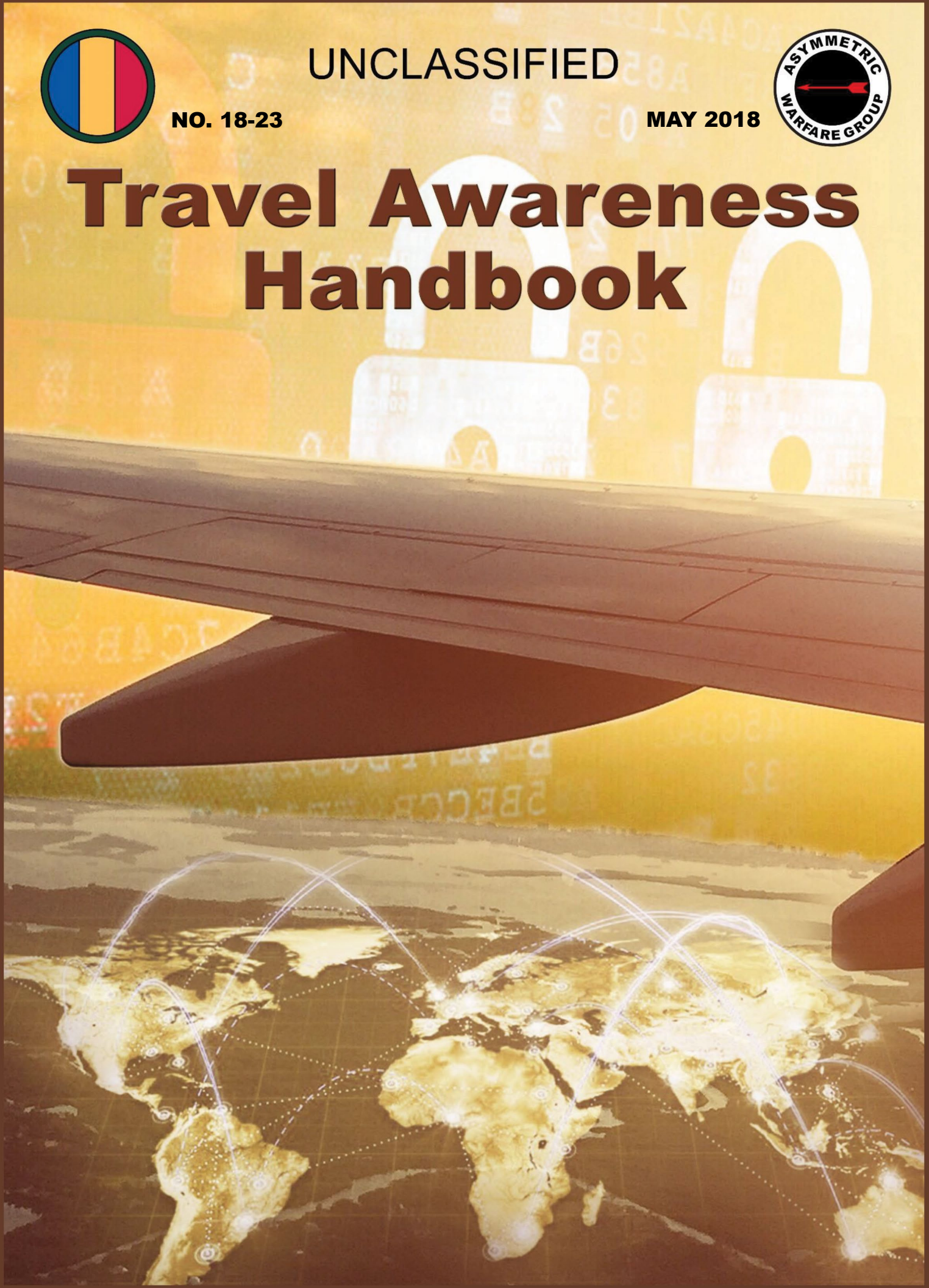
UNCLASSIFIED

NO. 18-23

MAY 2018

Travel Awareness Handbook



TRAVEL AWARENESS HANDBOOK

2018

U.S. Asymmetric Warfare Group
2270 Rock Avenue., Suite 5355
Fort Meade, MD 20755

CONTENTS

FOREWORD

As globalization rapidly condenses physical and digital spaces, the virtual space to reach out across the world has become more dense and complex. Methods and means of cheaper and more efficient travel draw the world closer. The interconnectedness of the United States Army to the world has made it necessary for habitual visits to bolster relationships with partner countries. These global partnerships require the United States Army to move its leaders and Soldiers to unfamiliar areas on a routine basis. Official travel has become a part of the decision calculus for commanders sending Soldiers on missions. Because of travel's inherent operational risk, travelers should observe the methods, means, and best practices to prevent or mitigate this risk, before, during, or after travel to ensure mission success.

Many of the United States Army's relationships leverage burgeoning and legacy technology for conducting meetings or conferences in a virtual domain. The virtual realm compensates for the inability to be physically present. Even as the United States Army uses technology to continue engagement when they cannot do so in person, face-to-face engagement remains optimal. Additionally, while strategies and methodologies for virtual training continue to develop, real world exercises will remain and require moving United States Army personnel around the world.

The means and capability exist for the United States Army to utilize direct travel to foreign countries on a regular basis. How do we prepare for the associated risks? Efficiency, commonsense and deliberate forethought. This handbook will review pre-travel planning considerations for staff planners to supplement their mission analysis. It will also provide considerations for operational security (OPSEC), cyber awareness, hotel selection, and hotel room considerations, as well as an example trip emergency plan to utilize in conjunction with Personnel Recovery Plans.

This handbook seeks to present the current best practices and codify topics to consider from pre- travel to post travel operations. This handbook will describe available and resident capabilities within a traveler's operational environment and applications of learned best practices using vignettes of real world situations. This handbook should serve as a supplement, not a replacement to mandatory 350-1 AT Level 1. Finally, this handbook will present recommendations to U.S. Army Battalion and Brigade Combat Team leaders to counter travel threats, vulnerabilities, and mitigate risks associated with worldwide movement of their Soldiers.

The world presents ever-evolving risks when placing Soldiers in unfamiliar environments. The United States Army must be active in adapting to this need/challenge and become comfortable with worldwide movement by capturing and learning from best practices. Applying critical thought and analysis prior to any mission is a common foundation for preparation. The idea of reinforcing a possible vulnerability is noted in *Epitoma Rei Militaris* (*Epitome of Military Science*) by Publius Flavius Vegetius Renatus, in which he states, *"The part which the enemy is expected to approach one should be particularly careful to reinforce."*

PURPOSE

Attacks on public locations, both in the U.S. and abroad, is a current and emerging threat. Locations such as hotels and restaurants offer a target-rich environment. They require little to no planning and are easy to execute by anyone with any type of weapon from a knife to a machine gun to explosives. When analyzing the events, there is little to no difference between these attacks abroad and an active shooter event at home.

In November 2008, ten members of Lashkar-e-Taiba, an Islamic militant organization based in Pakistan, carried out twelve coordinated shooting and bombing attacks over four days that killed or wounded at least 308 people across the city of Mumbai, India. The attacks were a chilling example of how a small squad of trained and prepared active shooters can be so effective. Recently, this style of attack also happened in Paris and Brussels.

In 2014, three U.S. Soldiers deployed to the West African country of Burkina Faso to conduct a mil-to-mil training event. They received a warning that they should not go to the training the following day. The next day the country erupted into a coup d`etat with thousands of protestors and rioters flooding the streets. The Soldiers, surrounded in the hotel by the protestors and rioters, had no plan for escape or defense. Only after being overrun in their hotel rooms did they consolidate and attempt to escape to a safe area. Beaten and robbed in the hotel, the team safely escaped and evaded across the city. A U.S. Embassy safe house was only two blocks away. There were also two senior U.S. officers at the same hotel. They made the call for help too late, and when they did call for help, the response was for them to “hold in place.”

In Nov 2015, a small team of active shooters stormed a U.S. Embassy-approved hotel in Mali where many U.S. Government (USG), including four Department of Defense (DoD) personnel, were lodged. For nine hours, the terrorists consolidated and killed anyone they considered non-Muslim. Several DoD and USG personnel hid in rooms and attempted to communicate for help. One USG member died during the attack.

In January 2015, a small active shooter team conducted an attack in Burkina Faso on a crowded street, restaurant, and hotel (U.S. Embassy-approved) frequented by westerners, and killed a U.S. citizen dining at the restaurant.

While all DoD personnel survived these attacks, they are great examples of why personnel need a security plan before and during any Temporary Duty (TDY). Personnel naturally tend to feel safe and consider the threat diminished when they are travelling in civilian clothes and living in hotels because it feels like a safe environment. However, recent history shows us that airports, hotels, restaurants, etc. offer many opportunities for both crime and terrorism.

The events described above offer insight to several tactics, techniques, and procedures for those on TDY. In relation to the enemy, time was the greatest factor. Decisions made in the initial seconds of an event are critical. These active shooter teams know they only have a limited amount of time before a police or military response. They all entered through main entrances, initially flowed to easy targets, killing anyone who was immediately available, and did not have the manpower to seal off secondary and tertiary exits.

On the friendly side, almost all personnel immediately ran back to or stayed in their rooms. These actions show a lack of training and preparation, as they had no security, escape, or communication plans.

The Department of State is responsible for the security of U.S. citizens abroad. In most situations, they are reliant on local forces to supplement their own security forces and their response time may not be very swift.

While attacks like those referenced above are easy media successes for terrorist organizations, crime remains the most common threat to U.S. personnel abroad. Accordingly, this handbook focuses on the vulnerability of Soldiers while transiting, living, and working around the globe to both terrorist attacks and common crime. Planning and preparing personal security prior to and during travel can help mitigate one's vulnerability against potential threats.

CHAPTER 1: PRE-TRAVEL PLANNING

Units plan for every mission they conduct. Planning for upcoming travel should be no different. There is no cookie cutter or prefabbed checklist to use. However, numerous websites, documents, and seasoned travelers can assist in thinking about what one needs and/or should plan for prior to execution. In this chapter, you will find suggestions of things to plan for, but this is not an all-encompassing list. The destination country may require some, some will be good techniques to consider, and some you may not need to use.

Country/Theater Clearance

Reference Department of Defense (DoD) Foreign Clearance Guide (FCG) for specific country requirements.

- Web address: https://www.fcg.pentagon.mil/
- Example requirements/instructions/information:
    - Travel restrictions
    - Mandatory pre-training and travel documentation
    - Medical requirements
    - Military uniform requirements
    - Customs/quarantine/lead times on specific cargo items
    - Host nation detention policy
    - LGBTQ considerations

Identify any additional documentation/memoranda or security clearance requirements for specific locations where you plan to conduct business (i.e., embassy access, military installations, Department of State restricted areas of travel)

- Ensure you have a valid passport.
- Visa requirements:
    - Determine whether a visa is required for travel into country.
    - Passports must be good for six months beyond the travel dates.
    - Some countries authorize military personnel to travel on military identification (ID) and 1610 and/or region specific orders such as “NATO Travel Orders”.
    - Confirm a country registration requirement if no visa is required.
    - Confirm if an exit payment is required.
    - Submit visa application through your S1 representative.
    - Consider visa lead times when planning departure dates.
- Country Clearance Request: (Reference Ch.1.A. Foreign Clearance Guide)
    - Submit Aircraft and Personnel Automated Clearance System (APACS)
        - Web address: https://apacs.milcloud.mil/apacs/
        - Have all passports and visas available for information requirements.
        - Know your in-country point of contact/location of business/lodging info.
        - Have entire team’s training/contact/itinerary information accessible.

        - Ensure all travelers are aware of any restricted areas for U.S. personnel and Department of State travel warnings, if applicable.
        - Include all emergency contact numbers in individual Trip Emergency Plan (reference Chapter 3 and Appendix A).

Enroll in the Smart Traveler Enrollment Program (STEP) for continuous and near real-time updates on safety conditions in country of travel.

- Web address: https://step.state.gov/step/
- If traveling to more than one country, submit all travel individually in the STEP system in order for the traveler to get notifications about each location. Entering multiple locations in one submission has led to travelers not receiving alerts for some countries.

U.S. Embassy Coordination

- Determine lodging options and/or requirements.
    - Research U.S. Embassy and/or Regional Security Officer (RSO) approved hotels.
- Determine country/U.S. Embassy rules for in-country transportation.
    - Do you require U.S. Embassy driver/local driver/rental car/public transportation?
        - Coordinate/confirm with U.S. Embassy for local drivers and/or vehicle. When using U.S. Embassy resources it may require the user to use the International Cooperative Administrative Support Services (ICASS) to pay for required support. Your unit S-4 should be able to provide assistance if needed.
        - Check with the U.S. Embassy for approved rental car agents.
- Travelers should only contact U.S. Embassy personnel with critical Request for Information (RFI) once research and internal resources are exhausted.
- Key personnel for RFIs: Global Combatant Command (GCC) desk officer, Army Service Component Command (ASCC) desk officer, RSO, Senior Defense Official (SDO), Defense Attaché (DATT).
- Review and update your Isolated Personnel Report (ISOPREP).
- Secret Internet Protocol (IP) Router Network (SIPRNet) web address https://prmsglobal.prms.af.smil.mil/prmsconv/Login/Logon

Travel Coordination/Considerations:

Defense Travel System (DTS):

- Government Credit Card (GOVCC) is required.
- Ensure GOVCC is active and turned on and you have an adequate credit limit.
- Update GOVCC account information in Defense Travel System (DTS).
- Flights:
    - Synchronize flight itinerary with other personnel in your party.
    - Conduct research on surrounding areas of possible layover airports.
    - Synchronize arrival time with mode of travel to hotel. (U.S. Embassy personnel, taxi, hotel shuttle, etc.)

- Hotel:
    - Research hotel security/threat history.
    - Conduct research on surrounding areas.
- Rental car (if applicable):
    - Confirm secure parking at hotel and research parking in business area.
    - Bring a navigation system and update the maps to ensure map data covers the area in which you are travelling.
    - Do not rely solely on cellphone navigation applications.
    - Learn the local driving laws and customs.
    - Consider obtaining an international driver's permit from the American Automobile Association (AAA).
        - Web address: http://www.aaa.com/vacation/idpf.html
- Meals, rations, local economy:
    - Determine if personnel are eating on local economy or provided rations. Coordinate with the ASCC if rations are required.
    - Visit state.gov for information on health considerations for local food.
    - Determine if local water is potable/safe to drink, and if not be cognizant of drinks containing ice.

Internal Mission Coordination

Identify personnel, training and equipment gaps and deficiencies prior to mission execution. Examples: Interpersonal skills, foreign weapons familiarization, partner nation doctrine, cultural training, expeditionary operations, etc.

Conduct unit level Soldier Readiness Processing (SRP)/Unit coordination

- S1/Personnel:
    - DD93/Service members Group Life Insurance (SGLI)
    - Orders/Memoranda required for country clearance.
    - Passport/visa (lead times vary for both items)
    - Additional pay-allowances authorized (hazard, imminent danger, etc.)
- Medical:
    - Country specific vaccinations and documentation up to date (International Certificate of Vaccination, a.k.a. "yellow card"). DoD CAC holders can find current medical threat information and vaccination requirements at https://www.travax.com.
    - Pack pills for minor medical issues (allergies, colds, cuts, aches, etc.)
    - Research local medical facilities and first aid items available in country and those the traveler should bring with them.
- S2/intel section:
    - Courier orders
    - Foreign Disclosure Officer (FDO) approved products (varying lead times)

    - Operational Security (OPSEC) briefing
    - S2 or Special Security Office (SSO) requirements
        - Submit pre-travel notification for foreign travel.
        - Joint Personnel Adjudication System (JPAS) requirements for security clearance transfer.
- S4/Logistics:
    - Coordinate shipping requirements (equipment/transit means/lead times)
    - Military driver's license
- S6/Communications
    - Activate and register Personnel Locator Beacon (PLB). Ensure the supported units and commands have the beacon information.
    - Determine availability of Non-Classified Internet Protocol Router Network (NIPRNet)/SIPR in country.
    - Determine cell and iridium coverage in country (times and locations). Ensure you know the password and dial out codes for all cell phones and iridiums.
    - Availability of Wi-Fi Hotspot/Broadband Global Area Network (BGAN). Determine in-country rules/regulations for use.
    - Unit communication card.
    - Consider type of receptacle/source of power at deployed location.
    - Battery requirements/restrictions
    - Determine pre/post-mission communication requirements.
    - Download cellphone applications that will be useful for traveling and working in the area (i.e. Google Translator, WhatsApp, Signal, etc.).
- Public Affairs Office (PAO) guidance for mission.
- Legal:
    - Last Will and Testament
    - Power of Attorney
    - Status of Forces Agreement
    - Rules of Engagement
    - Type of Authorities

Develop Mission Plans

Develop a Trip Emergency Plan. (Reference Chapter 3 and Appendix A)

Develop a communications plan:

- When using a Primary, Alternate, Contingency, Emergency (PACE) plan, ensure that you use separate communication systems for each category. Keep in mind that if you use two separate cell phones in categories, that loss of cell coverage could affect both categories.
- Setup communications devices with all pertinent PACE contacts.
- Rehearse each method of communication 24 hours prior to travel.

- Use as many different systems as possible in order to maintain communications with higher and friendly forces at all times.
- Continually refine PACE plan based on service coverage (landline, email, cellular, iridium, line of sight radios, PLB, etc.).

Identify reporting requirements:

- Confirm who needs the information/requires situational awareness: Parent unit/ASCC/GCC, Personnel Recovery (PR) cell, etc.
- Determine methods of reporting for each requirement. (i.e. email, text, voice, etc.).
- Establish distribution lists for efficiency and consistency.
- Travel updates/arrival and departure notification.
- Daily Sign of Life (DSOL) requirement.
    - What is the standard operating procedure (SOP) for DSOL?
    - How often are you required to send a DSOL?
    - What information does the SOP require be sent (i.e. status of travelers/personnel, weapons, equipment)?
    - What is the response SOP?
- Situation Report requirements

Develop Isolated Person/PR plan in accordance with Joint Publication (JP) 3-50 Personnel Recovery and Army Field Manual (FM) 3-50 Army Personnel Recovery.

Develop threat mitigation plan:

- Consider the team's pattern of life/military signature/social media/body language/group size/tourist locations/clothing.
- Frame the regional threats by "Risk to Mission" and "Risk to Force".

Develop team/individual medical plan:

- MEDEVAC availability, location, contact information.
- Primary and alternate medical facilities (level of treatment provided).

Initial entry plan:

- Account for all team members and equipment.
- Currency exchange in a trusted location (U.S. Embassy/stateside/airport/hotel).
- Acquire local maps.
- Coordinate in-brief with Defense Attaché/Regional Security Officer or a delegate from their office.
- Link up with host nation Point of Contact (POC) or sponsor.
- Acquire transportation (e.g. rental car, local driver etc.).
- Move to hotel and acquire lodging.
- Inconspicuously conduct area familiarization/rehearse emergency plan.
- Validate your PACE and send initial DSOL upon initial entry.
- Re-assess environment.

Post Travel plan:

- Develop a plan to document discussion points for the AAR.
- Have a plan to take and save photographs.
- Identify key leader engagements with host nation partners.
- Coordinate office calls/out-briefs with U.S. Embassy as required.
- Equipment accountability plan/identify tasks and responsibilities.

Know your operational environment

Use internet search to determine appropriate conservative clothing for travel to a specific region.

Use the U.S. Embassy website for your country of travel for information and threat awareness. (https://usembassy.gov)

Conduct individual country study and threat awareness research through Department of State (DoS), DoS Bureau of Diplomatic Security, and Central Intelligence Agency (CIA) factbook.

- Web addresses: https://www.state.gov; https://www.cia.gov/library/publications/resources/the-world-factbook/; https://www.osac.gov.
    - Study S2-provided country threat briefs.
    - Counter Intelligence
    - Transnational criminal and terror organizations
    - Review region specific medical threats/treatments.
    - Study key phrases and have a small language book and/or app on phone.
    - Print maps for locations of travel (Google maps, tourist maps, etc.).

Packing and Airport considerations

Be familiar with local airport checkpoint rules and requirements.

Be prepared to explain all items of equipment carried/checked.

Have Transportation Security Administration (TSA) authorized locks for all checked bags.

Do not be flashy. Keep a low profile and blend in to your environment. Be the "grey man" – do not stand out. See Chapter 4: Actions while Traveling.

Helpful Hints

Make color copies of important documents and email them to yourself. Examples: passport/visa, international driver's license, credit cards, orders/DD Form 1610.

- Have business cards made with appropriate contact information for Country team, ASCC, and GCC personnel.
- Inform personal financial institutions of travel. This will help in the event that you need to use your personal debit/credit card while deployed, so that the financial institution will authorize the charge where you are located. Notification will also help if fraudulent/unauthorized access happens to your accounts.

- Consider emergency funds/emergency credit card.
- Conduct currency exchange in airport or hotel to ensure you get the current exchange rate.

CHAPTER 2: OPSEC AND CYBER AWARENESS

Every day we send emails, browse the internet, download an app on your phone, use social media, etc. While this may seem to be small parts of daily personal life or even mission execution, it is through these routine uses of cyberspace that are vulnerable and our adversaries exploit. All of these actions occur in what is known as the Cyber Electromagnetic domain.

Cyberspace and the Electromagnetic Spectrum (EMS) also provide adversaries and enemies an effective, inexpensive, and anonymous means for recruitment, information activities, training, and command and control. The security of your personal and military devices such as smart phones, tablets, and computers, as well as the security of the information being transferred – personal and mission related – is your responsibility.

It is crucial that all Soldiers fully grasp the relationship between cyberspace and the EMS and maintain the necessary protection measures when using government and personal devices no matter where they are located.

For a more in-depth look at cyber security details, consult Appendix D, Cyber security reference information.

OPSEC

Conversations: You should consider that any conversation in a public area is subject to eavesdropping. Whether talking to a team member next to you or over the phone, the people around you may not be merely standing around but rather listening to you. Do not discuss operational information outside of a secure area.

Documents: Limit the amount of hard copies of documents you carry with you. If possible, email files to someone at your destination so that the files will be waiting for you. Consider removing unit logos or other conspicuous headings from documents that you hand carry, so that they do not draw attention from others if you intend to review them during your travel.

Radio Frequency Identification (RFID): Many credit cards, passports, hotel keys, and other cards have RFID chips embedded in them. While they make transactions easy to complete with just a Personal Identification Number (PIN), they also create an exploitable vulnerability. The use of an RFID blocking sleeve for each card or an RFID blocking wallet is highly recommended, even for daily use in the U.S.

Cyber Awareness and best practices

Cell Phones:

- Ensure your applications are up to date. Most updates include security patches for known vulnerabilities.
- Avoid turning your phone on immediately upon landing. When your phone connects to local towers, your location is traceable to anyone that may be searching for US personnel. A technique is to wait until you have completely exited the airport.
- When charging your phone in a public location, use a power-only port. If a USB charging station is the only type available, consider the use of a USB blocker (eg. PortaPow). This will restrict the

ability of someone to access your data. The same applies for rental cars. Either use the cigarette lighter with an adapter or use a USB blocker.

Computers:

- Ensure your antivirus software is up to date. The Army Home Use program makes it easy for Soldiers to secure their home computers by giving them free access to both Symantec and McAfee anti-virus and firewalls. Web Address: https://patches.csd.disa.mil/Metadata.aspx?id=79775
- Limit what you store on your laptop while traveling and remove files not needed during the mission. Make a back-up CD of important files.
- Use an encrypted folder if possible.
- Do not leave a laptop in a hotel or conference room unless necessary. Use a cable lock to secure the laptop and log off and/or turn it off while left unattended.
- Social Media
    - Turn off geo-tagging.
    - Adjust your privacy setting to the most restrictive.
    - Avoid posting any places or activities that identify the location of you and your team until you return home.

CHAPTER 3: TRIP EMERGENCY PLANNING AND PERSONNEL RECOVERY (PR) CONSIDERATIONS

Personnel Recovery (PR) for the Soldier

Individual PR Principles:

- Understand your Isolated Soldier Guidance (ISG) and special instructions.
    - "You are isolated if _____, move to _____"etc.
    - Challenge/password, letter/number of the day, etc.
- Know where you are at all times and the distance and direction to the nearest Friendly Force.
    - Look for memorable landmarks as you travel (checkpoints, etc.)
    - Know basic navigation – the sunrises in the east, constellations, etc.
    - Maintain and account for your recovery equipment.
        - Radios charged/Personnel Locator Beacon (PLB)-tested
        - Grid Reference Graphic (GRG)/maps, GPS/compass
    - Know how to communicate/signal both day and night.
        - Know Communications (COMs) plan, infrared (IR) devices

Plan: Evasion Plan of Action (EPA)

- Small-unit leaders must ensure that they plan their PR actions based off the higher command's PR plan or Concepts of the Operation (CONOPs), ISG, established SOP, and theater Special Instructions (SPINS) data.
- Develop the EPA to address the five PR tasks (report, locate, support, recover, and reintegrate); must be written based on the assets available and potential recovery forces.
- EPA informs the recovery force about the isolated persons (IP) intentions.
- In the absence of any other specific information or intelligence, PR cells and recovery forces will use this data to help plan a recovery. Ensure the appropriate commands have your EPA information.
- The minimum information requirement to produce an individual EPA is in FM 3-50.1.

Prepare: Equipment

- Survival, evasion, and recovery equipment requirements identified by higher commands and through training.
- Items to consider include, but are not limited to compass, GPS, map/GRG, evasion chart, imagery, radio or phone, pointee-talkee, electronic –PLB, radio, visual – laser, strobe, mirror beacon, water purification, and blood chit.

CHAPTER 4: ACTIONS WHILE TRAVELING

"Perception is reality"

Personality

Do not be a stereotype (i.e. gunslinger, secret agent, obnoxious, etc.).

Be aware of your body language, i.e. mannerisms, facial expressions, and posture.

Four things to consider about your attitude:

- Be confident: In your abilities/job/during presentations/build confidence in others through training.
- Be humble: You do not need to take credit for everything.
- Be friendly: Greetings, smile, expressions of gratitude, etc.
- Be yourself: Use your best qualities.

Maturity:

- Start quiet and ask the right questions.
- Will help you establish credibility with your audience.

Professionalism:

- How you handle yourself, in the situations you encounter.
- Use a positive mental attitude in accomplishing tasks.
- Demonstrated through actions and speech.

Demeanor:

- A subtle overall view of your personality style.
- Beyond superficial appearance and cordial telephone mannerisms lies a person. Someone trying to be a better person is helpful, kind and considerate in the workplace. They are supportive and encouraging for interventions or when providing assistance. They take the high road with their feet firmly planted on the ground.

Manners:

- Always be polite.
- Individuals that act rude are easier to remember.
- People will remember you by your actions.

Speech:

- Slow down your speech. Most individuals talk fast when nervous.
- Know your audience.
- Stay away from jargon and slang. It tends to make some nervous and others lose interest in what you are trying to tell them.

Hairstyle and Facial Hair

Male:

- Generally, military males are recognizable by their more traditional haircuts (i.e. high and tights, high fades, shaved).
- Preferably, travelers will keep a more professional, business style haircut (layered, blocked bottom vs faded) that is in keeping with military standards, unless the traveler is operating under approved relaxed grooming standards.
- Facial Hair: When/if the mission requires relaxed grooming standards; ensure that you are maintaining facial hair to the local custom and/or the approved standard.

Female:

- When not in a military uniform try to keep a more professional or relaxed style to blend with the area in which you are traveling and working.
- Be cognizant of certain styles (cornrows, highlights, pony tails, etc.) that are acceptable or viewed as out of place as they pertain to the area in which you will be traveling and working in.

Travel Attire

What to wear while transiting:

- Professional or Business: Dressing in a professional manner while traveling will help you blend in with many travelers no matter the destination. Business professionals travel as simple as a polo shirt tucked into a pair of jeans, paired with a matching leather belt and shoes. You can always dress more professional with a sport coat and/or slacks as well.
- Understanding the four levels of business dress code will help you understand how to blend with your environment and pack for your trip.
    - Corporate: suit mandatory, shirt and tie mandatory
    - Business Appropriate: shirt mandatory, tie optional, jacket mandatory, suit is preferred
    - Business Casual: shirt or sweater mandatory, jacket not required but preferred
    - Casual: jacket with T-shirt mandatory, with collared shirt or sweater optional, Jeans are OK if you are the boss or your home is the office. Can be difficult to pull off for a meeting, but acceptable for travel.

Examples of business appropriate.

Example of business casual.

- Tourist: Dressing as if a tourist in casual clothes that align with the climate and current weather of your destination is probably the easiest, and most service members will have more of this type of attire. The downfall is this may make you stand out more as an American tourist while traveling.

Example of tourist dress.

- Backpacker/Hiker: Many backpackers travel throughout the world making it easy to blend in with them. When planning to wear this attire, ensure that you are not mixing luggage (i.e., leather briefcase with North Face pack) and your attire matches the climate and local weather.

Examples of backpackers/hikers dress.

- Military:
  - This should always be a last resort unless it is a requirement by your Chain of Command or supported unit.
  - Do not wear military style or affiliated clothing and/or hats. (Check with your organization/Foreign Clearance Guide for further clothing guidelines).

Examples of clothing to avoid while traveling.

- Jewelry
  - Be wary of traveling with too much or expensive jewelry. Thieves easily recognize these items.
  - Wearing jewelry such as class rings, unit rings, Killed in Action (KIA) remembrance bracelets, etc. give away your affiliation with the military and/or the U.S.


Examples of jewelry to avoid while traveling.

- Local clothing:
  - Upon arrival to the area in which you will be working, travelers may want to consider purchasing some local clothing. Local clothing is the best way to blend into the local area while not conducting official business. When conducting official business ensure you are in the appropriate attire (i.e. official duty uniform, business, etc.).

- When purchasing local clothing ensure that it is not offensive for an outsider or foreigner to be wearing the clothes while in the area.

Packing

Use standard civilian luggage instead of military duffle bags. Do not include rank or organization information on luggage tags.

Packing considerations for carry-on luggage:

- Ensure that your carry-on(s) meet the requirements of the Transportation Security Administration (TSA) and the airline you will be using. Do not forget to check all airlines you may be using from departure to the return home.
- It is highly recommended that travelers pack clothes for the following day's activities in the carry-on. Luggage is easily lost/misplaced by airlines when changing planes. Depending on the country you are transiting to, it may be one to two days before you get your luggage returned.
- If carrying a small purse or a handbag, use one that has a cross body or cross shoulder strap, allowing your valuables to stay close to you while leaving your hands free. Ensure that carried purses and handbags are closed at all times unless you are actively reaching for something inside of the bag and close it immediately after you've retrieved what you need.
- Maintain positive control of high-dollar items (laptops, jewelry, etc.). Airlines are not responsible for theft from any baggage.
- Avoid carrying pills (supplements, vitamins) beyond/other than prescription medication properly documented in the original containers.
- Avoid carrying Table of Allowances-50 (Army-Issued Individual Equipment (TA-50)) in carry-on bags. If required, stow in checked baggage.

Example of preferred carry-on luggage to use while traveling.

Packing considerations for stowed luggage:

- Ensure you are familiar with the TSA and Airline Requirements and Considerations.
- Review your final destinations customs rules and procedures for entering. Know what is and is not acceptable to enter the country.

- Know the rules and regulations of departing airports and customs for your return travel.

Packing considerations for military equipment:

- Check country specific restrictions in Foreign Clearance Guide's reference to TA-50 in checked bags, as some items may be unauthorized in that country.
- Try to keep your luggage low visibility and avoid using traditionally ruggedized military luggage and cases.

Examples of military style luggage and gear.

Airports and Transportation Terminals

Avoid hanging around the check-in counter/kiosks and other areas on the unsecured side of TSA/security checkpoints. Most attacks occur prior to the security checkpoints and places where large groups of people loiter.

CHAPTER 5: HOTEL AND ROOM SECURITY

Hotel Security

There are several considerations when selecting a hotel:

- Use on-base facilities when possible or U.S. Embassy designated hotels.
- Distance and route availability to/from U.S. Embassy and areas of work.
- Layers of security outside/inside hotel.
- Infiltration (INFIL)/Exfiltration (EXFIL) or Extraction points from hotel.

Hotel and room security considerations:

- Inspect for possible hiding areas in the room.
- Security of windows/doors (the front desk may have a tool to open windows, if needed for an emergency).
- Any bars or other obstructions on windows.
- Determine the reliability of night watchmen/roving patrol. Are they qualified/armed? Are they establishing routines?

Force Protection (FORCEPRO) considerations:

- Carry a portable security system for your hotel room door. (see Appendix B)
- Web cam software to convert your webcam into a motion-sensing security camera.
    - http://www.ispyconnect.com
    - http://download.cnet.com/Webcam-Motion-Detector/3000-2348_4-75609375.html
- Build rapport with hotel staff and security personnel.
- Decrease presence while at hotel (i.e., lower profile, conversations, and limit time in public areas).
- Vary times and/or location for link-ups with team members and U.S. Embassy personnel. If possible, use different entrance and exit points from the hotel and parking lot.
- Try to select a room above the third floor, but below the eighth floor. Some foreign fire departments do not have the capability to reach above the eighth floor. Your room location should be away from the fire exit and not too close to the elevator. Consider trying to change your room if staying for a long period.
- Maintain control of your key/card at all times. Ensure you do not give out your room number, especially around persons not in your group.
- Know where the emergency exits, plans, and equipment are located on each floor and in the amenity locations throughout the hotel.
- Move the furniture available in your room to block entry access in case of an emergency.
- Create a hotel strip map, if not available at the front desk, in order to learn the layout of the entire hotel and grounds.

- Maintain a redundancy in communications at all times. Ensure your cell phone has the numbers for all members of the group, emergency services, U.S. Embassy, etc. Check landline phones in hotel and room in cases of power outages and ensure each phone has the numbers for police, fire, and rescue services. Hotel may also be equipped with a two-way radio.
- When entering an elevator, attempt to enter when multiple people are entering rather than just one other unknown person. As you enter, stand as close to the control panel as possible. If attacked, press the call button, emergency button, or as many floor buttons as possible.

Other Best Practices:

- Tell-tales: An indicator, signal, or sign that conveys the status of a situation. Tell-tales, when tripped, provide an indication to the traveler that an intrusion of the room and/or drawer was made/attempted.
- Attempt to identify if there are other U.S. personnel staying in the hotel.
- Obtain local area maps and/or tourist maps to improve situational awareness of the area.
- Verify and then reassess E&E and PR plans: Identify and ensure routes for egress, rally points in and out of the hotel.
- Continue to assess layers of security outside/inside hotel throughout the duration of the trip.

General Daily Personal Protection

Make friends and do not be afraid to talk to people. Tip the concierge and other locals who provide assistance. Per Diem is to supplement your travel costs not to be additional personal income. You are in a foreign country and should use it for mission purposes. In doing so, you may increase your own personal security by making friends and being friendly with others.

Should you see a dangerous situation developing - yell. USE YOUR VOICE! A loud voice can be a very effective tool for both defense and alerting others of an impending threat. If you shout at a suspicious person “STOP!”, GET BACK!”, and/or “GUN!” that may be enough to stop them or it may show you a clear determination that they are closing the distance and give you time to react. Either way, others will become aware of the situation.

Whether you are traveling in the Continental U.S. (CONUS) or Outside the Continental U.S. (OCONUS), you should never leave your room without certain items. Every time you close the door to your hotel room, you should realize you might never see it again and ensure you have what you need in the case you cannot return to it. At a minimum, consider taking your passport and/or military ID; cash, both U.S. and local currency; and your PLB and/or cell phone. Your cell phone should already have important numbers entered such as Marine Post 1 (U.S. Marine Security Guard at U.S. Embassy), teammates, your hotel, etc. You need to re-check those numbers if you move locations. Sometimes you will change cell carrier areas and the dialing codes may change. If you do not have a cell phone have a list of important numbers and a method to pay (i.e. phone card).

A multi-tool and/or pocketknife. Always check local laws in relation to pocketknives. Most countries have very strict laws on carrying knives so a simple multi-tool is usually a better option. Daggers and “fighting knives” are discouraged in a non-tactical situation for possibility of general arrest. Defensive strike pens are also a consideration. A small flashlight with a heavy metal bevel will serve as a good defensive tool to

throw an attacker off balance and for striking. It also serves multiple functions, which makes it a more worthwhile item to carry. The Surefire Scout is one example of this type of flashlight.

The Department of State is the lead for the protection of U.S. Citizens in foreign countries. They need to be part of your plan and informed of your plans.

CHAPTER 6: ACTIONS WHILE IN COUNTRY

Intelligence Preparation of the Environment (IPOE)

Conducting a thorough country study and area recon during mission planning is a good practice; you should continue this process once you arrive in country. Budgeting time for and conducting area familiarization, if possible, will help to confirm, deny, or change previous planning considerations. During area familiarization it is beneficial to identify locations of the following facilities and what routes could be used, both by vehicle and on foot, to arrive there: hospitals/clinics, U.S. and other coalition embassies, local military and police outpost/bases, U.S. and host nation government facilities, airports, public transportation hubs, and other U.S. military in the area.

There are numerous items to consider when conducting your IPOE. Break them into categories, as needed, such as depicted below, for organizing your research.

- Area and/or structures: Political precincts/districts, religious boundaries, police/military boundaries, criminal/threat zones, governmental/official buildings, displaced persons camps, street structure patterns, etc.
- Organization/People: Political/military, religious sects, criminal groups, Non-Governmental Organizations (NGOs), ethnic groups, cultural nuances, media or messaging.
- *Events: "Work week", National/provincial elections, holidays (religious/national, Ramadan, Eid'Al Fitr, etc.), agricultural seasons, trade cycles, world events, natural disasters.

  *Events can be routine, cyclical, planned, or spontaneous activities that significantly affect organizations, people, and military operations.

Threat Awareness

When conducting global missions, Soldiers/Units may find themselves operating under unique circumstances where military assets are minimal. When an area contains a small U.S. force footprint, those personnel generally have a limited logistic chain, live on the economy, and have access to limited Personnel Recovery (PR) mechanisms and medical facilities. Additionally, sometimes when the U.S. force footprint is small, host nation emergency services can also be unreliable.

Travelers will need to determine the threats that they may encounter while traveling on global missions. It is encouraged, if not required, to receive a threat brief from the U.S. Embassy. Try to identify potential for host nation (police, military, and government) hostility toward foreigners and, specifically, U.S. personnel.

There are numerous threats travelers could encounter while abroad. Many of them fall outside the combative threats that Soldiers have trained for during present conflicts, such as Improvised Explosive Devices (IEDs). Examples include, but are not limited to: kidnapping, hijacking/carjacking, assassination, arson/Fire and Smoke as a Weapon (FSW), Weapons of Mass Destruction (WMD), cyber (Financial/Security), murder, ambushes, armed assaults, hostage taking, barricades, exploitation, maiming, extortion (check-points), and theft.

Types of Threats

Criminal Threats: Actions by persons with malicious, financial, or personal motivations not connected with larger political or military efforts. In many countries, the criminal threats below may be the most common or most likely threat that encountered:

- Gangs/organized crime
- Thieves (property/identity)
- Prostitutes
- Con-Artists/scams
- Hackers

Law Enforcement/Military: Keep in mind that an encounter with local law enforcement or military is a possibility and there is a potential for criminal activities to occur during these encounters. It is a best practice to comply with any demands to avoid further conflict. Attempt to notify your POC before, during, and/or after a hostile encounter. Listed below are some situations to be aware of:

- Someone impersonating a police officer or military service member
- Corruption (bribes, illegal seizures, and wrongful detention)
- Collection of personal information
- Work with hostile or foreign intelligence services

Foreign Intelligence Services (FIS): An intelligence service responsible for foreign intelligence gathering and analysis. The foreign intelligence service activities are not limited to their country of origin. Trade, transnational business and student exchange, all extend the international reach of foreign intelligence services. Foreign Intelligence Services (FIS) can conduct hostile intelligence operations. These operations span all intelligence tactics to include traditional espionage (tradecraft), the use of sophisticated electronic devices, and technology transfers.

Cyber Threats: Online hacking and theft of confidential information such as credit cards, social security numbers, etc. The accidental loss or sharing of personal information can make you the target. Limiting exposure to online threats is very important.

Lone Wolf: A lone wolf is someone who commits, prepares for, or suspected of committing or preparing for, violent acts in support of some group, movement, or ideology, but who does so alone, outside of any command structure and without material assistance from any group.

Insider Threat:

- Collection by host nation partners on U.S. personnel for targeting.
- Violence stemmed from anti-U.S. sentiment and/or grievances.
- Theft of property or classified materials.

Terrorist/insurgent: Actors aiding in a political or military effort for which you are the intended target.

Indirect threats: Actions taken where the local population or rival threat elements are the intended target, but you are unintentionally affected. For example:

- Protests
- Riots

- Civil Instability
- Drastic change in political climate
- Turf Wars
- Neighborhood crime

Travelers should determine their protective posture and measures based on five factors:

- Type of threat**:** Ambush, roadblocks, IEDs, street crime, etc.
- Situations and locations where threats are most likely to happen: In vehicles, at choke points, in specific neighborhoods, in particular regions, day versus night, etc.
- Cause of the threat:
    - Crime/banditry: Malicious, financial, or personal motivations not connected political or military efforts.
    - Direct threats: Actions taken by a threat (usually politically or militarily motivated) where U.S. personnel are the intended target.
    - Indirect threats: Local or rival threats are the intended target, but U.S. personnel are unintentionally affected.
- Threat level: The likelihood that you will face the threat (high, medium, low).
- Potential changes in threats: Mindful of a changing environment and emerging threats.

The presence of any threat indicator should trigger a closer examination of the situation to determine whether a change is likely.

- Situational awareness. This is primarily a matter of vigilance (constantly looking for changes) and discipline (remembering to ask yourself whether anything has changed, either at the end of every day or week). Establish a baseline of your environment and actively hunt for anomalies (changes) based on normal patterns of life.
    - Depending on your environment, what are the most likely and most dangerous possibilities?
    - Continue to develop you plan of action to address these possibilities.
- Near- to mid-term changes. Indicators of changes in the situation may point to a potential change in near- to mid-term threats. Political change, regional stability, riots, elections, etc.
- Warning of imminent confrontation. The local populace and security forces will have warning signs of confrontations (military battles, riots, etc.). Use their visible preparations for confrontations as indicators of an imminent threat.
- Regional/Area of Operations Indicators:
    - Demobilization of soldiers: Unemployed soldiers will often take mercenary-style jobs, using skills for other employers.
    - Poor unemployment and economic conditions: May signal unrest in the area as locals become desperate to provide for their families.
    - Government budget constraints (lower pay to soldiers or police): Soldier and police morale may significantly decrease if they feel their living wage is insufficient.
    - Splits within military/rebel command structures.

    - Increased use of indiscriminate weapons and tactics against enemies and/or unarmed citizens.
    - Military offensives for which there are no clear battle lines.
- Security Forces Preparations Indicators:
    - Military convoys on the road: Increased patrols and presence in the area. Convoys may consist of acquired civilian trucks and other vehicles, rather than expected military vehicles such as HMMWVs.
    - Increased recruiting: Additional advertisements in newspapers and television and a larger military presence around schools.
    - Departure of soldiers' families: Areas around military bases may become less busy, with fewer people frequenting local shopping areas.
    - New checkpoints or checkpoints manned by soldiers instead of police: Soldiers carrying heavy weaponry may replace friendly local police. Wire, barriers, and other methods begin to reinforce checkpoints.
    - Designation of restricted areas: Areas that were once frequented by the public will suddenly be placed off limits, often denoted by signs and wire.
- Local Preparation Indicators:
    - Families departing from area: Neighbors and local families suddenly packing large suitcases or boxes as if in preparation for being away for an extended period.
    - Hoarding of food, supplies: Grocery stores and local hardware stores are suddenly having a problem keeping supplies in stock and shelves often appear empty.
    - Staff staying home with families: Large numbers of embassy staff or other local personnel calling in sick or asking for an extended amount of days off.
    - Children staying close to home/parents: local schools closing unexpectedly or having extremely low attendance.
    - Markets closed/limited: Markets that were once busy now seem desolate. Vendors, shoppers, and tourists have all stopped coming to public markets, or the markets themselves may be closed.
    - People not going out at night: Curfews may have been imposed on the local populace, or there is just no activity after dark. Areas that were once busy at night, such as local clubs, are either closed or nearly empty.
    - People staying off the road: Less activity on the road. Roads that may have been jammed with traffic on the way to work just a few days ago are nearly empty.
- Criminal Threat Indicators:
    - Loitering during work/school hours: School age or working age men and women loitering in odd areas for hours at a time, often in large groups.
    - Bars on windows/doors: Common buildings such as grocery stores, schools, government buildings, and homes have steel bars over windows and doors.
    - Graffiti: Assorted graffiti in public areas. If possible, find out what local graffiti symbols mean and to what groups the graffiti may belong.

    - Damaged property/vandalism: Property, especially government buildings, police stations, schools that have had windows broken out, been burned, or otherwise damaged.
    - Minimal essential services: Sewage, water, electricity, and/or trash are reduced or stopped.
- Terrorism indicators: Non-direct threats can support terrorist operations and goals through criminal activities.
    - Surveillance
    - Elicitation/inquiries: Prostitution, illicit activity, bars, clubs, etc.
    - Testing Security: Unauthorized areas, fake IDs, etc.
    - Funding: Moneychangers, illicit activities, prostitution, donations, money laundering, frauds, etc.
    - Acquiring Supplies: Caches, missing personal or unit items
    - Impersonation: Fake IDs
- Most threats can be mitigate by completing a thorough area study, knowing your environment, maintaining situational awareness, practicing good OPSEC, maintaining personal security (Two-man rule, informing others of plans), watching for pre-incident indicators, and using common sense.

Individual Protective Measures

Target selection: Terrorists and criminals prefer a soft target that involves little risk and a high probability of success. They are unlikely to select a target that involves high risk with little or no chance of success. Individual protective measures may affect target selection. There are two types of targets, hard and soft.

- Soft targets tend to be unarmed, accessible, predictable, unaware, and/or have a low security profile.
- Hard targets tend to be armed, have a hardened vehicle/residence, have communications, an escort vehicle, maintain heightened awareness, and/or are unpredictable.

Ease vs. value: Threats will not attack a hard target unless ordered to do so or the value outweighs the risk. In most cases, they will simply pick an easier target. One of the best ways to make yourself an easy target is to form regular routines.

Travel in Country:

Travel Protective Measures:

- Carry your documents strategically and consider using a “mugger’s wallet”. Use an old wallet that contains a small amount of local currency, an expired hotel key card, old receipts from cash purchases, and other non-attributable items that you are willing to give up if robbed. Keep your real wallet in your front pocket/pocketbooks close to your body.
- Know the safe areas: Avoid hostile demonstrations, areas of civil disturbance, ghettos and mobs.
- Create a crisis response plan and disseminate to all members of the team, the country team, and your home station unit POC. Considerations for your plan should include, but not be limited to:
    - An evacuation plan that includes where to go for evacuation.

    - Rally points for all locations you plan to be.
    - Know safe areas and possible hostile areas along your routes.
    - Locals may be "immune" to seeing street crime and not willing to assist.
    - POC list for personnel to contact in country and other locations.
    - Be prepared for a confrontation (Fight or flight).
- Keep a "go bag" ready and accessible at all times. (See Appendix C)
- Avoid public transportation as these places may become crowded.

Pedestrian Travel:

- Be alert and in the moment, but careful not to be overly cautious. This can raise suspicion of law enforcement.
- Know your environment and exercise situational awareness while being mindful of potential surveillance.
- Train yourself to walk facing vehicle traffic while adhering to the normal flow of pedestrian traffic.
- When walking along a sidewalk, stay toward the center.
- Stay near people and avoid isolated areas.
- Use light and noise advantage
    - Walk in well-lighted areas where there are other pedestrians.
    - Avoid areas where noise will drown out your cries for assistance.

Vehicle Operations:

- What are the local traffic patterns and laws?
- Vehicle availability: 4X4, front wheel drive, rear wheel drive
- Familiarize yourself with the routes and area prior to driving.
- Documentation: License, registration (plates/stickers), required decals
- Cellphone/radio: Call Signs or POC's
- Ensure you have updated GPS/maps for the area you are driving.
- Familiarity with right side driving vehicles.
- Create a vehicle-packing list for the environment you are traveling in. Ensure to have enough water and snacks/food to sustain all occupants for at least 24 hours. Attempt to store items out of site to prevent potential theft, and use caution when securing these items to prevent harm to passengers in the event of an accident/roll-over. There is no "one size fits all" packing list. Depending on your Area of Operation (AO), and mission, you may need to develop a packing list to meet your specific needs. You may consider a variation of packing lists that could include survival items, vehicle recovery items, safety items, medical supplies, communication, etc. (See Appendix C for examples)
- Vehicle Maintenance:
    - Identify individuals on your team that may have the talent to conduct expedient repairs in an emergency. (See Appendix D for examples)

- Identify local vehicle repair sites (U.S. Embassy repair facility or vetted repair facility). When using off-site repair facilities make every effort to remove personal, high dollar and sensitive Items, or observe the repairs to prevent loss of these items.
- When possible, keep common repair parts on hand (petroleum, oils and lubricants (POL), spare tire, flat tire repair kit, hoses, filters, drive belts, spare batteries, etc.)
- Always check the glove compartment and under the seats for personal items.

- Navigation:
  - Develop efficient route planning techniques for both rural and urban navigation. Consider primary and alternate routes to safe locations in the event of an emergency.
  - Develop driver/passenger communications while driving and navigating.
  - Limit halts for map checks.
  - GPS-dependent navigation provides efficient and known routes, but limits area awareness, route information, and individual memory.
  - Map-dependent navigation provides good area awareness, but it is potentially inefficient and requires frequent checks. An operational area map with routes and locations could compromise your plans.
- Vehicle:
  - Always keep the gas tank at least half-full and fill up whenever possible in the event you must evade an attack or the AO.
  - Key Control
    - Control your keys at all times.
    - When you leave your car with parking attendants or mechanics, leave only your ignition key.
    - Keep any copies of the vehicle key separate from the primary.
  - Keep your vehicle in good repair at all times. Review the scheduled maintenance and ensure the vehicle is good prior to taking possession. A down vehicle may cause you to become an isolated person.
  - Try to get a vehicle with an interior trunk escape latch.
  - Carry fire extinguishers in the vehicle.
  - Equip the vehicle with first aid and survival kits (See Appendix C).
  - If the vehicle is equipped with armor, make sure the vehicle suspension is able to handle the extra weight.
- The Driver:
  - The driver should be trained and prepared to respond to any situation.
  - The driver's primary responsibility is to drive the car. Until the vehicle comes to a halt, the driver should not use a gun, a radio, or any other device.
  - The car, in many cases, can serve as an excellent weapon and/or tool of escape.
  - Many schools offer classes in defensive/antiterrorist driving. If these schools are not available, there are excellent internet resources (video) that provide instruction.
  - The driver should always maintain a cautious (and careful) attitude.

- While driving, the driver should visualize two or three blocks ahead. He should constantly think "what if" during the entire drive.
- If/when using an assigned driver (chauffeur) check with the embassy or MILGRP for prospective drivers. There are three basic rules to follow:
  - Driver remains with the vehicle at all times.
  - While he is waiting for your arrival, instruct the driver to stand away from the car and observe for anyone tampering with it.
  - If the driver is not at the vehicle when you approach, do not enter it.
    - Prearrange a signal with the driver showing that it is safe to board (such as the driver taking his hat off or placing a pack of cigarettes on the dash).
    - Never give your itinerary to the driver. Be particularly cautious about giving out schedules.
    - Inform the driver of your destination only after he starts the car.
    - Never enter the vehicle with a substitute driver until you have checked his credentials with the embassy or MILGRP.

- Considerations while traveling in a vehicle:
  - As a passenger, ensure to stay mentally alert at all times.
  - A small mirror attached to the passenger's visor can help you observe the rear, since the driver will be focusing on operating the vehicle.
  - Constantly vary your routes and routines.
  - Drive with the doors locked and always fasten your seat belts.
  - Minor Traffic Accidents:
    - Quickly determine whether it is a ruse to stop your vehicle.
    - If you suspect a ruse, leave the scene of the accident and drive directly to the embassy or MILGRP.
    - Report the accident and your involvement to the local police as soon as possible.
  - Halted by Police:
    - If the police halt you, do not get out of your car.
    - Keep the engine running and roll down the window low enough to allow voice communication and the passing of documents.
    - Stay alert for unusual actions.
    - Should the situation warrant a sudden exit, proceed to the embassy or MILGRP and immediately report it.
  - Roadblocks/Checkpoints:
    - Quickly determine if the roadblock is official by studying the uniforms and vehicles of the police or the military. Uniforms should match, and equipment should be alike. Criminals/terrorists steal uniforms and will have imperfections.
    - If the threat is imminent, keep your vehicle as far out of any "kill zone" as possible.

        - At no time should you allow yourself to be boxed in without the possibility of escape.
    - Inner/Left lanes (Region Specific):
        - Drive in the far left lane so that your vehicle is unable to be forced to the curb.
        - At traffic lights or stop signs, stay in a lane that will allow maneuverability out of a crisis. Allow at least 8 to 10 feet between your vehicle and the one in front of you. (The rule of thumb is one foot of ground between the rear tire of the vehicle in front of you and the top of your hood as you are looking over your steering wheel.)
    - If there is a decision to run the roadblock consider:
        - What lies ahead
        - Is turning around possible
        - Moving through vs. moving around the obstacle
        - Using the vehicle as a weapon

Improvised Weapons

An improved weapon is a device originally intended not to serve as a weapon, but has the ability to. Improvised weapons are used when conventional weapons such as firearms are unavailable or inappropriate. Basic principles of improvised weapons include:

- benign and not automatically viewed as a weapon
- strong enough for its purpose
- better than an unarmed option
- quickly and easily employed

Examples of common improvised weapons include:

- car keys
- water bottle
- umbrella
- hairbrush/metal comb
- backpack/purse
- belt
- tightly rolled newspaper
- sporting equipment
- carabiner
- flashlight, lock, or a heavy object in a sock or pillowcase.

CHAPTER 7: POST TRAVEL

After Action Review (AAR)

Conduct a thorough AAR from before travel started, during travel, and the return home.

Adjust any travel SOPs and inform future travelers of your lessons learned.

Intelligence Debriefs

Ensure you coordinate and conduct any required intelligence debriefs with the ASCC and/or GCC.

Upon return to home station conduct a foreign travel debrief, and report any unusual encounters with your Unit S2 or Special Security Officer (SSO).

Travel Documents

Keep all travel documents (i.e. receipts, vouchers, etc.) until DTS is complete, the government travel card and traveler receives payment, all credit cards used during travel are paid, and credit card/bank statements are received.

Documents and notes

Consolidate and record notes in a post travel report IAW your units SOP.

Sanitize all personal notebooks.

Electronic maintenance

Update all security software.

Have your communications section analyze government equipment for any tampering before connecting to any government network.

Social Media Awareness

Remove Publically Available Information (PAI) in pictures and information before posting.

CONCLUSION

In summary, the purpose of this document is to serve as a reference guide to assist you with preparing for situations you may encounter during travel. Although no one can predict every situation that may arise, you should have a basic understanding of what situations travelers have faced in the past and ways to prepare and react to them. It is your responsibility to research all aspects of your upcoming travel, prepare contingencies, and continually refine your plans, even after arrival. Many people have experience traveling, whether with the military or as a tourist, and most of the time they have not faced any significant issues as described in this document. However, the intent is to assist you in preparing for that one time when you may have to make a quick decision using only the tools you have to save yourself or others.

Everyone thinks, “It will never happen to me.” The more preparation you do now, the more likely you are to have a safe and successful mission.

APPENDIX A

Example of a Trip Emergency Plan

Note: These are minimum requirements. Consult Service and Unit PR POCs for specific OCONUS travel requirements that may be more detailed and restrictive.

I. All travelers should complete and submit a Trip Emergency Plan (TEP) to all of the following: their unit PR office, their service component PR Coordination Center (PRCC) or the COCOM Joint Personnel Recovery Center (JPRC), and the supported country U.S. Embassy RSO/ODC.

II. See the example of a Trip Emergency Plan format on the next page. This plan will contain these four elements at a minimum:

1. Who, What, When, Where of travel
2. Communication PACE plan
3. Actions upon Isolation PACE Plan
4. Include a list of survival and communication equipment and contact numbers.

NOTE: PR plan may be part of a component force protection plan requirement. Check component requirements.

III. All travelers should:

A. Have a communication capability to alert the Personnel Recovery Infrastructure of isolation. Examples of how to meet this requirement: have access to a cell phone, Satellite Phone, 406 emergency beacon, Blue Force Tracking Devices 911, etc.

B. Have a procedural check-in plan in place while traveling in an Area of Responsibility (AOR). Accomplish this by setting up a daily check-in procedure with a Unit POC, the DATT/SDO, the component PRCC, or other control center. Movement Reports – Emailed to _____: Complete this prior to departure and upon arrival at deployed destination. Daily Sign of Life (DSOL) – Emailed to_____.

C. Carry a visual signal device, a map of the area, a medical kit, and potable water or a means to purify. It is highly recommended that personnel traveling outside of major urban areas also carry a blood chit, a Visual Language Translator (VLT), additional maps, a secondary communication device, and additional survival gear that could support the isolated personnel for up to four days.

IV. Locate the for contact information of the Component Personnel Recovery cells and Joint Personnel Recovery Cell.

V. Key numbers

Intl access from U.S. is 011/from Europe is 00 ("+" on cell phone automatically inserts appropriate int'l access code.)

UNCLASSIFIED (may be classified once completed) – UNCLASSIFIED//FOUO			
PERSONNEL RECOVERY(PR)/ISOLATED PERSONNEL(IP) ACTION PLAN ITINERARY			
Name(s) (Who)	Destination(s) (Where)	Arrival Date(s) (When)	Departure Date(s) (When)

Briefly describe your mission profile (What) APACS#

Communications Devices	
What Communications Devices do you have?	IDs/Phone #s/Freqs/Sim #/Etc

What is your Communications PACE plan and Accountability procedures?			
PACE	Description (means)	Personnel accountability procedures	Frequency
Primary			Daily – every 24 Hrs or during movement
Alternate			Daily
Contingency			
Emergency			

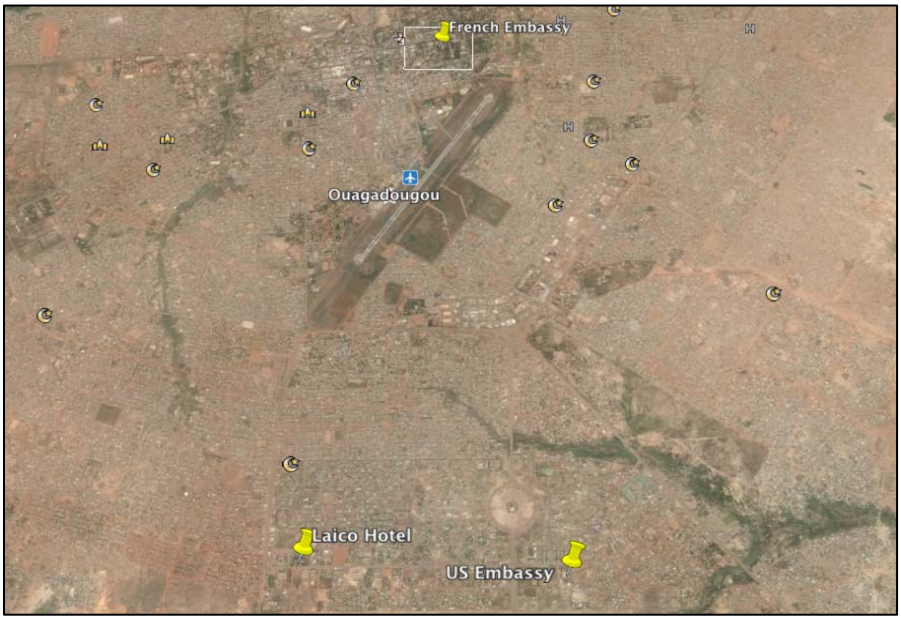
What PR equipment do you have?		Numbers saved in cell phones	
Signaling	Survival	e.g. In Country POC	
		e.g. Component JOC	
		e.g. Component PRC	
		e.g. Marine Guard 24/7	
COCOM JPRC 24/7		e.g. HN equiv "911"	
COCOM JOC 24/7		e.g. Hotel –	
Embassy Switchboard		e.g. Tricare/Medical SOS	
OPS			

What is your "actions upon isolation" PR Movement Plan (PACE Plan)
PRIMARY: ALTERNATE: CONTIGENCY: EMERGENCY:

The following pages of the TEP should include maps from the airport to the hotel, the airport to the embassy, the hotel to the embassy, and any other known locations of travel.

Below are examples of maps of the local airport, hotel and embassies. Add details to the maps such as pre-planned primary and secondary routes for everyone's knowledge as well.

Note: Routes will need to be confirmed when in country, as some roads will no longer exist, be unpassable by vehicle, or overly crowded during travel times.



Example imagery

Example imagery

APPENDIX B

Hotel Security Devices

Below are examples of door security devices. These devices may make it more difficult for an attacker to enter a hotel room.

Veritas Traveler's Doorstop

Doorjammer Portable Security Device

Mace Big Jammer Door Brace

APPENDIX C

In Country Packing List Examples

Example of “Go Bag” items

“Go Bag”

Pictured:

- Credit card with RFID sleeve
- Passport/documents with RFID sleeve
- Water purification system (iodine tablets)
- Fire starter
- Multi-tool
- Whistle
- Signaling devices
- Evasion Kit
- Small device charger
- Space blanket

Not Pictured:

- Rations and supplies
- Bottled water

- Maps
- Small supply of cash
- Traveler's checks (ensure they are accepted)
- Flashlight/headlamp with spare batteries
- First aid kit

Vehicle Equipment List

Baseline:

- “Go bag”
- GPS
- Maps
- Spare key for vehicle
- Communications equipment (PACE)
- Spare tire (full size)
- Jack and tire iron to change tire
- Basic vehicle tool kit
- Emergency kit
- Coins/passes for tolls
- Snacks
- Bottled water
- Pen/paper
- Digital recorder
- Camera
- Cigarette lighter adapter

Long-term TDY/mission dependent considerations:

- Vehicle recovery gear (tow strap, tree saver, come-along)
- Fuel cans
- Change of clothes
- First aid kit (See Safety and Survival below)
- Ammo
- Weapons


Example of Survival Kit items

Survival Kit:

- Adhesive tape
- Antiseptic ointment
- Alcohol swabs
- Band-Aids (assorted sizes)
- Blanket
- Disposable gloves
- Gauze pads
- Hand sanitizer
- Plastic bags
- Scissors and tweezers
- Small flashlight and extra batteries
- Triangular bandage
- Burn-aid gel
- Snake bite kit
- Disposable emergency blanket
- Instant cold pack
- Instant hot pack
- Combat gauze
- Tourniquet

Medicines:

- Loperamide (anti-diarrheal)
- Malarone (anti-malarial)
- Tylenol

- Ibuprofen (anti-inflammatory)
- Benadryl (allergic reactions)
- Cipro (broad spectrum antibiotic)
- Epinephrine or Epi Pen (serious/fatal allergic reactions)

Personal Essentials:

- Water: One gallon per person per day. Drier, hotter climates may require more.
- Food: Bring food for twice the amount of time you plan on being gone: trail mix, beef jerky, fruits, dry/canned food, etc.
- Extra Clothes: Nobody likes to sit in wet clothes for an extended period.
- Sun block
- Rain Jacket
- Trash bags (keep your trail clean)
- Maps, information about the area
- Compass and/or GPS
- Water purification tablets (Iodine)

Communication:

- PACE plan for communications (Redundancy)
    - Primary: 2 way vehicle to vehicle (Multiband Inter/Intra Team Radio (MBITR))
    - Alternate: Cell phone
    - Contingency: Satellite Communication (SATCOM)
    - Emergency: Iridium
- Power converter/inverter if necessary
- Spare batteries
- Solar panels for charging small devices

Safety:

- Safety glasses
- Leather gloves
- Fire extinguisher (Preferably mounted in the vehicle in an easily accessible location)
- Flares
- Tarp
- Flashlights
- Matches/lighter

APPENDIX D

Cyber security reference information

Cyber Electromagnetic Activities (CEMA) Defined

The cyber domain and the Electromagnetic Spectrum (EMS) are used together in everyday activities, both personal and military. The electromagnetic spectrum is the physical medium that devices (such as computer, phones, routers, radios, etc.) use to wirelessly transfer data/information. Cyberspace is the networked non-physical terrain in which data/information exchange occurs between computers (i.e. the internet). A basic way to view the concept of Cyber Electromagnetic Activities (CEMA) is to consider your home network. For example, you use your computers, tablets, smart phones that wirelessly receive/transmit data via radio frequencies (which is in the electromagnetic spectrum) and exchange information that resides on the internet (cyberspace) such as browsing websites, updating social media, downloading media, reading/sending emails, etc. Wi-Fi, cellular networks, or satellite communications are all just means you can use to access networked information in the cyber domain.

Cyberspace

Cyberspace is broken into three specific levels: physical, logical, and cyber persona. Each of these layers are interdependent networks and information that build the cyberspace structure and ways we communicate. When mission analysis is completed, the cyber threat is viewed as a mesh of these three layers. Specific analysis is conducted considering the above information and associating it with the correlating cyber threat layer.

- The physical network is considered the local level. This layer includes geographic and physical network components. The geographic component is the physical location of elements of the network. The physical network component includes all the physical equipment associated with links (wired, wireless, and optical) and the physical connectors that support the transfer of code and data on the networks and nodes. For example, physical networks components may include wires, cables, radio frequencies, routers, servers, computers, radars, weapons systems, telecommunications systems, personal digital assistants, and other networked devices where data is created, manipulated, processed and stored. The geographic component would then be the locations of all those devices and connections. U.S. Commanders and staffs identify physical entities in cyberspace that may require specific effects and prioritize them for information collection, targeting, and assessment.
- The logical network layer is thought of as a mobile layer that incorporates the invisible information being transmitted as well as the visible mobile devices being used. It consists of the components of the network that are related to one another in ways that are abstracted from the physical network. For instance, nodes in the physical layer may logically relate to one another to form entities in cyberspace that are not tied to a specific node, path, or individual. Web sites hosted on servers in multiple physical locations where content can be accessed through a single uniform resource locator or web address provide an example. U.S. Commanders and staffs identify logical entities in cyberspace that may require specific effects and prioritize them for cyberspace information collection, targeting, and assessment.

- The cyber-persona layer is the social layer and is one of the most vulnerable layers because of the interaction with other people or organizations. Whether Facebook, Foursquare, Google+ or other networking sites, you are putting information out about yourself and potentially your mission that could be used by adversaries. The cyber-persona layer is an abstraction of the logical network, and it uses the rules of the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. This layer consists of the people who actually use the network and therefore have one or more identities that can be identified, attributed, and acted upon. These identities may include e-mail addresses, social networking identities, other web forum identities, computer internet protocol addresses, and cell phone numbers. Cyber-personas hold important implications for Army forces in terms of attributing responsibility and targeting the source of a cyberspace threat. Because cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, significant intelligence collection and analysis capabilities may be required.

CEMA APPLICATION

CEMA is used in almost every aspect of accomplishing the mission. From surveillance, to communications on the battlefield, to targeting, to battlefield situational awareness, all of these efforts require the use of some aspect of the cyber domain and/or the Electromagnetic Spectrum. The increased use of wireless systems – including the use of Commercial Off-The-Shelf (COTS) systems – makes the available EMS a high-demand resource. The resulting electromagnetic environments in which forces operate are highly contested and congested, making unencumbered access to the EMS problematic. The most important thing to stay focused on is that just as we have interests and operations in Cyberspace and depend on cyberspace, so do our enemies.

Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 1-02). Operations in cyberspace contribute to gaining a significant operational advantage for achieving military objectives.

CEMA VULNERABILITIES AND THREATS

Cyber-security is vital to protecting the confidentiality, integrity and availability of your information and operations. It is critical to your mission success and therefore must be part of your risk management processes. It is essential in assisting you with identifying vulnerabilities and taking the necessary steps to conduct your daily operations. Army regulations, policies and guidance provide the Army imperatives authority, responsibility and accountability necessary to promote a culture that is risk aware and complies with practices that minimize vulnerabilities to Army networks, systems and information. (FM 3-38)

Threats exist to information on Government devices operating on Government networks, Government devices on non-government networks, and personal devices on private and public networks. The physical vulnerabilities, insider threats, and virtual threats can cause a breach in mission information or a compromise of Personally Identifiable Information (PII) that may result in jeopardizing national security, the lives of soldiers on the ground, and an individual's identity. The impact of any of these threats is detrimental to the overall mission and can cause significant consequences.

Cyberspace threats are real, sophisticated, growing, and evolving**.** As the Army trains, organizes, and equips to take full advantage of cyberspace's potential, you must recognize that adversaries want to undermine your ability to operate freely. You must anticipate threats' attempts to disrupt missions, plan for an adversary's potential ability to destroy friendly networks, and account for the impacts of social networks on Army operations.

Be aware of your surroundings when you are conducting personal business, talking on the phone, or video chatting. You never know who is around the corner listening to and taking notes about you. Your Common Access Card (CAC) protects sensitive information in emails and computer files by allowing you to encrypt them.

Physical Vulnerabilities: Loss of individual CAC, compromising/sharing Personally Identifiable Number (PIN), leaving your computer or device logged-on and unattended, allowing someone else to use your login credentials, being overheard while talking on a phone or over a video chat. These vulnerabilities are things that you can easily control at a personal or individual level. Some of these may seem common sense, but they are still a first layer of mitigation that can help ensure the safety, security, and success of your mission. Always maintain control of your CAC and SIPR Token. Your CAC is a physical piece of Information Awareness (IA)/Cyber-security and is tightly bound to your online identity and it must be protected at all times, even when not in use. If you lose or misplace it, report it as soon as it is confirmed to be missing.

Insider Threats: individuals acting suspiciously (odd work habits, unexplained communication with foreign or questionable organizations), requesting access to information that is outside the scope of their responsibility or need to know**.** Be on the lookout for things that do not make sense about individuals where you work. The odd work habits, late hours, or unexplained foreign interaction could be indicators that something is wrong. Use extra caution and report it.

Virtual threats**:** viruses, Trojans, malware, web crawlers, identity theft.

- The Internet poses serious potential threats. You must constantly ensure all computers and devices meet the appropriate security requirements before connecting them to the network. All office and home computers must be up to date with required system security patches, Anti-Virus software applications, and should only be connected to the internet from behind a firewall. The Army Home Use program makes it easy for Army Soldiers to secure their home computers by giving them free access to both Symantec and McAfee anti-virus and firewalls.
- Web Address: https://patches.csd.disa.mil/Metadata.aspx?id=79775
- Example: Phishing emails claim to be from a trusted source and requests your personal information, or directs you to a seemingly innocent website. These phishing attempts are usually obvious. However, phishing is a major issue that plagues the Army. Phishing is often successful because the improved quality of these attacks makes it more difficult to identify them as a hoax. Phishing attacks have also become more sophisticated, targeting specific individuals with content customized to them.

  *This is just one type of attack – the bottom line is if the email seems odd, out of place, asking for sensitive information and you cannot verify the sender or purpose, report it.

Mobile and Cellular

Mobile and cellular devices use a wireless signal from the mobile unit to the base station/cell tower and from the base station to the base station controller. Wireless signals can be highly vulnerable to recording, interception, tracking, and data mining.

Department of Defense and Army policies prohibit connecting unauthorized information systems to the network, and prohibit conducting official business on personally owned devices that do not meet Army standards and certification requirements. The Bottom Line Up Front (BLUF) is do not connect your personal devices to a government network and do not house unauthorized PII on your personal devices. Although the Army is currently considering a strategy to allow personal mobile devices access to the Army Network, personal cell phones, tablets or other mobile devices are currently not authorized for access and government use.

Using unapproved devices for official business is not only a security violation, but could also cause major security incidents jeopardizing sensitive information and putting our operations and personnel at risk. Compromising classified information in these cases is a serious security violation that may result in punitive actions.

A major vulnerability to mobile technology is interception, when the enemy intercepts information or a transmission between you and the intended recipient. Wireless connections (Wi-Fi, Bluetooth, Cell phone connections) can be intercepted at any point; if precautions are not taken to ensure that the information is secured or certain information is not transmitted under vulnerable conditions the result could be significantly detrimental. Example of a vulnerable network would be using a public Wi-Fi connection at a coffee shop or searching for a "free" internet connection at an airport. If you do not know the source of the signal, do not trust it.

Eavesdropping

- A primary risk is eavesdropping --- that is, someone being able to "listen in" on the phone call or video chat without the knowledge of those on the line. An attacker can eavesdrop from many locations on a cellular telephone phone call. A key contributing factor is that people will often talk more loudly when they are using a mobile device, increasing the risk of interception with minimal technology required.
- More advanced interception can happen if the enemy is using an environmental microphone. This risk centralizes on the importance of minimizing risk by keeping your voice down, only using the devices in areas you know are secure, and not discussing personal information, government information, or information relating to your mission or purpose in that location.

Downloaded code

- Many of today's cell phones allow code to download and run. The phone's user can download the code or it can be "pushed" by the provider or attacker. This code could change the behavior of the cell phone. For example, it has been widely reported in England that the police have downloaded "wiretapping" code to certain cell phones. This code turns on the microphone whenever the police want, allowing them to use the phone to bug a room.
  *The only way to protect yourself against this kind of threat is to remove the battery.

Recording

- Answering Machines: It is common for telephone conversations to be inadvertently recorded by answering machines. This risk applies to both wired telephones and to wireless ones.
    - Handset voice recorders. As the memory in cell phones increases, it is expected that cellular telephones themselves will increasingly be equipped with the capability to record "voice memos" or to record entire telephone conversations.
- Traffic analysis is another tool that can be used against you as its information that can help establish a pattern about what you do, what you are interested in, and who you talk to.
    - Call Detail Information: Cell phone providers typically record the time, date, duration, calling number, called number, and location of the cell phone for every phone call placed on their network. Some (but not all) of this information is presented to subscribers on their telephone bill. Both the records in the provider's computers and the printed (or downloaded) bill could disclose a caller's relationship or location without their knowledge.
    - Call History: Cell phones will record call detail information and store this information in the phone itself as a "history" of recently placed, received, or unanswered calls. This information can be disclosed to anyone who is holding the telephone.
    - Phone Book: Just as the call history can contain confidential information, so can a telephone's phone book.
- Cached Information is like the internet history or temporary internet files on your home or work computer.
- Recovery of Deleted Messages: Just like any other computer system, phones do a poor job of actually overwriting the data when a user tries to delete a message. In practice, this means that Short Message Service (SMS) messages, call logs, and even the list of cell towers that your phone has touched can be retrieved by an attacker or forensic expert. So if you do not want it to be seen later, do not send it.

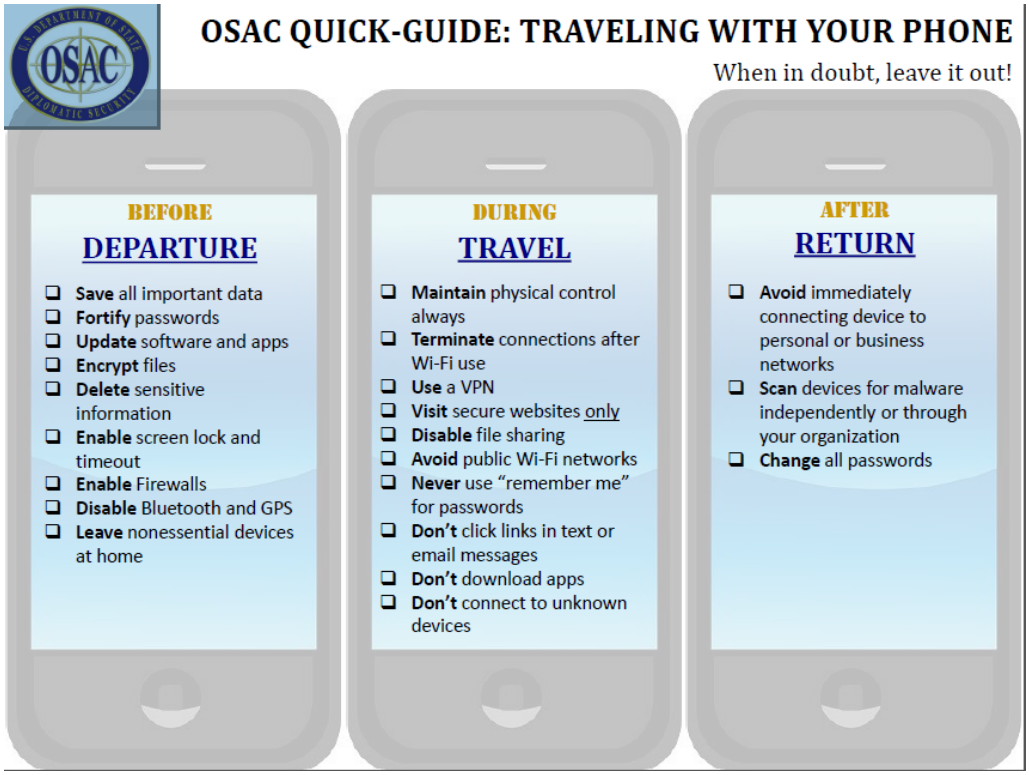
Geolocation

Geolocation is the ability to use a cell or Wi-Fi network to establish your location information. In order to function properly, the telephone network needs to know where the phone is located. It has been widely reported that some telephone providers keep this location information on file for extended periods. This information can be made available to the police or other organizations under certain circumstances.

- Global Positioning System (GPS): Because of the U.S. E911 regulations, many phones sold in the U.S. are now also equipped with a Global Positioning System receiver. This makes it even easier for the provider/attacker to establish the cell phone's position.
- Geotagging: Pictures you take with you GPS enabled device will geotag your photo, embedding information into the metafile about when, where and with what type of device you took the photo. Uploading this file to websites such as Facebook, Foursquare, or Flickr can create a digital footprint of everyplace you have been that is accessible to almost anyone.
- Tracking: Some phones allow themselves to be locked. If locked, both the phone's call history and the phone book cannot be accessed unless the phone is unlocked. Be aware; however, all phones have "administrative codes" that allow them to be unlocked in the event that the subscriber

forgets the password they used to lock the phone. If having the phone on for communication means is necessary, turn off the GPS. However, be aware that your phone can still be tracked through its cellular connection pinging from cellular tower to tower. This method is more advanced, however not impossible.

- Targeting: Cell phones emit radiation. This radiation can be used for targeting weapons. HARM (High-Speed Anti-Radiation) missiles, in particular, can use the radiation emitted from a cell phone as a homing beacon.
- If you do not want your positioned tracked, turn off your cell phone!



Social Media

Active social networking on a personal level is a great way to keep in touch with friends, family and colleagues. It is even used on a military level as a means of information dissemination. However, just as they are able to track your status, location, mood, destination, and likes, so can our enemies. Be cautious with the information that you post on social media sites.

The Federal Bureau of Investigation (FBI) has a great breakdown of the Social Networking threats. Read these types of attacks and think about it next time you log on to your social networking site. There are primarily two tactics used to exploit online social networks. In practice, they are often combined.

- Computer savvy hackers who specialize in writing and manipulating computer code to gain access or install unwanted software on your computer or phone.
- Social or human savvy hackers who specialize in exploiting personal connections through social networks. Social hackers sometimes referred to as "social engineers," manipulate people through social interactions (in person, over the phone, or in writing).

Humans are a weak link in cyber security, and hackers and social manipulators know this. They try to trick people into getting past security walls. They design their actions to appear harmless and legitimate. Falling for online fraud or a computer hack could be damaging for an individual victim as well as the organization for which the victim works.

Baiting

Someone gives you a Universal Serial Bus (USB) drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer. Do not use any electronic storage device unless you know its origin is legitimate and safe. Scan all electronic media for viruses before use.

Click-jacking

Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking frauds have employed “Like” and “Share” buttons on social networking sites. Disable scripting and iframes in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

Cross-Site Scripting (XSS)

Malicious code is injected into a benign or trusted website. A stored XSS attack is malicious code that is permanently stored on a server and a computer is compromised when requesting the stored data. A reflected XSS attack is when a person is tricked into clicking on a malicious link. The injected code travels to the server then reflects the attack back to the victim’s browser. The computer deems the code is from a “trusted” source. Turn off “HTTP TRACE” support on all web servers. Research additional ways to prevent becoming a victim of XSS.

Doxing

Publicly releasing a person’s identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles. Be careful what information you share about yourself, family, and friends (online, in print, and in person).

Elicitation

The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. Be aware of elicitation tactics and the way social engineers try to obtain personal information.

Pharming

Redirecting users from legitimate websites to fraudulent ones for extracting confidential data. (e.g., mimicking bank websites). Watch out for website Uniform Resource Locators (URLs) that use variations in spelling or domain names, or use “.com” instead of “.gov”, for example. Type a website’s address rather than clicking on a link.

Phishing

Usually, an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim. Do not open email or email attachments or click on links sent from people you do not know. If you receive a suspicious email from someone you know, ask him or her about it before opening it.

Example: In March 2011, hackers sent two spear phishing emails to a small group of employees at a security firm, RSA. They only needed one employee to open an infected file and launch the malware. The malware-downloaded information from RSA that then helped the hackers learn how to defeat RSA's security token. In May and June 2011, a number of defense contractors' networks were breached via the compromised RSA token.

Phreaking

Gaining unauthorized access to telecommunication systems. Do not provide secure phone numbers that provide direct access to a Private Branch Exchange or through the Public Branch Exchange to the public phone network.

Scams

Fake deals that trick people into providing money, information, or service in exchange for the deal. If it sounds too good to be true, it is most likely a fraud. Cybercriminals use popular events and news stories as bait for people to open infected email, visit infected websites, or donate money to bogus charities.

Example: Before the 2010 World Cup, cybercriminals offered tickets for sale or sent phishing emails claiming you won tickets to see the event. After the death of Osama Bin Laden, a video claiming to show Bin Laden's capture was posted on Facebook. The video was a fake. When users clicked on the link to the video, they were told to copy a JavaScript code into their browser bar, which automatically sent the hoax to their friends, and gave the hackers full access to their account.

Spoofing

Deceiving computers or computer users by hiding or faking one's identity. Email spoofing utilizes a sham email address or simulates a genuine email address. IP spoofing hides or masks a computer's IP address.

CEMA SECURITY AND PROTECTION

Secure Data and Connectivity

- Physical Security: If you work in a public place often and tend to leave your laptop unattended, invest on a physical laptop lock to anchor your notebook to the desk. It is a simple way to deter thieves. Maintain strict accountability of any mobile device you have and ensure that it has authentication applied to access the device. (Fingerprint, password, passcode, etc.)
- Back Up: Always have a current backup of your important data. Backing up your computer will help you restore things in the event of theft or a hard drive crash. When your laptop is docked back at home or the office, use an external hard drive to back up your documents. However,

ensure that if the disk contains personal or mission related information, that the backup disk is encrypted to minimize risk.

- File Encryption: Encrypting folders and disks. Use approved tools to encrypt an entire hard drive or just a folder full of files. When you encrypt data, you use a secret key to scramble it into an unreadable format, which foils any thieves' attempts to read your private files. To decrypt it, you need a master password. On a Mac, you can create an encrypted disk image by using the Disk Utility application. Macs also come with File Vault (in System Preferences, Security), which encrypts your home folders' contents keeping unwanted eyes out. Windows Vista and the upcoming Windows 7 offer Bit-Locker, a data encryption application.
- Secure Connections: Securing your network traffic via a Secure Shell (SSH) tunnel. Another common technique among the tech elite is the use of a SSH tunnel, or a secure connection to an outside computer (like your home server or office computer) to connect to the internet. From the network you are already on, it looks like you are sending encrypted information to a single destination; in reality, you are using a trusted remote server as a proxy for all your network activity.

Digital Security: Best Practices

- Mobile users should have a healthy paranoia about the possibility of getting their notebook stolen or hacked while they are using a public Wi-Fi network at the airport or coffeehouse. Protect yourself and by placing proper security measures when operating in public areas.
- Turn on your firewall. When you are on an open Wi-Fi network, make sure you have your laptop's firewall on and blocking unwanted incoming connections. In Windows' Control Panel, click on Windows Firewall. On your Mac, in System Preferences, go to Security and click on the Firewall tab to turn it on.
- Password protect your system and do not share folders. When you are at home, sharing a document folder with other computers behind your firewall is a good way to share among your own systems. However, when working on public or other than home networks, your shared folders can create a vulnerability that can cause havoc on your system and compromise your mission, operational, or personal information. Make sure your shared folders are password protected when you are not on a safe network. Even better, turn off all sharing when you are on a public network.
- Use https (secure connections to web sites) whenever possible. When you're checking your webmail like Gmail or Yahoo Mail, or visiting any site with the option, make sure you're using the https:// (instead of http://) connection to encrypt any information you submit there, like your password. Most modern webmail and calendar programs like Gmail and Google Calendar offer an https:// option.
- Do not save your web site passwords in your browser without encrypting them. If you save your web site passwords inside your browser, you save a whole lot of time. However, if a thief, co-worker, or relative uses your computer, you have left your system and information completely unsecured for that person to log into your accounts. Example, it is popular to use mobile applications or applications on PCs and Macs to have a keychain, or a stored database of usernames and passwords. Having all of this sensitive information in one location creates a single point of entry that, if compromised, can pose significant risk to your personal or mission-related information.

Incident Response: What Doctrine Says

Information: Mission related or PII must be handled with extreme caution. Risks can be any one of the following:

- Unauthorized Disclosure of Classified Information (spillage): Higher-level classified information is placed on a lower level classified information sys-tem (i.e., sending an email that contains Secret content on the NIPRNet).
- Loss or Compromise of PII: PII information can uniquely identify, contact, or locate a single person (i.e. posting a personnel roster, which includes names, Social Security Numbers (SSNs), addresses and medical information on a public website). Specific instructions on PII incidents and the reporting processes are on the Records Management and Declassification Agency's website located at: https://www.rmda.belvoir.army.mil
- Receipt of suspicious emails and phishing scams to provide passwords or other sensitive information to an unknown source.

AR 25-2 outlines sanctions that may be imposed for civilian, military and contractor personnel found in violation of Army security practices.

- AR 25-2, paragraph 1-5.j states that military and civilian personnel may be subjected to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring the implementation of DoD and Army policies and procedures.
- AR 25-2 further stipulates that military personnel may face administrative as well as non-judicial or judicial punishments authorized by the Uniform Code of Military Justice (UCMJ). Similarly, sanctions for civilian personnel may include administrative actions as well as judicial punishment. In addition, defense contractors' employees must perform under the terms of the contract and applicable directives, laws, and regulations.

Routine uses of cyberspace, such as sending e-mail, using the Internet, and developing a briefing document, may not be considered a cyber operation but may have an impact on the overall integrity and security of the mission. It is through these routine uses of cyberspace that most of the vulnerabilities on U.S. networks are exposed to and exploited by adversaries. Protecting yourself and your information in the cyber and electromagnetic domains is a personal responsibility. When in doubt, turn off the device, take the battery out, and use secure means of communication to discuss personal and mission related information.

REFERENCES

- Publius Flavius Vegetius Renatus, Epitoma Rei Militaris (Epitome of Military Science)
- Aircraft and Personnel Automated Clearance System (APACS) https://apacs.milcloud.mil/apacs/
- ATM Card skimmers and fraud https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=20279
- AWG Expeditionary Operations Training Curriculum (EOTC) on ATN https://atn.army.mil/dsp_template.aspx?dpID=503
- CIA World Factbook https://www.cia.gov/library/publications/the-world-factbook
- Department of State: http://www.travel.state.gov/
- DoD Foreign Clearance Guide: https://www.fcg.pentagon.mil/
- Global Incident Map: http://globalincidentmap.com
- International Drivers Permit through AAA http://www.aaa.com/vacation/idpf.html
- Jihad Watch: www.jihadwatch.org
- Level I Antiterrorism Awareness Training, Internet resources links https://jkodirect.jten.mil/Content/1718390/1/resources/Antiterrorism_Internet_Links.html
- Native Prospector: https://www.opensource.gov
- Patronus Analytical Homepage: Provides aid worker fatalities, provides NGO security resources, etc.: http://patronusanalytical.net/
- Smart Traveler Enrollment Program" (STEP): https://step.state.gov/step/
- Small Wars Journal: http://smallwarsjournal.com/
- Trip Advisor: www.tripadvsior.com
- Wiki Maps: www.wikimapia.org
- TRADOC G2 Handbook No. 1.01, Terror Operations: Case Studies in Terrorism
- FBI/USDOJ: Study of Active Shooter Incidents in the United States between 2000 and 2013
- DHS Active Shooter: How to Respond: www.dhs.gov
- AWG TPR: Capture Avoidance/Personnel Recovery Plan
- LTC Dave Grossman, On Killing
- http://www.bsr-inc.com/training-courses/becon/
- OSAC photo: http://globalhealth.ucdavis.edu/local_resources/pdfs/OSAC-Quick-Guide-on-Best-Practices-while-Traveling-with-Mobile-Devices.pdf
- JP 1-02
- AR 25-2
- FM 3-50
- Photos: Courtesy of Asymmetric Warfare Group (AWG)

ASYMMETRIC WARFARE GROUP
2270 ROCK AVENUE
FORT MEADE, MD 20755

THINK. ADAPT. ANTICIPATE.

www.awg.army.mil