Cybersecurity and Travel to China or to the Russian Federation

Recent press coverage in the *N.Y. Times* (see "Traveling Light in a Time of Digital Thievery" in the reference list at the end of this document) has increased popular concern about the cyber security of travelers to China or to the Russian Federation. This document is meant to provide a basic briefing for higher education users on this topic of concern.

• U.S. travelers are believed to be priority targets for cyber attack and monitoring/surveillance, particularly if they are known to be engaged in classified or proprietary research in a STEM (science, technology, engineering and mathematics) discipline. Institutional leaders, those who are politically or religiously active, fluent speakers of the local language and individual tourists may also be actively targeted, however all American should assume that they are potentially at risk if traveling to China or Russia.

• Laptops, tablets, e-book readers, smart phones and even regular cell phones taken overseas may be successfully attacked and compromised via malware or automated attack tools. Commercially available security software, even when completely up to date, may not prevent such compromise.

• Electronic devices may also be at risk of physical tampering or theft, particularly if those devices are left unattended (including devices left locked in a hotel room or even left locked in a hotel safe while dining, shopping or touring). On the other hand, carrying one's laptop or other electronic devices continually may increase their risk of being accidentally lost or forgotten, or stolen by a thief/pick pocket. On balance, however, we recommend you keep your devices with you at all times.

• Devices taken across international borders may be subject to involuntary official governmental review and even complete duplication (e.g., in some countries, Customs officers may temporarily seize your device, and potentially keep a copy of one's entire system on entry or exit).

• Use of encryption may be forbidden in some countries. For example, while many US universities routinely require whole disk encryption to protect personally identifiable information (PII) on laptops, some countries (such as China and the Russian Federation) do not allow importation/exportation of encrypted devices. While some whole disk encryption products, such as TrueCrypt, allow you to attempt to conceal encrypted disk partitions, attempts at hiding encrypted disk partitions may nonetheless be detected, and lying in response to border official questioning about the existence of encrypted disk partitions may be a potentially serious criminal offense.

• Access to some web sites, including access to some mainstream popular western social media web sites, may be technically blocked. Secure ("https") web sites and use of institutional virtual private networks ("VPNs") may also be blocked by some countries, because it is more difficult for national authorities to monitor that encrypted traffic. Attempts to circumvent national censorship (e.g., with Tor, Ultrasurf or similar products) may be blocked and/or punished if noticed.

• Personal privacy may also not be respected abroad. Assume that even nominally private spaces (such as hotel rooms and rental cars), may in fact be subject to video, audio, or other monitoring. Such surveillance may be able to track where you are, and see whatever you may be doing, what's on your laptop, and what you type on your keyboard. Conversations, whether on your phone or face-to-face with a colleague, may also be monitored, including conversations held in open areas (parabolic microphones can readily capture conversations held in open areas). Local colleagues may also be required to report on any conversations held with foreigners.

Obviously these considerations may make traveling to China or Russia quite challenging.

Recommendations:

1. If possible, avoid traveling to China or the Russian Federation.

2. If you must travel to China or the Russian Federation, leave all electronic devices in the U.S. and inform colleagues that you will be "off the air" for the duration of your travel. Minimize the length of your stay in those countries.

If you are travelling without your own laptop, you may be tempted to use a computer in a cyber cafe of hotel business center, however those systems have a very high probability of being infected with malware (which may capture anything you type, including your username, password, credit card information, etc.), or of being routinely and actively monitored by national authorities.

Therefore, never use shared computers in cyber cafes or hotel business centers, or systems belonging to other travelers, colleagues, or friends.

3. If you are absolutely unable to be offline for the duration of your travel, do *not* take your normal day-to-day devices with you. Use a new temporary device, such as an inexpensive new laptop or a throw-away prepaid cell phone purchased just for that trip, instead.

Be sure that any such new system is fully patched, and has all institutionally recommended security software installed, but otherwise minimize what it contains, and while abroad, minimize your use of that system.

Ensure it requires a long/complex password for access, and keep it completely off (not just sleeping or hibernating) when you're not actively using it, and keep it in your physical possession at all times.

Assume anything you do on that system, particularly over the Internet, will be intercepted (in some cases, encrypted network traffic may be decrypted).

Upon return to the U.S., immediately discontinue all use of that temporary system, and have it reviewed for indications that it may have been compromised abroad. The system should then be sanitized and disposed of.

Change any/all passwords you may have used abroad.

Some Additional Things to Consider If Travelling to China or Russia:

Before You Travel:

— Tape-over any integrated laptop cameras.
— Have a computer technician physically disconnect any integrated laptop mikes.
— Install a privacy screen (such as those from 3M) on your laptop to discourage so-called "shoulder surfing."
— Disable all file sharing.
— Disable all unnecessary network protocols (such as WiFi, Bluetooth or infrared).
— In case your system is lost, stolen, seized or destroyed, take a full backup.
— Leave all unneeded door keys, smart cards or USB format PKI hard tokens, one time password crypto fobs, and similar access control devices in the United States.
— Be sure to clean out your purse or wallet, particularly if you normally carry notes about various accounts or passwords. Any RFID cards (including U.S. Government Nexus "trusted traveler" cards) should be carried inside an RF-shielded cover.
— If you need to send or receive email while traveling, create a temporary "throw away" account on Gmail or a similar service before you travel.

While Abroad:

— Do not use your regular email account. Do not send any sensitive messages via email.
— Avoid making or receiving voice calls, using voice mail, using IM or SMS, or sending or receiving faxes.
— Even powered-off cell phones may be able to be turned into surreptitious monitoring and geolocation devices. If you don't want to be geographically tracked, or you're attempting to have a confidential conversation, cell phone batteries must be removed.
— Any/all CDs, DVDs, thumb drives, attachments, links and "QR" cell phone bar codes must be considered to be potentially hostile and malware infected.
— Do not use USB-based public battery charging stations; the USB interface to your device they may allow the charging station to do more than just provide power.
— Do not purchase new hardware while traveling.
— Do not purchase or download any new software while traveling.
— Do not have any of your electronic devices "repaired" or "worked-on" while abroad.
— Any discarded items (such as notes, documents, diskettes/CDs/DVDs) may be retrieved, analyzed and potentially exploited.
— Tor (and other so-called censorship circumvention tools) may be blocked, or may provide imperfect anonymity; use of such tools may attract official attention, and may result in you being investigated and punished or expelled.
— Guides, drivers, and interpreters may report on your activities.
— Beware of attempts to put you in embarrassing or compromising positions. You may be getting targeted for eventual extortion.
— While abroad, register with the nearest U.S. Embassy or Consulate and please report any suspicious incidents you experience to them.
— If arrested, taken into custody, or interrogated, do not make any statements or sign any documents, particularly if they are written in a language you don't know. Ask to have the U.S. Embassy or Consulate notified of your detention at once.

References

— "Beware of Juice Jacking," http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

— "Browsing the Broken Web: A Software Developer Behind the Great Firewall of China," http://www.troyhunt.com/2012/03/browsing-broken-web-software-developer.html

— "China-Based Hacking of 760 Companies Shows Cyber Cold War," http://www.businessweek.com/news/2011-12-22/china-based-hacking-of-760-companies-shows-cyber-cold-war.html

— "Foreign Spies Stealing US Economic Secrets in Cyberspace," Office of the National Counterintelligence Executive, Oct 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

— "Lawmakers say Capitol computers hacked by Chinese," http://www.usatoday.com/news/washington/2008-06-11-2277390014_x.htm

— "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation," March 7th, 2012, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf

— "Pentagon Sees N. Korea Cyber Threat, 2012 Provocations," March 28th, 2012, http://www.reuters.com/article/2012/03/28/usa-korea-north-idUSL2E8ESVOR20120328

— "Richard Clarke: China Has Hacked Every Major US Company," http://www.zdnet.com/blog/security/richard-clarke-china-has-hacked-every-major-us-company/11125

— "Shadows In the Cloud: Investigating Cyber Espionage 2.0," April 6th, 2010, Information Warfare Monitor and Shadowserver Foundation, http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0

— "The Dark Visitor: Inside the World of Chinese Hackers," http://www.thedarkvisitor.com/

— "The Government's Four Cyber Silences: Testimony of Jason Healey, Director, Cyber Statecraft Initiative, Atlantic Council to the US-China Economic and Security Review Commission on 'Developments in China's Cyber and Nuclear Capabilities,'" March 26, 2012, http://www.uscc.gov/hearings/2012hearings/written_testimonies/12_3_26/healey.pdf [note in particular the discussion of "national responsibility" and "The Spectrum of State Responsibility" in Table 1 on PDF page 9]

— "The OpenNet Initiative," http://opennet.net/ [the OpenNet Initiative tracks government deep packet inspection and censorship efforts]

— "Tips from the National Counterintelligence Executive: Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices," http://www.ncix.gov/publications/reports/traveltips.pdf

— "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor, March 29, 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

— "Traveling Light in a Time of Digital Thievery," February 10th, 2012, http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html

— "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," James R. Clapper, Director of National Intelligence, January 31, 2012, http://www.dni.gov/testimonies/20120131_testimony_ata.pdf

— "US Expels Venezuelan Diplomat Over Cyberespionage Allegations," January 10th, 2012, http://intelnews.org/2012/01/10/01-905/

— "U.S. Probes Whether Laptop Copied On China Trip," http://www.usatoday.com/news/nation/2008-05-29-US-china-laptop-copied_N.htm