



ÆGIS journal

Addressing threats that affect your bottom line

Volume 11 Number 3, March 2008

From the case files of

LUBRINCO

<http://www.lubrinco.com/>

1-212-695-1759

and



<http://www.feeinc.com/>

1-480-838-1728

Due diligence outside North America and Western Europe? Call us!

This month's features:

- 1. Asset Location and Due Diligence — More unintended consequences**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Demystifying OPSEC assessments: A “how to” primer**
- 3. Executive Protection — Concealed carry**
- 4. Technical Issues — Decryption through memory theft**
- 5. Real Stories from the Field — Interpreting the news**
- 6. Book and Product Reviews — How Doctors Think**
- 7. Subscription/Unsubscription/Copyright Information**

1. Asset Location and Due Diligence — More unintended consequences

In the January issue article ~~*Guns or butter*~~ *Gasoline or eggs* we discussed the fact that the current enthusiasm for ethanol from low biomass sources like corn (the Brazilians use higher mass sugar cane) had unintended consequences. More information has become available, and we thought it should be shared, as it points up the importance of always asking the following five questions before implementing any policy or measure:

1. What problem is the policy or measure trying to solve?
2. How can it fail in practice?
3. Given the failure modes, how well does it solve the problem?
4. What are the costs, both financial and social, associated with it, and flowing from its unintended consequences?
5. Given the effectiveness and costs, is the policy or measure worth it?

The problem we are trying to solve is dependence on expensive foreign oil, which is a significant problem, both long and short term. A secondary problem (assuming you have no children and don't care about the *déluge* if it comes *après vous*) is the reduction of greenhouse gases, which were estimated to be in the neighborhood of 20 percent with increased use of ethanol. An article in last month's Science magazine entitled *Use of U.S. Croplands for Biofuels Increases Greenhouse Gases Through Emissions from Land-Use Change* (you can read the abstract at <http://www.sciencemag.org/cgi/content/abstract/319/5867/1238?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&fulltext=ethanol&searchid=1&FIRSTINDEX=0&issue=5867&resourcetype=HWCIT> if you don't get it at home) noted that "corn-based ethanol, instead of producing a 20% savings, nearly doubles greenhouse emissions over 30 years and increases greenhouse gases for 167 years." We don't claim to be mathematicians, but it seems to us that this looks like the numbers are going in the wrong direction....

To add to the mix, the *Organization for Economic Cooperation and Development's* paper *Agricultural market impacts of future growth in the production of biofuels* of 1 February 2008 (<http://www.oecd.org/dataoecd/58/62/36074135.pdf>) estimates that to meet a target of 10% biofuel use 30% of farmland needs to be devoted to growing the biomass. We have additionally read estimates that to meet a 15% target we need to use the entire U.S. corn crop, which represents about 40% of the world's corn.

The diversion of food to fuel has already had a significant effect on the world's poor, and has certainly been noticeable in American food budgets. You can safely expect food prices to continue to escalate.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Demystifying OPSEC assessments: A “how to” primer.

While we, in this journal, deal with OPSEC in the commercial environment, it is always instructive to see how OPSEC is approached in the military environment, where it was developed and where it is widely used.

Contributed by LCDR Daryl Haegley, Navy OPSEC Support Team OIC and NETWARCOM's Force OPSEC Program Manager located at Navy Information Operations Command-Norfolk. Winner of National OPSEC Individual Achievement Award and DOD CIO Award, he is an OPSEC Certified Professional (OCP). (lclohan@email.msn.com). Contributed articles do not necessarily reflect the viewpoint of AEGIS.

OPSEC Assessments Purpose: Determine susceptibility to adversary exploitation

OPSEC is commonly defined as the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning operations or other activities (“Loose Lips Sink Ships”). Integral to the OPSEC process is the requirement to conduct regular OPSEC Assessments. The Department of Defense Directive (DoDD) 5205.02, Operations Security, dated 06 March 2006, defines an OPSEC Assessment as “An evaluative process, usually conducted annually, of an operation, activity, exercise, or support function to determine the likelihood that critical information can be protected from the adversary’s intelligence.” Additionally, Joint Pub 3-13.3, Operations Security, dated 29 June 2006, describes an OPSEC assessment as “an intensive application of the OPSEC process to an existing operation or activity by a multi-disciplined team of experts. Assessments are essential for identifying requirements for additional OPSEC measures and for making necessary changes in existing OPSEC measures.”

Assessments are conducted only after an organization has identified its Critical Information (CI). Critical information is defined as “Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequence for friendly mission accomplishment (Joint Pub 1-02). CI is often referred to a subset of Essential Elements of Friendly Information (EEFI). For example, an EEFI would be “When will the special

operation commence?” and the corresponding CI would be “Saturday, January 6th, 0600.” The identification of CI is important in that it focuses the OPSEC Assessment on evaluating protection of vital information rather than attempting to protect all classified or sensitive information. The list below serves as a good reference to generate a CI list for your organization:

- Unit capabilities or degradation
- Details of plans, operations, orders, or programs
- Reference of mission associated information, such as personnel/equipment deployment dates or locations
- Specific tad/tdy deployment data, including personnel numbers, duration, location, systems, etc.
- Specific details concerning tad/tdy travel itineraries and purposes of travel by key personnel
- Association of abbreviations, acronyms, nicknames, or codewords with projects or locations
- New, projected, or expanded secure communications capabilities

OPSEC assessments are different from security evaluations or inspections in that an assessment attempts to reproduce an adversary’s view of the operation or activity being assessed. Independently, a security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations. Essentially, OPSEC assessments enable an evaluation of current OPSEC measure effectiveness.

Although OPSEC Assessment findings are not provided to the assessed unit’s higher headquarters, Commanders or OPSEC assessment teams may forward to senior officials generic lessons-learned on a non-attribution basis. Lessons-learned from assessments should be shared with command personnel in order to advance the command’s OPSEC posture and mission effectiveness. Further, leaders and decision makers are shown the resources required to adequately protect against adversary exploitation. Findings should be labeled and handled at appropriate classification level (SECRET or CONFIDENTIAL) depending upon vulnerability results. See your Information Security Manager for guidance. COMFLTFORCOM states in 042111Z Jun 04 message that, “Leaders must pursue every effort to ensure that highest OPSEC measures are followed and OPSEC integrity is maintained. Make OPSEC a priority with daily emphasis from senior command personnel to the newest recruit and observe strict adherence to OPSEC in all transactions and/or communication lines to ensure classified or otherwise sensitive information is not inadvertently disclosed.”

OPSEC Assessment bottom line: OPSEC is emphasized, security is improved, threat awareness raised and mission success rate increased.

Recommended assessment procedures

The steps listed below provide the basic and logical steps to conduct an OPSEC Assessment and have been used at many Department of Defense (DoD) shore based Navy ships and forward deployed organizations world wide with consistent, positive results. It is highly recommended that all the steps be read first to gain insight to the entire assessment process prior to its execution. For example, if communications security (COMSEC) monitoring is going to be part of the assessment, scheduling may take several months. Although no specific or unique training is required to administer and conduct an OPSEC assessment, it is assumed that the organization’s OPSEC Officer and working group members have completed basic OPSEC education and understand OPSEC fundamentals. If training is required, OPSEC training sources (formal and CBT) are referenced at the very end of this document. Complete each step in the order listed below:

1. Complete the “Rate Your OPSEC” survey below to determine the status of your organization’s OPSEC program. Upon completion, proceed to step 2.

Rate Your OPSEC		YES	NO	Progressing
Instructions:				
Assess your command's OPSEC posture by completing the following questions. Insert 10 for a "Yes" response, 0 for a "No" response and 1-9 in "Progressing" (depending on the degree you feel your command is at in regards to that question.)				
1. Does your command have an OPSEC Officer in writing?				
2. Has the OPSEC Officer received formal OPSEC training or completed the OPSEC 1301 CBT?				
3. Does your command have				

an OPSEC instruction?			
4. Has your command conducted an annual OPSEC assessment?			
5. Does your command have an OPSEC working group?			
6. Is your command's Critical Information available to all personnel for awareness?			
7. Does the command have a shred or paper destruction Policy?			
8. Does the command provide OPSEC training during command indoctrination?			
9. As a minimum, does the command provide yearly OPSEC GMT?			
10. Does your command utilize OPSEC awareness products? (I.E. Posters, signs, etc.)			

Total score = **0**

Upon score calculation, determine whether your program is satisfactory or requires improvement. Scores greater than 85 represent OPSEC programs that require minor adjustments. Scores less than 85 require greater emphasis and concerns should be addressed immediately.

- In the event you answered “No” to the Rate your OPSEC survey questions: (1), (2), (3), (5), or (6), then corrective action needs to be taken prior to conducting an assessment. When the survey answers are “Yes” or found to be satisfactory, proceed to step 3.

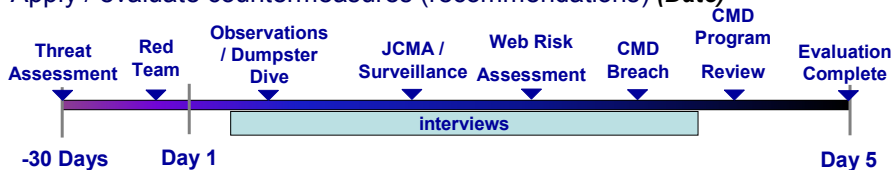
3. Assemble your Working Group to determine an appropriate execution timeline for this assessment. To optimize the effectiveness of an OPSEC program or assessment, a comprehensive understanding of relevant processes, activities, business practices, and applicable critical information is required. This is most easily obtained through a working group whose representatives (at least one) are derived from each division, department, directorate, etc. For example, Operations, Communications, Logistics, Intelligence, Administration, Public Affairs, etc. each should include a participating team member. Another benefit is that the working group will consist of subject matter experts with intimate knowledge of routines, inter-workings, and potential vulnerabilities. If involved with Information Operations (IO) missions or planning, including Psychological Operations (PYSOP) and Military Deception (MILDEC) representatives will improve the OPSEC working group's impact to mission success. If not already completed, the working group will generate the Critical Information list. It is recommended the events proceed in the following order to include, but not restricted to: (details of each broken out farther below)

- A. In Brief
- B. Threat brief
- C. Red Team activities
- D. Observations, space walk-throughs and dumpster dives
- E. Conduct OPSEC interviews
- F. COMSEC Monitoring
- G. Web Risk Assessment (WRA)
- H. Physical and electronic integrity breach
- J. Command program review
- K. Assessment wrap-up; Plan of Action & Milestones (POA&M)

Below is a generic timeline depicting the general sequence of events:

Timeline

- Verify CI / EEFI (**Date**)
- Obtain threat assessment: NCIS (**Date**)
 - Foreign intelligence service collectors, terrorists, criminals
- Identify Vulnerabilities / Conduct assessment (**Date**)
 - Evaluate command emphasis, awareness, training; conduct interviews
 - Emulate threat: Open source discovery, dumpster dives [*test physical security, observe routines, monitor comms & network – not performed*]
- Assess risk of vulnerability findings (**Date**)
- Apply / evaluate countermeasures (recommendations) (**Date**)



Sample five-day assessment daily POA&M:

Monday (Day Month Year)

- | | |
|-------------|--|
| 0900 | Team leaders muster |
| 0930 – 1415 | Surveillance of building(s); Dumpster dives; Working Group members walk through assigned spaces with checklist |
| 1430 | Team leaders muster for debrief |

3. Tuesday (Day Month Year)

- | | |
|-------------|--|
| 0900 | Team leaders muster |
| 0930 – 1415 | Surveillance / intrusion of building(s); Conduct interviews / space walk through |
| 1430 | Team leaders muster for debrief |

4. Wednesday (Day Month Year)

- | | |
|-------------|--|
| 0900 | Team leaders muster |
| 0930 – 1415 | Intrusion of buildings; Dumpster dives; Policy review; Conduct interviews / space walk through (cont.) |

1430 Team leaders muster for debrief

5. Thursday (Day Month Year)

0900 Team leaders muster

0930 – 1415 Intrusion team compile findings for out brief; Policy review (cont.) / compile findings for out brief Conduct interviews / space walk through (cont.)

1430 Team leaders muster for debrief

6. Friday (Day Month Year)

0900 Team leaders muster

0930 – 1215 Conduct interviews / space walk through (cont.) / compile findings for out brief
Dumpster dives / compile findings for out brief

1300 Final Out Brief (all WG members)

A. Threat brief

Commander, NETWARCOM recently commented on the persistence of adversarial intent and capability: “The threat vector is 360 degrees, the enemy is ever vigilant probing and collecting 24/7, and our information is constantly at risk, at work and at home. You must be at GQ round the clock.” In order to understand what threats are relevant to your organization, obtain a local threat briefing from the organization’s intelligence representative or Service investigative branch agent (i.e. Navy would contact the Naval Criminal Investigative Service [NCIS]). The presentation will provide actual adversarial intentions and capabilities that need to be emulated in support of the assessment. This brief should be presented prior to the execution phase of the assessment, as it will raise the level of awareness of all personnel. Without this brief, an assessment may focus on erroneous adversary capabilities and portray irrelevant vulnerabilities.

B. Red Team activities

A group of individuals with proper authorities will replicate adversary capabilities as outlined in the Threat Brief. By simulating malevolent intent via a wide spectrum of institutional or ad hoc methodologies, potential vulnerabilities are usually uncovered. From network penetration to dumpster

dives and from attempts to gain building access without proper identification to monitoring conversations at local areas of personnel congregation, the Red Team demonstrates the adversary's view. After weaknesses are identified, specific mitigation strategies are developed to prevent exploitation. Before the assessment begins, Red Team members and activities will be identified and approved via a document (otherwise known as a "Get out of Jail free Card") by the organization's Commander, OPSEC and Security Officers.

C. Observations, space walk-throughs and dumpster dives

These functions can be conducted by working group members or the Red Team. Through observations, one can identify potential vulnerabilities via visible indicators, predictable patterns, entrance procedures, poor security practices, etc. Dumpster-dives reveal the organization's policy on discarding documentation, classified and unclassified. Team members will explore discarded contents in workspace and outside containers for disclosures of the organization's critical information (operation or exercise). Even though an organization may not "own" the dumpster at the end of the pier, it is imperative to identify what an adversary will have access. Immediately inform the information security officer / manager once classified information is discovered. Policy changes are typically recommended upon assessment observation and dumpster dive findings. Use the following list to conduct a space walkthrough. Comment on any poor security practices noticed during walk-through not listed below:

Office/Space checked: _____ Date checked: _____

_____ CI Cue Card (Yellow Card) posted near phone/computer?

_____ Posters Posted

_____ Phone stickers on phones and legible

_____ Shredders available and operable

_____ Burnbags available

_____ Personal information in the open/posted

_____ Unoccupied computers logged on

_____ Computer passwords written in open

_____ Computer screens facing windows

_____ Safes locked when not in use

_____ Cell phones in spaces

Use the following checklist for trash searches:

Trash / Recycle Receptacles or Dumpster location _____ Date / time checked: _____

____ Privacy Act information, to include but not limited to SSN, addresses, phone numbers, and family information

____ POD / POW

____ Documents related to command, mission and critical information

____ Supply requests and / or equipment inventories

____ Discarded / unopened mail, whether personal or command specific

____ Itineraries / VIP schedules

____ Joint/ Navy doctrine, publications and instructions

D. Conduct OPSEC interviews

OPSEC interviews provide a non-attributable means of acquiring insight to potential vulnerabilities that organizational personnel may be aware of, yet tend not to disclose during the course of everyday activities. The names of the interviewees are NOT disclosed to facilitate non-attribution. Questions are developed by the OPSEC working group to gain insight to OPSEC awareness and practices. Often the questions reflect the chief concerns of the Commander. Responses are collated and integrated into the out brief. It is recommended that working group members pair-up and interview organizational personnel, preferably not from the interviewer's division, department, etc. Interviewers from different areas of the organization tend to make those interviewed more comfortable and able to provide honest answers, not the answers they think the organization wants to hear.

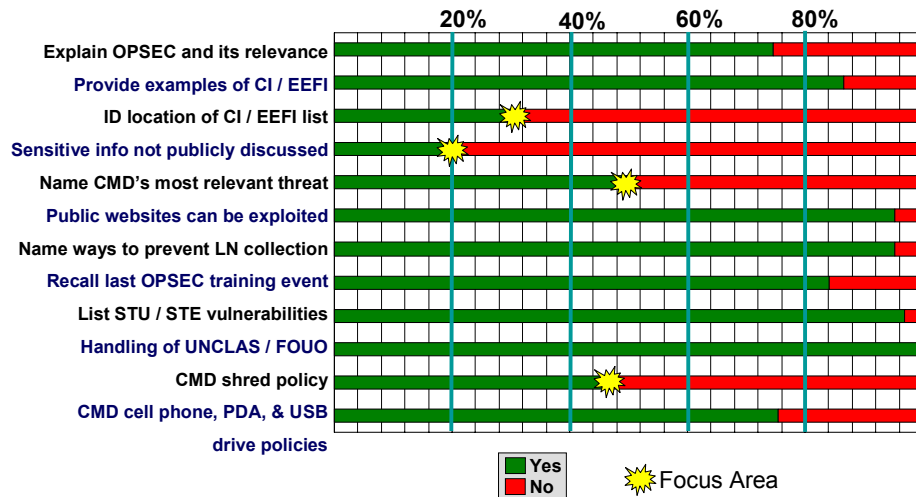
Optimally, one-person interviews an individual while another records the response. However, other interview options may be used to attain the required insight to the OPSEC posture. For example, one can interview small groups of similar ranking personnel, similar division personnel, etc. Sample interview questions

Regarding the number of interviews required: depending upon the organization's size, number of interviewers and time allotted, the working group will propose – the commander decides – on a “representative sample” percentage. As with any survey / polling data, the smaller the sample size, the less accurate the results. Ten (10) percent is usually too small and one hundred (100) percent is often too difficult. If each working group member interviews seventy (70) percent of each division, then a representative

sample is readily achieved. As personnel are the key to protecting an organization’s critical information, OPSEC interviews are fundamental in understanding their ability to prevent its exploitation.

Metrics from interviews are focus-area indicators. Keep the number of questions to ten or twelve. Ask open-ended questions, but grade them as “yes” or “no.” Therefore, data from hundreds of interviews can be simply captured in spreadsheet form. For example, ask, “Explain what OPSEC is and why it is important.” Correct responses will be marked “yes” and incorrect responses marked “no,” as the following slide depicts:

Combined Total (126)



E. COMSEC Monitoring

Unfortunately, personnel commonly discuss an organization’s critical information via un-secure government communications (phones, e-mail, etc.). Army General McKiernan stated in August 2006 that, “Even when the user turns it off, a wireless device can be remotely turned on to eavesdrop and retransmit conversations, typically within 20 feet of the device. Because there are no external indications of active use, the user will not know that the device has been turned on.” If requested, your organization can request and authorize the Joint COMSEC Monitoring Activity (JCMA) monitor government communications for references of the organization’s critical information (working group provides target information to JCMA). Prior to communications monitoring, it is imperative that personnel are provided notice of proposed monitoring (attain Legal Council approval). Results are

typically compiled daily and provided to a single designated individual (i.e. OPSEC Officer). Findings identify whether or not personnel divulge critical information via un-secure communications modes and are non-attributable as the offender's name is not identified, only the revealing disclosure content.

F. Web Risk Assessment (WRA)

An Al Qaeda training manual recovered in Afghanistan states, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy." Justifiably, information posted on an organization's publicly accessible website must be regularly reviewed to ensure it is free of critical information and or information that provide adversarial advantage. Additionally, web site material will be analyzed for accumulation of seemingly unrelated topics that when aggregated, disclose information useful to adversaries. SECDEF promoted in an Information Security/Website Alert on August 2006, "All personnel have the responsibility to ensure that no information that might place our service members in jeopardy or that would be of use to our adversaries is posted to websites that are readily accessible by the public."

During an assessment, a working group or Red Team member will review the organization's web page for Critical Information as well as ensure compliance with DoD regulations and instructions. The Navy Information Operations Command Norfolk maintains a cadre of Web Risk Assessment experts and a website (<https://www.nioc-norfolk@navy.mil/operations/wra/wra.shtml>) filled with resources (checklists, references, etc.) promoting effective WRA. Findings must be discussed with the Public Affairs Officer.

G. Physical and electronic integrity breach

If applicable, approved and pre-coordinated, Red Team personnel will attempt to compromise building integrity through attempts to bypass or circumvent physical and / or electronic security measures. The Red Team should never cause physical damage to any property or person while conducting their duties as a simulated aggressor. It is, however, acceptable to leave a mark, i.e. Red Team sticker, to illustrate the fact that vulnerability was identified and the potential of compromise or disclosure was probable. Before the assessment begins, Red Team members and activities will be identified and listed on a limited distributed document (Get out of Jail free Card). The following checklist serves as a good reference:

_____ Badges properly checked at Entrance / Quarterdeck

- _____ Badges openly worn outside
 - _____ CO/XO or VIP arrival/departures repetitive
 - _____ Building doors secure during / after hours
 - _____ Outside exit only doors secured
 - _____ Cipher locks easily bypassed
 - _____ Piggybacking occurs (someone holds door, others enter without swiping badge)
 - _____ Shoulder Surfing opportunities exist (ease of observing other's PC screens)
- Date of intrusion attempt: _____ Building: _____ Areas observed / Areas breeched: _____

H. Command program review

During this portion of the assessment, a designated team member from the working group should review all applicable documentation and procedures related to the organization's OPSEC program. For example, has the OPSEC Officer and working group members obtained current letters of designation? Has training been conducted and documented? Have instructions and standard operating procedures (SOPs) been updated? Use the checklist below to gauge the adequacy of your program:

- _____ OPSEC Officer designated via appointment letter
- _____ Critical Information List (CIL) developed, relevant and posted near PCs, phones, copiers, faxes, shredders, etc.
- _____ Assessment results from previous year (formal and/or informal)
- _____ Command OPSEC instruction, policy, or plan on file
- _____ Personal Electronic Device (PED) policy
- _____ Shred policy

I. Assessment wrap-up; Plan of Action & Milestones (POA&M)

When all assessment activities are complete and data compiled for summarization, it is recommended that a Power Point brief be built for the Commander's out brief. The out brief should include key findings and recommendations for corrective action with specific remediation milestones and designated action officers. This brief should serve as a POA&M

template for the working group to identify and track all deficiencies and prepare them for the six-month follow-up report.

4. Based on the above, present Commanding Officer with an In-Brief prior to the assessment and obtain approval to proceed. Proceed to step 5.
5. Request COMSEC monitoring support if required / needed. Due to many requests for this limited resource service, scheduling must be done months in advance. If this resource is not available, continue with the assessment but make a note of it during the Out-brief. Proceed to step 6.
6. Contact command Intelligence department, (i.e. N2, G2, S2, J2 etc.) or Service investigative branch (i.e. NCIS, OSI, CID, etc.) for a threat brief / analysis of local threat intent and capabilities. Proceed to step 7.
7. Assign team leads for designated portions of the assessment (i.e. Dumpster dive, Interviews, Observations, etc.). Proceed to step 8.
8. Begin assessment in accordance with your POA&M. After each assessment activity has been executed, proceed to step 9.
9. Upon completion of the execution phase, and all information has been gathered, it is recommended the working group begin compiling a comprehensive report to present findings to the Commander. It is recommended a short Power Point brief reflecting these findings and recommendations for corrective action are presented to the Commander.

SECDEF's DODDIR 5205.02 directs, "As an operations activity, OPSEC will be considered during the entire lifecycle of military operations or activities" and "Ensure adequate practices are in place to prevent adversaries from taking advantage of and aggregating publicly available information...and other detectable activities to derive indicators of U.S. intentions, capabilities operations and activities." Conducting OPSEC assessment via the steps outlined above ensures SECDEF requirement fulfillment.

3. Executive Protection — Concealed carry

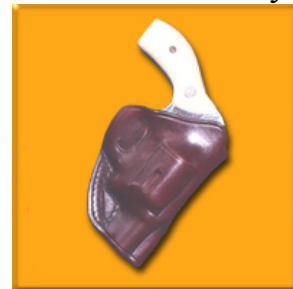
We are not folks who habitually carry guns either personally or professionally. On the other hand, there are times when we need to carry guns, and to have them concealed. Ease of concealed carry depends on four factors: The clothing you are wearing, your size, the size of the guns you are carrying, and your choice of holsters.

If you are wearing baggy clothing, such as you often see in high school students, you can carry weapons with relative ease (<http://www.youtube.com/watch?v=8bMz0m6XHXs>). In our case, we generally are wearing suits or jackets and slacks, so we don't have quite as many options. To make matters worse, while one of us is relatively large of stature (over six feet), the one most likely to be carrying is almost half a foot shorter. Which leaves us with choice of gun and holster as the factors that can be controlled.

Semi-automatic weapons tend to be thinner, and somewhat more easily concealed than revolvers. Unfortunately, this editor has had some unfortunate experiences with semi-automatic weapons, and is therefore more comfortable with (and therefore carries) revolvers. By the same token, larger caliber weapons tend to be somewhat bulkier, and this editor favors (a subject worthy of a separate article) cartridges with large slow bullets, and has ended up choosing a short-barreled .45acp Smith & Wesson 625-2 revolver. This is an N-frame revolver, and, even with a short barrel, a BIG gun. The ability to conceal this weapon in this set of circumstance depends on the holster.

In theory, the ideal choice would be an inside-the-pants holster. Unfortunately, in order for an inside-the-pants holster to be workable in practice, you have to have something more than single-digit body fat, otherwise the gun against bone soon becomes excruciating. Which for this editor means a belt holster worn outside the trousers.

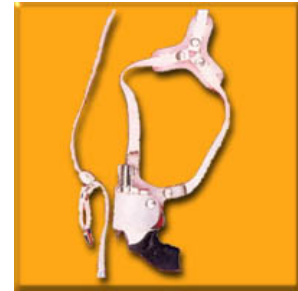
There are many of these available, but the best we have found are made by Ken Null (<http://www.knullholsters.com/>) in Resaca, Georgia. We prefer his holster in shell horsehide. Our holster of choice is his model RSS, which carries at the perfect angle to draw, and yet is extremely difficult for anyone else to take from the holster. We are able to carry a very large gun with nobody being aware of its presence. At \$125, it is not the cheapest holster around, but we consider it to be the best for our circumstances.



A crucial adjunct to a belt holster is the belt. We have been using Null belts for decades. Indeed, we just replaced one of our belts, which, after roughly twenty years of use was starting to show enough wear that we felt it warranted being replaced. Again, we prefer his belts in shell horsehide. They come either cordovan

with a brass buckle (\$135) or black with a silver buckle (\$225). The standard model CBT combat belt is 1.5” and locks the holster firmly to your body. The CBT is handsome enough to be worn with your best suit with nobody being aware you are wearing a gun belt – thus explaining Null’s motto of “unseen ... in the best places” – and will last you literally decades.

Null, one of the most innovative bespoke holster makers, has a number of very interesting holsters. One of our personal favorites is his SMZ shoulder holster. Many shoulder holsters hold the weapon with the barrel pointing down or, worse, facing back. When you draw the weapon it passes by your arm and everyone behind and to the side of you, which is a safety no-no. The



SMZ holds the gun with the barrel facing up and the butt under your armpit. To draw the weapon you simply reach under your jacket, grab the grip in a perfectly normal manner, and bring it straight forward. It is a fast draw, and an extremely comfortable holster that can be worn all day. While intended for small frame revolvers – it is perfect in combination with a S&W Centennial, which is an ideal small carry revolver – we had one made for our N-frame, and it has worked well for us over the years.

An alternative for the j-frame revolver is Null’s model SKR, which was designed based on feedback from the SMZ, and which encloses the gun more completely.



If your life depends on concealed carry, we would strongly recommend Ken Null holsters to you.

4. Technical Issues — Decryption through memory theft

Of late we have seen a number of articles on a new way to get decryption keys, in this case, by pulling out the DRAM and reading it. You can see this demonstrated at <http://citp.princeton.edu/memory/>.

This is another threat that isn’t keeping us awake at night. For a start, while all our data is encrypted using Private Disk (see the November 2006 issue of *ÆGIS*), the keys are only in memory when the disk is mounted. When we leave the office, we dismount the virtual drive, and the keys disappear. I believe that the developers actually wrote the program.

But let us say that they didn’t do this. We are still not worried. In order for someone to get to the DRAM several things have to happen. First, the machine has to be unattended. Second, it has to have the keys still in

DRAM, where it only stays for something between a few seconds and a few minutes. Putting aside all the other issues, if you shut down a machine and stay with it for two or three minutes, it is unlikely that this will be a problem for you in any real term.

We cannot, however, say the same for a key logger. If someone is able to plant a key logger (or key logger software) on your machine, then they will not only have the encryption keys, but also actual data that is entered. This seems to us to be a more realistic concern to us if someone can get access to a machine.

5. Real Stories from the Field — Interpreting the news

Recently we had to go to Nevis, and discovered that American Airlines had cancelled the flight because of what appeared to be a crash and fire on the runway. So we flew to St. Kitts and took the ferry.

Sometime later we drove past the airport, and noticed that planes were arriving and departing, and that there appeared to be no wreckage. When we asked, we discovered that the large fire truck had broken down and was waiting for a part, and that American was uncomfortable with the capacity of the smaller fire truck in case of a crash, and had therefore cancelled their flights until the big truck was repaired. Other airlines, flying smaller planes, had no such concerns, and were still flying.

The lesson here is twofold. The first lesson is that it is good to have alternative plans in place before you need to get in our out of a country, and for dealing with emergencies.

The second lesson is that what you read may not always explain what is happening. We saw this recently when the sister of a friend asked her fruit vendor, who was from Kandahar, how things were in his country. He said that there was not really much of a country left, as the Americans had blown up everything built since the Soviets had blown everything up. She then asked how they were dealing with the bad guys from al Qaeda, and he replied with some puzzlement that the people from al Qaeda were the ones giving them food and medical supplies, and visiting their children in the hospital. If this sounds familiar, it is because it replicates the experience of Hamas being a primary source of social services in Palestine, and winning the election. This chicken-in-the-pot approach is a factor that should be considered in understanding the effect of foreign policy, and yet is often is not thought through or taken into account.

6. Book and Product Reviews

How Doctors Think

Jerome Groopman, MD

Publisher ISBN-13: 9780618610037 336 pages \$15.95

<http://www.houghtonmifflinbooks.com/mariner>

When we were in graduate school, we took a class with a clinical psychologist who spent a lot of time discussing cases in which he had been brought in to do second-opinion psychological evaluations. In every case he found an underlying physical cause for the mis-labeled psychological diagnosis, and was able to help the victim, er, patient, be healed. His message to us was firstly that we should look for a medical cause before accepting a psychological diagnosis, and secondly that when someone got sick, it was important to do our homework in helping the doctor reach an appropriate diagnosis and treatment.

There is some question as to exactly how many people die each year due to unfortunate medical factors, but we recall having read that it approached 210,000. By medical factors we mean either medical mistakes (looking at the x-ray backward or prescribing the wrong dose of a prescription medicine) or incorrect diagnosis (which accounts for about 80 percent of the cases in question), or avoidable drug interactions (which account for a significant percentage of hospitalizations). Jerome Groopman's book, *How Doctors Think*, is designed to help patients help their doctors come to the right diagnosis.

The book begins with a puzzling case of a woman who had been wasting away for the fifteen years of her treatment. While any careful reader of *ÆGIS* would have made a correct diagnosis on page two of the book (And no, we are not cunning diagnosticians: We happened to discuss it briefly in the March issue, and know about it only because we have a friend who suffers from it) it took the patient fifteen years to find a doctor who would make the correct diagnosis, on page fifteen, of celiac disease.

Groopman goes through the causes of misdiagnosis, and comes up with practical you (or those acting on your behalf) can ask to help your doctor come up with the right diagnosis. To try and jog an ER physician – or any physician – into thinking widely about your problem, you can ask “What is the worst thing this can be?” This can be helpful if the doctor doesn't like you (doctors sometimes don't like sick people they can't easily diagnose, noncompliant people, or people whom they don't like for mysterious reasons), or is fixated on a particular diagnosis. Another question is “What

body parts are near where I am having my symptoms?” Also, asking “Is there anything that doesn’t fit?” might get the doctor to think about anomalous data which might be a clue rather than a mere outlier.

Another reasonable question is “What else could it be?” And if you have a fear or suspicion that you have been afraid to mention, it is a good idea to bring this up as a possibility to be looked at. An equally valid question would be “Is it possible that I have more than one problem?”

He writes that “Patients can help the doctor think by asking questions. If he mentions a possible complication from surgery, they can ask how often it happens. If he talks about pain and lingering discomfort from a procedure, they can ask how the pain compares with having a tooth pulled under Novocain, or some other unpleasant event. If he recommends a procedure, patients can ask why, what might be found, with what probability, and, importantly, how much difference it will make to find it.”

You should also ask whether a treatment is standard, or whether different specialists recommend different approaches, and why. And how time-tested a new treatment is.

Another significant issue was understanding prognosis. In one case an oncologist told a patient that there was a thirty percent reduction in mortality with chemotherapy. The numbers, however, indicated that this meant that in five years while ten out of a hundred who did not take chemotherapy would die, with chemo seven – thirty percent fewer – would die. While a thirty percent reduction might get us into chemotherapy, seven out of a hundred versus ten out of a hundred would induce *us* not to take chemotherapy, with its attendant loss of quality of life.

When we look at a book we tend to dog-ear it so we can pull up appropriate quotes. In this book we had 23 pages marked. Since we obviously cannot discuss here all the pieces we thought significant, we urge you to get a copy and read it several times. It is quite likely that doing so will keep you, or someone you care for, alive or less hurt.

Because *How Doctors Think* the critical issue of health care, and is something every reader will have to deal with at some point in time, we have added it to our list of must-read books. Past must-read books are, in alphabetical order:

- *All You Need Is Love, and Other Lies about Marriage* by John W. Jacobs, M.D (<http://www.lubrinco.com/ejournal/ej200504.pdf>)

- *Better* by Atul Gawande, M.D.
(<http://www.lubrinco.com/ejournal/ej200708.pdf>)
- *Beyond Fear* by Bruce Schneier
(<http://www.lubrinco.com/ejournal/ej200309.pdf>)
- *Corporocracy* by Robert A. G. Monks
(<http://www.lubrinco.com/ejournal/ej200802.pdf>)
- *The End of America*, by Naomi Wolf
(<http://www.lubrinco.com/ejournal/ej2000711.pdf>)
- *Inside the Tornado* by Geoffrey A. Moore
(<http://www.lubrinco.com/ejournal/ej200211.pdf>)
- *Rediscover Your Native Fitness (PACE)*, by Al Sears, M.D.
(<http://www.lubrinco.com/ejournal/ej2000711.pdf>)
- *Reinventing the CFO* by Jeremy Hope
(<http://www.lubrinco.com/ejournal/ej200708.pdf>)
- *Taking Sex Differences Seriously* by Steven E. Rhoads
(<http://www.lubrinco.com/ejournal/ej200411.pdf>)
- *What Clients Love* by Harry Beckwith
(<http://www.lubrinco.com/ejournal/ej200508.pdf>)
- *With Winning in Mind* by Lanny Bassham
(<http://www.lubrinco.com/ejournal/ej200509.pdf>)

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2008 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.com).

LUBRINCO provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

- **Identification, valuation, and protection of intellectual assets and critical information.**
 - American businesses lose \$300 billion in revenues annually to competitive intelligence, economic espionage, inappropriate disclosure, and information theft.
 - LUBRINCO provides private sector consulting access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information.

- Implementing an OPSEC program is likely to increase revenues for an at-risk operating group by \$75 million.
- **International asset location and due diligence.**
 - Location of concealed assets in fraud, theft, and divorce.
 - Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, and the Caribbean.
 - Financial fraud, anti-money laundering, and anti-corruption program development and training.
- **Protection of management, staff, and families.**
 - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
 - When traveling and living overseas.
 - When transporting items of substantial value.

LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

For information on **LUBRINCO** and its services, or for the archive of all past issues of **ÆGIS** in PDF format, please go to <http://www.aegisjournal.com/>.

Subscription to **ÆGIS** is available for \$15 per year in North America and \$20 per year outside of North America.

To sign up for a **complimentary subscription** to **ÆGIS** or the **ÆGIS** PDF notification list, send an email to subscribe@aegisjournal.com.

To subscribe to our AvantGo channel, go to http://avantgo.com/channels/_add_channel.pl?cha_id=1773

To be removed from the subscription list, send an e-mail to unsubscribe@aegisjournal.com.

If you know of anyone else who should be receiving **ÆGIS**, please send their e-mail address to subscribe@aegisjournal.com.

If there is a topic that you would like to know more about, send it to editor@aegisjournal.com and the editors will consider it as the topic for an article in an upcoming issue.

If you would like to submit an article for publication in **ÆGIS**, send it as an attachment to an e-mail to editor@aegisjournal.com. Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in **ÆGIS** constitutes a license to **LUBRINCO**, and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of **ÆGIS**, you may do so freely as long as appropriate source, copyright, accreditation, and link to the **ÆGIS** Web site is included. This should be in the form

Article Title, from the March 2008 **ÆGIS** (© 2008 **LUBRINCO** and FE&E), to be found at <http://www.aegisjournal.com/>.

ÆGIS is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in **ÆGIS** should be construed as legal advice. The information provided is "general information," not "specific advice."

The solution to any problem is highly dependent upon the precise facts involved. Thus, before making any reliance upon anything said here, you should consult with an appropriately skilled professional. Opinions expressed by contributors are not necessarily endorsed by the publisher, and may be presented to encourage a dialogue among subscribers. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in **ÆGIS**.

Please be safe, and be smart.