Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Be Paranoid

If you are traveling to, and working in, closed society countries you will be under attack for your information.

Whether it's their laptop which is targeted for its data; their smartphone for eavesdropping, phone calls, contacts and e-mail; or direct elicitation for what they know, they will have their pockets picked unless prepared for this culture shift.

Closed society countries, for the purposes of this article, are countries known to engage in business espionage, and who restrictions on legitimate business counterespionage protection efforts.

These tips have been gathered from a variety of sources. They also include my first-hand experiences, and correspondence with people in closed society countries to obtain definitive answers about laws governing topics like Technical Surveillance Countermeasures (TSCM) inspections.

Two important points to keep in mind.

1. Obtaining definitive answers about what is/isn't permissible is difficult. Few people with whom I communicated in these countries would answer questions about electronic eavesdropping detection directly, or would state anything with certainty. The impression I received is that they really didn't know the answers.

What they did tell me revealed that there are many levels of bureaucracy; authorities overlap each other; and the rules are open to interpretation depending upon the person or circumstance at the moment.

2. This article does not contain legal advice. (Do as I did, contact a law firm (from your country), which has local offices in the country to which you are traveling. They can best assist with you with your questions requiring legal advice.)

Background

Foreign travel always brings security questions. For many countries the advice is simple, like "don't carry too much cash," and "don't drink the water".

Some countries are far different. They want your information. These are usually, but not always, closed society countries.

This excerpt from a New York Times article is an excellent cautionary tale, and provides fourteen security tips within just two of the following three paragraphs.

"When Kenneth G. Lieberthal, a China expert at the Brookings Institution, travels to that country, he follows a routine that seems straight from a spy film.

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

He leaves his cellphone[1] and laptop[2] at home and instead brings "loaner" devices[3], which he erases[4] before he leaves the United States and wipes clean the minute he returns[5]. In China, he disables Bluetooth[6] and Wi-Fi[7], never lets his phone out of his sight[8] and, in meetings, not only turns off his phone[9] but also removes the battery[10], for fear his microphone could be turned on remotely.

He connects to the Internet only through an encrypted[11], password-protected[12] channel, and copies and pastes his password from a USB thumb drive[13]. He never types in a password directly[14], because, he said, "the Chinese are very good at installing key-logging software on your laptop."

What might have once sounded like the behavior of a paranoid is now standard operating procedure for officials at American government agencies, research groups and companies that do business in a closed society country.

Preparing Employees

Employees who understand why they are taking severe information-security precautions when they travel make the best information defenders.

Step 1: Understand the adversary and appreciate their spying capabilities.

Adversaries may be categorized into roughly six groups, with some being members of more than one group.

APT Spies (The Primary Opponent)

Advanced Persistent Threat (APT) spies are well-organized, well-funded groups; most often governments. They are most often located in "closed" countries, with direct (or close) government ties.

Their goal is to steal intellectual property. Unlike Professional Corporate Spies who seek quick financial gain, APT agents think long-term, big-picture. Duplicating their victim's best ideas and products in their homeland is the primary objective.

Professional Corporate Spies

Calling themselves everything from Competitive Intelligence Professionals to Business Consultants to Freelance Writers, they are really professional criminals, and comprise the largest threat in this secondary group. Their intelligence collection tactics mimic the APTs, but lack some of the governmental clout. They are interested in any information that can turn a profit for them. They are not too choosy about picking their clients.

Corporate Spies

These are your direct competitors. They are usually interested in specific pieces of intellectual

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

property or competitive information. Their time line is short-term to mid-term.

Activists

Activists are motivated by religious, environmental, political, or other deeply held beliefs. Usually they are after publicity for their cause, but when pressured, can slip into espionage and sabotage mode if it will help the cause.

Cyber Soldiers

Sometimes acting as Activist, APT or Corporate spies, Cyber Soldiers are also out to disrupt the businesses they attack. The usual MO is a computer based attack advanced by social engineering, dumpster diving, workforce integration and other on-site collection techniques such as electronic eavesdropping.

Internal Traitors

These are employees, service personnel, consultants and others with free access to the company. They often arrive early, stay late and prefer taking their vacation in cash instead of time. All espionage tactics are available to them. It is believed that 50% of information loss thefts have an insider component to them.

When employees understand who they are up against, and why, information-security requirements requested of them are taken more seriously.

Recommendations

The following is General Information Security Awareness & Advice to keep in mind while traveling in (or through) closed society countries. You may not be able to employ every bit of advice, in every situation, but everything that you *can do* will help.

Security is always a question of:

"How high do we build the wall?"

Answer…

*"Just high enough to keep **them** out."*

Awareness Checklist

- Assume your communications can be monitored by the government. This includes hotel, meeting room, business office bugging, and all forms of electronic communications.
- The use of communications encryption may be considered illegal. Certain exceptions may be available to financial industry transactions. Encryption of data on your personal devices is usually allowed, though if seized you may be asked for the decryption key or password.
- Anything left unattended may be subject to retrieval of information from it. This includes:

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

computers, smartphones phones, USB sticks, external hard drives, and written items.

- Spyware may be introduced onto computers, cell phones, and other devices which can hold computer instructions. This may be accomplished while the device is unattended, or an unintentional download from e-mails or web sites.
- Gifts may contain surveillance electronics (bugs, GPS tracking devices, etc.).
- Electronic surveillance devices may be planted in your transportation (rental car, corporate aircraft, etc.) Do not assume that any vehicle provides privacy.
- Personal surveillance and social engineering tactics may be used against you. Tactics may include: location tracking; "the friendly stranger" who wants to help or talk; and engineered compromising positions, for blackmail purposes.
- Be aware that foreign nationals employed by your company may also be employed by, or be under obligation to, the host government.

Advice Checklist

- Bring only "isolated" electronics, electronics to be used only on the trip, and which are never connected to other systems (like the company LAN, computer back-ups, or even computer-stored cell phone address books and back-ups).

  This advice applies to all information carrying and communications items, (smartphones, cameras, laptops, tablets, USB sticks, etc.)
- Bring as few of these electronics as possible. If everything can be accomplished with a smartphone, just bring that.
- If you need to enter a password for any Internet activity try to enter it using the cut and paste method, never type it using the device's keyboard. Tip: Keep passwords on an encrypted USB stick, and cut and paste from that. Change passwords upon returning home.
- Keep your electronics with you at all times.
- Keep the amount of information on these electronics as small as possible.
- Disable the Wi-Fi / Bluetooth options.
- Set up the filtering on your e-mail so that you don't receive anything except e-mail you know comes from safe and verifiable sources.
- Use VPN (Virtual Private Network) for your confidential communications.

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

- Take advantage of communications apps which offer encryption (Skype, Zoom, Signal, Viber, Telegram, FaceTime, iMesssage, etc.) for audio/video calls. While nothing is guaranteed to be 100% secure, these will help.
- Password protect your electronics. Encrypt the contents. A password alone will not prevent the theft of unencrypted information.
- While flying to closed society countries be aware your communications will be routed to them once you are within their 200 mile limit. This is a good time to stop communicating.
- Do not purchase electronics while in a closed society country.
- Keep electronic communications short, dull, boring and devoid of critical information.
- If you must use a wireless connection, close all unnecessary programs, and remove USB attachments.
- Be aware of visual spying - on your screen, and on your fingers while entering keystrokes. Your actions may be recorded optically at close distances, and equally well at far distances. Remember, your eyeglasses, windows, and other reflective surfaces behind you, can provide a readable reflection, too.
- Create alternate wording for sensitive or confidential information when communicating with the home office. Practice using the wording before leaving on the trip. You want to be low-key, but not appear sneaky.
- Upon returning home, have the IT department check all electronics for spyware, wipe-erase all storage media, and store the electronics for use on the next trip. Remember, keep them isolated. Do not connect them to anything.
- Upon returning home, conduct a Technical Surveillance Countermeasures (TSCM) inspection of corporate aircraft, and all items brought back: gifts, meeting materials, audio-visual equipment, luggage, etc.
- Use a data blocker while charging computers, tablets, smartphones, etc. to isolate your data from possible spyware.[1]

[1] https://counterespionage.com/malicious-usb-cable-detector-instructions/

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Detecting Electronic Surveillance

Conducting normal Technical Surveillance Countermeasures (TSCM) inspections in a closed society country can be problematic.

Possible issues faced include...

- Importation of TSCM instrumentation is not allowed, or requires a special permit.
- Multiple jurisdictions with individual and/or conflicting ordinances.
- Approvals or permits may not be honored by every government official equally.
- Corruption.
- Impulsive discretionary powers.
- Equipment may be confiscated without remuneration.
- TSCM activity could be classified (mistakenly or intentionally) as spying, thus subjecting the participants to imprisonment, and the company to fines, loss of business, etc.

Even so, deleting inspections from your security strategy is a mistake. Your organization's information is the target of more than just governments.

You have the ability to thwart (or at least make very difficult) attacks from all six of previously mentioned adversarial vectors.

Information Security / Electronic Surveillance inspections, specially modified to conform with local restrictions, can (and should) be conducted.

A high level of security can be achieved by engaging the services of a Technical Information Security who specializes in Technical Surveillance Countermeasures (TSCM) inspections. Have them evaluate your business locations. Even if only using test instrumentation—commonly used by an IT technician for routine testing and maintenance—the results can be very effective.

How it's done...

Ideally, plan on conducting inspections using a low-cost kit consisting of common test equipment and hand tools. In some cases, these items may be purchased locally and left at the inspection location for use each visit.

Plan on leaving untouched any government surveillance devices found. Just knowing the surveillance devices are there is beneficial. It forces you to develop a communications work-around strategy, and can help prevent the inadvertent loss of your most confidential communications.

After the initial inspection, which should include an information-security survey, implement your consultant's recommendations about: perimeter security, information handling, sensitive

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

wastepaper disposal, and closing any other loopholes which puts information at risk of being stolen.

Your technical specialist can also place unobtrusive security seals on inspected communications devices (and elsewhere) to detect intrusions between inspections.

Conduct re-inspections on a regular basis to detect: new issues, deteriorating security hardware, and previously instituted security policies and procedures not being followed.

Mitigating Surveillance and Information Loss

A special information protection protocol is required when conducting business in closed countries. This protocol, will be driven by any restrictions the country imposes. In turn, this affects how all other opponents are handled.

Closed-Country Information Security Protocol

The intelligence collection process usually includes some form of electronic information gathering. Bugs, wiretaps, keystroke loggers, hidden voice recorders are the easiest signs of an attack to spot. Historically, this is why the protection process begins with a TSCM inspection of the sensitive areas.

Traditional TSCM inspections usually require instrumentation which may not be legal to import or use in a closed-country. This modifies the inspection process. Knowledgeable information security technicians can get around this limitation and will still be very effective.

Instrumentation restrictions also increase the importance of preventative security measures, as well as employee information security policies and procedures.

A closed country customized inspection…

- Physical inspection for electronic surveillance devices.
- Physical inspection for modifications within electronic devices.
- Physical inspection for modification of security alarms, door locks, etc. which would allow easy unauthorized entry into the protected space.
- Physical inspection of the protected space to identify physical security flaws which would affect information security.
- Observation of information handling procedures to identify security loopholes.
- Sealing and inventorying of electronics - using serial numbered security tape to detect future tampering (computers, cell phones, etc.)
- Establishing a written company policy on information security - specifically tailored to the hostile environment.

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

- In certain cases, providing information security training to the local office manager so that they can provide employee training on an on-going basis.
- Conducting periodic on-site reviews to identify new vulnerabilities, ensure information security standards are being met, and to identify deterioration of existing security hardware and standards.

Extra Credit — The MOSCOW RULES

This version of the Moscow Rules (developed by the CIA during the Cold War) comes from my late friend Glenn Whidden (retired CIA). It remains a valid template for behavior in closed society countries today.

FOR COUNTER ESPIONAGE INVESTIGATIONS

1. Assume that all (Local Nationals) LN's are hostile.
2. Assume that an approach by a non-LN is hostile until proven otherwise.
3. Assume that there is always hostile physical surveillance unless counter-surveillance proves otherwise.
4. Assume that all telephone conversations are monitored by LN's.
5. Assume that all enclosed areas are bugged unless they are 'secure' rooms.
6. Assume that incoming and outgoing mail will be subject to hostile examination.
7. Assume that anything that is left unattended will be subject to examination by LN's.
8. Assume that locks left unguarded or unprotected will be manipulated or bypassed and the material they protect will be compromised.
9. Assume that simple traps will not deceive LN's.
10. Assume that any guard can be recruited by LN's or is himself an LN agent.
11. Assume that a pair of guards can be recruited by LN's or are themselves agents of LN's.

FOR COUNTERMEASURES INSPECTIONS

1. Assume that the eavesdropper is listening in the sensitive areas.
2. Assume that an eavesdropper has an agent near the sensitive area.
3. Assume that the eavesdropper is watching the entrances of the facility.
4. Assume that the eavesdropper can maintain a low vulnerability status when he is not listening.
5. Assume that the eavesdropper is monitoring the NLJD band of frequencies.
6. Assume that the eavesdropper is watching for sweep receiver radiation.

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Satellite Phones

Securing voice communications is a common question raised by executives, especially in areas where cell phone coverage is limited or non-existent. Using satellite phones is a common solution, but is it permissible?

In India, for example, it is illegal without the proper permissions. In China, it's hard to tell if their permissions laws are enforced, based on my research alone. There is conflicting information on the Internet.

RECOMMENDATION

Contact your law firm to have them research the latest laws for the country you are visiting, or passing through, **before** you bring a satellite phone.

Information Security Tips for Travelers to Closed Society Countries

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Suggested Reading

- Staying Safe Abroad: Traveling, Working & Living in a Post-9/11 World [2]
  Edward L Lee II
- Preparing a Business Laptop for Overseas Travel [3]
  Patrick Lambert
- Digital Privacy at the U.S. Border: Protecting the Data On Your Devices [4]

This paper has good tips for protecting your electronic information while traveling. Keep in mind, although the paper focuses on the United States border crossings, you will also be dealing with the country you are visiting. And, some of them are a whole lot more aggressive.

- Digital security tips and resources for journalists. [5]

About the Author

Kevin D. Murray is a Technical Information Security Consultant who specializes in TSCM for business, government and at-risk individuals.

He is also the author of, "Is My Cell Phone Bugged? Everything you need to know to keep your mobile conversations private," [6] and publishes Kevin's Security Scrapbook - Spy News from New York. [7]

His Android app SpyWarn 2.0™ allows average individuals to conduct their own forensic cell phone exam to determine if it is infected with spyware.[8]

Mr. Murray is a Certified Protection Professional (CPP); Certified Information Security Manager (CISM); and is a member of ASIS and the International Association of Professional Security Consultants (IAPSC).

Murray Associates provides advanced eavesdropping detection (technical surveillance countermeasures, TSCM) and counterespionage consulting services to business, government, and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.
https://counterespionage.com

---

[2] https://amzn.to/2MFdHRH

[3] https://tinyurl.com/yb9p2kxj

[4] http://tinyurl.com/hvtzzl9

[5] https://ijnet.org/en/story/digital-security-tips-and-resources-journalists

[6] https://amzn.to/2MDSnfr

[7] https://spybusters.blogspot.com/

[8] https://play.google.com/store/apps/details?id=com.spybusters.spywarn.app