intelligence service may employ more aggressive provocation tactics. The methods used could be both indirect and direct.**
- **While most harassment incidents are intentionally obvious-meant to intimidate or “test” a traveler’s reactions-many intelligence activities are conducted without the target’s awareness.**

Foreign Travel & Counter-Intelligence Briefing

A COLLECTION METHOD

EAVESDROPPING – Listening to other people's conversations to gather information.

- **Frequently done in social environments where attendees feel secure and more likely to talk about themselves or their work**
- **Venues include restaurants, bars, and public transportation**
- **May occur in radius of six to eight seats on public transportation or 10-12 feet in other settings**

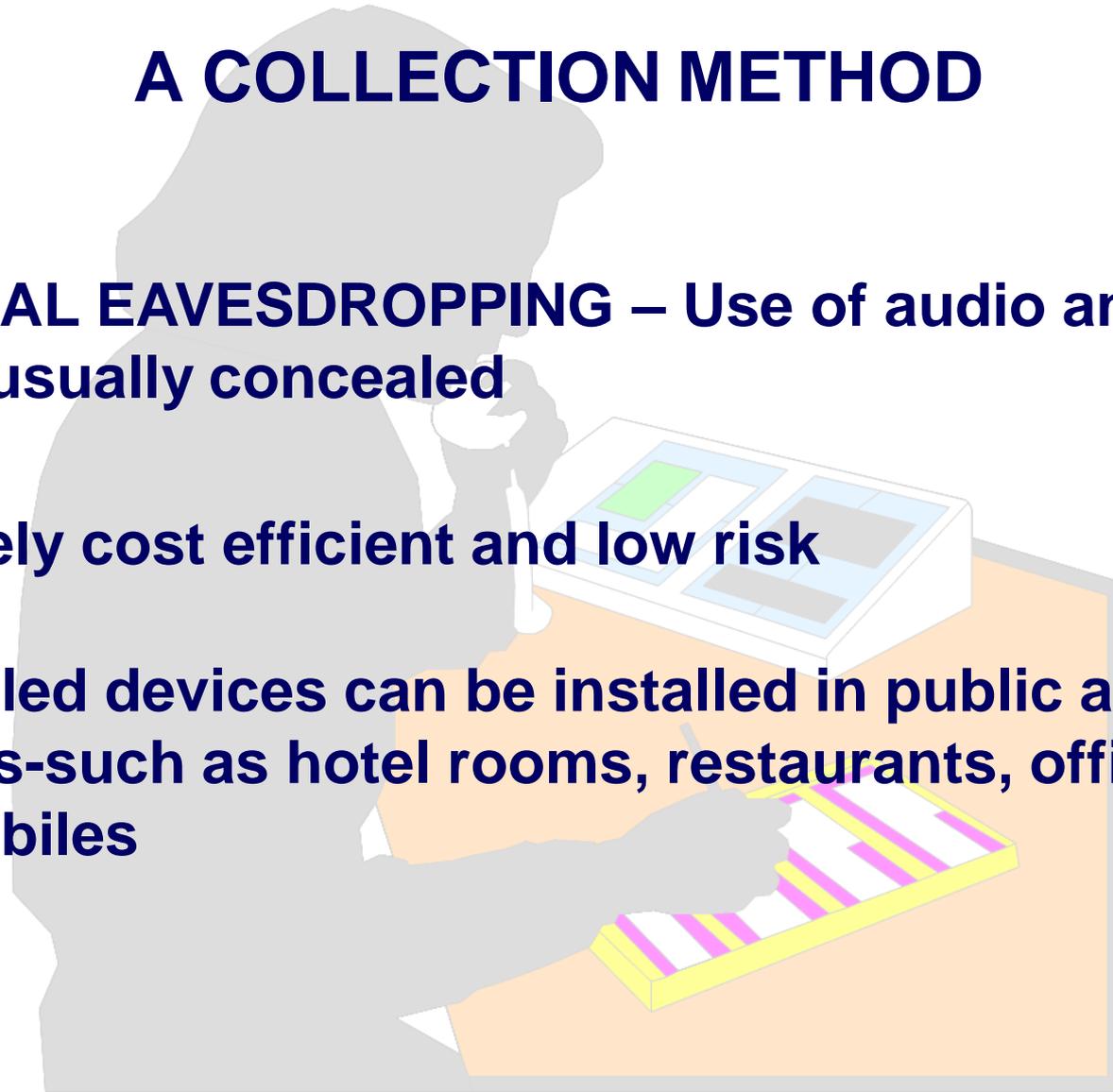


Foreign Travel & Counter-Intelligence Briefing

A COLLECTION METHOD

TECHNICAL EAVESDROPPING – Use of audio and visual devices, usually concealed

- **Relatively cost efficient and low risk**
- **Concealed devices can be installed in public and private facilities-such as hotel rooms, restaurants, offices, and automobiles**



Foreign Travel & Counter-Intelligence Briefing

A COLLECTION METHOD

“BAG OPERATIONS” – Surreptitious entry into someone’s hotel room to steal, photograph, or photocopy documents

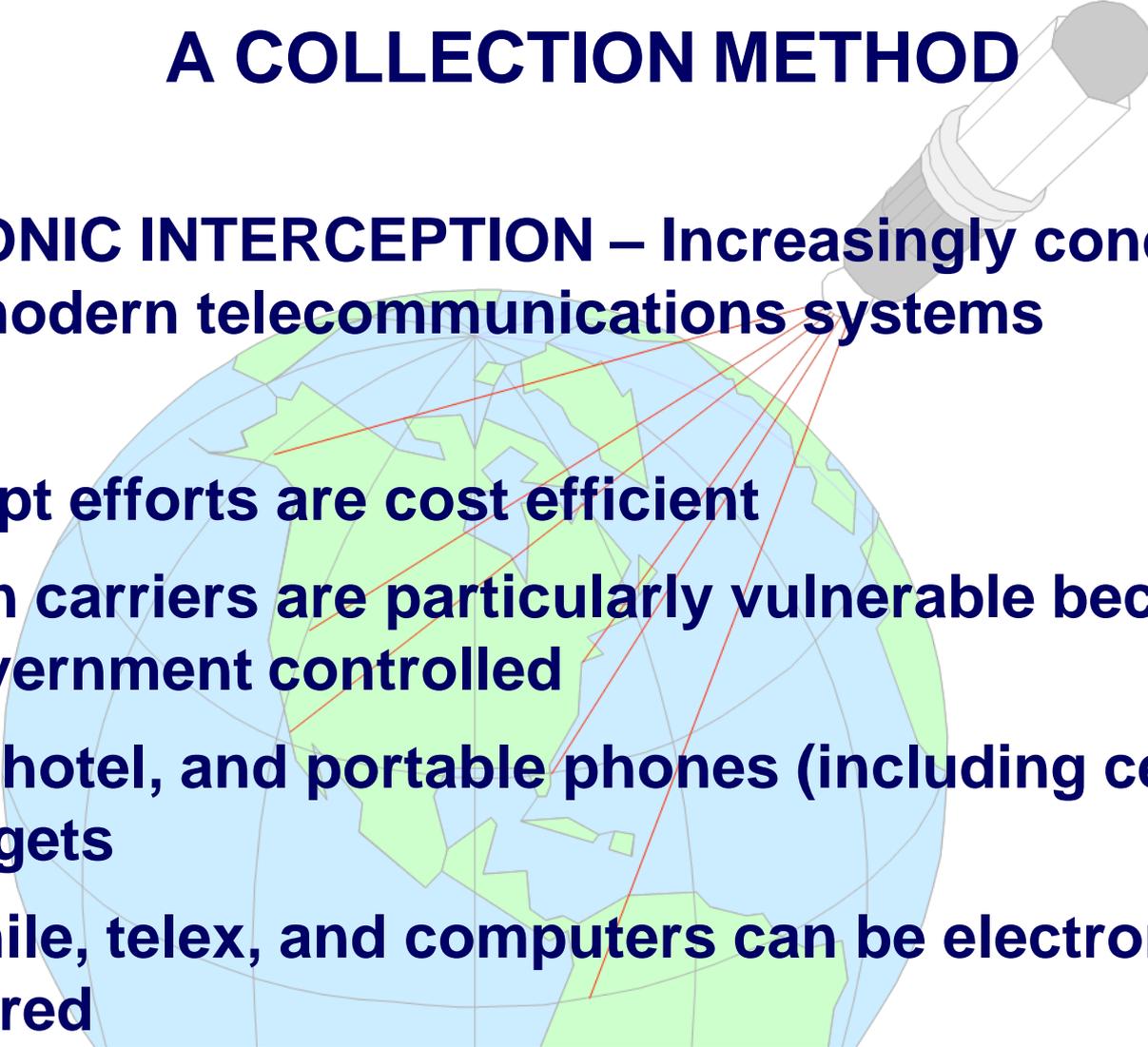
- **Many times conducted by host government services**
- **Third-country services also active**
- **Frequently done with cooperation of hotel staff**

Foreign Travel & Counter-Intelligence Briefing

A COLLECTION METHOD

ELECTRONIC INTERCEPTION – Increasingly conducted against modern telecommunications systems

- **Intercept efforts are cost efficient**
- **Foreign carriers are particularly vulnerable because most are government controlled**
- **Office, hotel, and portable phones (including cellular) are key targets**
- **Facsimile, telex, and computers can be electronically monitored**



Foreign Travel & Counter-Intelligence Briefing

SECURITY TIP

Common sense and basic counter-intelligence awareness can protect you against foreign intelligence service activities.

- Do not leave sensitive documents or equipment unattended in hotel safes-such information should be stored in appropriate secure facilities**
- Do not discuss sensitive matters outside US Offices-hotel rooms or other public venues are rarely suitable for sensitive discussions**
- Do not use computer or facsimile equipment at foreign hotels or business centers for sensitive or classified matters**
- Do not divulge information to anyone not authorized to hear it, including personal information about yourself or colleagues**

Foreign Travel & Counter-Intelligence Briefing

SECURITY TIPS

- **IGNORE OR DEFLECT INQUIRIES OR CONVERSATION**
ASK SOME QUESTIONS OF YOUR OWN
PROVIDE NON-DISCREET ANSWERS
LEAVE TALK TO SOMEONE ELSE
- **Keep unwanted material until it can be disposed of – burn or shred paper and cut floppy disk in pieces and discard**
- **Keep your personal computer as carry-on, never check it with your luggage and, if possible, remove or control storage**

Foreign Travel & Counter-Intelligence Briefing

SECURITY TIPS

- **Take time to use secure communications equipment at any appropriate U.S. Government Facility**
- **Report any counterintelligence incident to the relevant U.S. Government**
- **When traveling overseas, suspect incidents should be reported to either the U.S Embassy, Consulate or the State Department at the nearest U.S. Diplomatic Facility**

Foreign Travel & Counter-Intelligence Briefing

PROTECTING YOURSELF

- Report any attempt by a foreign national or stranger to establish a continuing association, arrange future meetings, or correspondence
- Report any contact with anyone whom you suspect may be attempting to gather 'sensitive' information from you
- Maintain a high level of personal standards and conduct... Keep in mind that you are a foreign guest and a representative of the United States

THE REQUIREMENT TO REPORT IS IN THE BEST INTEREST OF OUR COUNTRY'S NATIONAL SECURITY.

Foreign Travel & Counter-Intelligence Briefing

PROTECTING YOURSELF

- **Do not become involved in local political matters of any kind.**
- **Do not include military or other restricted areas in your visits or picture-taking tours.**
- **Avoid unknown candid or commercial photographers.**
- **Do not promise favors, such as mailing letters for strangers or hand-carrying letters or other items back to the United States for them.**

Foreign Travel & Counter-Intelligence Briefing

ONE LAST REQUIREMENT

Remember, you have an individual responsibility for safeguarding U.S. government classified or unclassified sensitive information, as well as a responsibility to protect company proprietary.