SITUATIONAL AWARENESS

"Fortune favors a prepared mind." (Louis Pasteur)

Situational awareness reflects the "human dimension" of homeland security which is a subset of the "human factors" approach which aims to apply the social and behavioral sciences to the early detection, analysis, and understanding of terrorist intent. Situational awareness can be done by people alone, while the human factors approach often requires the integration of technology, like biometrics or screening devices. In any intelligence, surveillance, or reconnaissance context, people and their perceptions of reality are your best sensors, and unbeatable if combined with corroborative evidence from mechanical sensor devices. Ordinary people often see or witness things which turn out to contain valuable information or little "snippets" that help "connect the dots." One of today's most daunting challenges is to create informational systems with "humans-in-the-loop" (Endsley 1995) so that thinking agents can detect and report "pre-incident indicators" or intuitions (Gonzalez 2004). The science of intuition, hunches, and gut feelings is also relevant. Many people discount or think poorly of such science, but it is important to note that people are generally able to focus more accurately on what's important when they have become knowledgeable about the threats facing them (Adams 1995). Threat assessment (Borum et. al. 1999; O'Tool 2000) consists of all the investigative and operational activities designed to identify, assess, and manage anything which might pose a threat to identifiable targets. A "threat" can be an verbal expression of intent, a symbolic gesture (e.g., motioning with one's hands as though shooting at a person), or simply a pattern of thinking that one notices about another person. It is important for average, ordinary persons to improve their threat assessment capabilities, and this is usually done by improving situational awareness.

Simply put, situational awareness (SA) is knowing what is going on around you. The following are some technical definitions of situational awareness:

- **"the perception of elements in the environment along with a comprehension of their meaning and along with a projection of their status in the near future" (Endsley & Garland 2000)**
- **"the continuous extraction of environmental information along with integration of this information with previous knowledge to form a coherent mental picture, and the end use of that mental picture in directing further perception and anticipating future need" (Dominguez et al. 1994)**
- **"all knowledge that is accessible and can be integrated into a coherent picture, when required, to assess and cope with a situation" (Sarter and Woods, 1991)**
- **"the combining of new information with existing knowledge in working memory and the development of a composite picture of the situation along with projections of future status and subsequent decisions as to appropriate courses of action to take" (Fracker 1991)**
- **"the knowledge that results when attention is allocated to a zone of interest at a level of abstraction, and the recognition of particular states of dynamic variables in a given scenario, and the formulation of a diagnosis regarding the processes underlying these present states" (Fracker, 1988)**

The concept of situational awareness (SA) has its roots in the fields of air traffic control, airplane cockpit control, manufacturing process control, military command and control, and information warfare. Most writing on the subject is aviation or military related, although in the field of business, one might find SA mentioned in the context of competitive intelligence or computer forensics. In the field of medicine, SA might be a part of emergency room management or forensic nursing. In computer science, one might discover discussions of SA on the topics of multimedia, virtual reality, gaming, and artificial intelligence. In psychology, one might find SA talked about in books on perception, memory, or cognitive semantics. Human factor engineering or ergonomics

are other fields where one might encounter the term.

PROFILES AND INDICATORS

In criminal justice, one is most likely to encounter SA within the topic of profiling. Profiling is slightly different from situational awareness, but some of the basic ideas are the same, such as the use of common sense and "outthinking" the enemy. In the homeland security context, SA is also similar (but slightly different) than what the TSA calls "behavioral detection" which involves undercover officials blending in among citizens to look for telltale facial expressions and body postures which betray fear, stress and deception. It is unfortunate that most people are only familiar with the contributions of serial killer profiling to criminal justice, so here are some examples of *various other profiles that exist* in police science, criminal justice, and criminology:

"Drug Courier" Profile	***"Gang Member" Profile***
• Rear end of vehicle dragging low • Spare tire in back seat to make room in trunk • Tinted windows or other modifications to vehicle • Very little luggage in out-of-state vehicle • Good-guy decals such as pro-police stickers • Decals of rock bands or drug-related decals • Multiple deodorants to mask odors • Dirty vehicle with clean plates or vice-versa • Unusual driving, weaving, or perfect driving	• Usually male • Admits to having had school problems • Has inadequate family affiliation or family history • Comes from lower socioeconomic background • Has negative role models; uses gang signs • Is very street smart, aggressive and antisocial • Has no father figure or dysfunctional one • Likely suffers from learning disability • Wears certain symbols, insignia or tattoos
"Child Molester/Pedophile" Profile	***"Snapping in Workplace" Profile***
• Extroverted with image of being overadequate • High self-esteem, insightful, articulate • Projects image of stable home and family life • Marriage is a sham and everyone knows it • Uses spouse as personal manservant • Open in talking about sexual history • Lies about things like having college education • Able to cover up drug or alcohol problem • Denies responsibility for basic facts about conflict • Seeks opportunities to be around children • Likes making children feel like adults • Collector of sex toys or pornography • Has no conception of normal childhood	• History of violence • Psychosis and/or projection • Romantic obsession with co-worker • Chemical dependence • Depression • Pathological blaming • Impaired neurological functioning • Elevated frustration level • Interest in weapons • Evidence of personality disorder • Vocalization of violent intentions • Evidence of strange or bizarre behavior • Recent or upcoming disciplinary hearing

BOMB THREAT INDICATORS

The U.S. Department of Transportation (Office of Federal Transit Administration) in their

March 2003 issue of *Transit Security Newsletter* suggested that employees and the public use the following indicators to identify unusual packages, suspicious substances, and anyone who is acting suspiciously. These indicators are known as the Large Vehicle Bomb Indicator Checklist, and are presumably unclassified, but just in case, I've backed off from providing the full list and am only providing a sample for educational purposes.

Large Vehicle Bomb Indicator Checklist

1. Holes in vehicle
2. Excess weight
3. Interior blacked out
4. Recently painted
5. Parked near possible target
6. No loading or unloading
7. Unusual smells (fuel or smoke)
8. Tampering or modifications
9. String, wire, or tape visible
10. Excess wire or cable apparent
11. Other antenna in sight
12. Fresh undercoating
13. License plates unusual
14. VIN number unusual
15. Reported stolen
16. New parts added

In addition to vehicle and package bombs, one must be alert for signs of suicide bombing, which according to Yorum Schweitzer's article at the ICT website typically involves a bomb worn on the body (the Turkish, Palestinian, and Tamilese modus operandi), a suitcase bomb (the Jihadi and Lebanese modus operandi), or a vehicle of some kind (the Al-Qaida modus operandi). *True suicidal motivations are complex*, and there may be additional motives which make the act more closely fit a homicidal model. There are also significant ethnic and religious differences. For example, if authorities had known what to make of all the shaved-off body hair in the motel rooms the 9/11 hijackers stayed in the night before, this might have indicated a certain Muslim desire to smooth the passage to paradise in the pursuit of deluxe martyrdom. *Most suicidal ideation checklists are, unfortunately, derived from mental health assumptions of "depressive" pre-incident indicators.* However, Marquise (2004) has a set of indicators used in SLATT training which expresses an admixture of "depressive" and "anxious" elements, and again, only a partial list appears below:

Suicide Bombing Indicator Checklist

1. Makes suicide note or video
2. Gives possessions away
3. Little regard for future
4. Social isolation from others
5. Sweating and mumbling
6. Inappropriate attire
7. Last-minute indulgence in "sin"
8. Surveillance of target
9. Increased religious involvement
10. Buying of props or disguises
11. Tends to keep hands in pockets
12. Unresponsive to verbal commands

TERRORIST THREAT INDICATORS

The most commonly used set of terrorist indicators are those provided to law enforcement and selected members of the public by the Joint Terrorist Task Forces (JTTFs) which are partnerships associated with the FBI Office of Counterterrorism. Again, this is unclassified information, but is of a sensitive nature, so I've backed off from being complete and only provided a brief sample (of a Sept. 2004 list) for educational purposes, as follows:

Terrorist Activity Indicators

1. Male, late 20s to early 30s
2. Recently entered U.S.
3. Owns or interested in heavy vehicles
4. Interest in flight training or diver training

8. No signs of employment, but lots of $
9. Appears to have previous military/security training
10. Numerous calling cards or cell phones

5. Interest in remote control devices	11. Pays in cash; refuses maid service
6. Connected to extremist organization(s)	12. Recent treatment for chemical burns or radiation
7. Appears engaged in surveillance activity	13. Possesses untraceable ID documents
	14. Unusually calm and detached behavior

Most terrorist attacks are planned weeks, months, or sometimes years in advance, so *it might be useful to distinguish between "long-term" warning signs and "short-term" warning signs*. Long-term signs would involve the terrorist "planning" stage, and for this, a rather lengthy list of indicators might be needed. The planning stage includes such things as reconnaissance, obtaining fraudulent documents, and accumulating funds and supplies. More short-term indicators would be the kinds of things involving surveillance, transportation, and housing. The basic pattern is one where *the terrorists try to move around the country in an effort to throw authorities off* their trail, leaving "sleeper cells" in their wake. Despite the advanced security precautions that terrorists usually take (Dyson 2005), the planning stage, in some respects, offers law enforcement its best chance of preventing terrorism. Following Dyson's (2005) lead, and to some extent, Marquise's (2004) also, let's consider elements of the planning stage as attack preparation indicators, which can be partially summarized in the checklist below:

Terrorist Pre-Attack Preparation Indicators	
1. Reading extremist/radical literature	9. Rental of storage units
2. Studying law enforcement procedures	10. Rental of living unit for fairly large group
3. Monitoring homeland security efforts	11. Frugal living arrangements and lifestyle
4. Interest in maps, photos, blueprints	12. Borderline bank, mail, credit card fraud
5. Interest in cameras, observation equipment	13. No interest in mastering English language
6. Interest in military-style clothing, equipment	14. Connections to suspicious groups
7. Suspicious immigration documents	15. Connections to foreign charity groups
8. Counterfeit or altered identification cards	16. Secure computers, other electronic devices

Now, it is with the above set of pre-attack indicators that most civil liberties advocates draw the line. After all, any number of innocent people could engage in some of these activities. For example, someone could be a "news junkie" who surfs the Internet to read extremist or radical writing; a "police wannabe" who studies law enforcement; a military-style weapons "enthusiast," or simply a criminal justice student studying terrorism and counterterrorism. *It's unlikely the civil liberties question will be resolved anytime soon*, as like with questionable research ethics, the greater good of the results for all of society (unattainable by other means) outweighs the potential harm to individuals (if no torture, maiming, or murder occurs). This 1948-era Nuremburg Code ethics characterizes much of U.N. thinking on the subject of internal security, the 1964 Helsinki Accord position on human rights, and the American post-9/11 approach to homeland security. It's unfortunately a throwback perspective from more modern positions that could be taken, but it is at least an ethical standpoint. When involving ordinary citizens in profiling terrorists, it's a good idea to teach those citizens how to overcome stereotypes and "conditioning" which makes them think of a certain type of person whenever they think of "terrorist." A good example of such de-conditioning can be found at Pennsylvania's Terrorist Awareness site which reinforces that you CANNOT identify a terrorist by how they look, what they eat, where they're from, or what they

say. It is also recommended that citizens who report suspicious things should be required to meet with the first responder to answer/discuss any questions and/or point out the exact location of suspicious happenings. It is probably NOT a good idea to allow ordinary citizens to engage in following or tailing suspicious persons. Pennsylvania has actually rejuvenated some of its *loitering laws* to provide the following checklists for "suspicious" things citizens should be on the lookout for:

Checklists for Suspicious Persons, Activities, & Items
1. An unidentified individual observed loitering near a facility or in the lobby of a facility for an extended period of time. 2. An unidentified individual observed wandering throughout a facility. 3. An unidentified individual dressed in oversized or inappropriate clothing (e.g. - a long heavy coat in warm weather) that appears to be concealing something. 4. An unidentified individual entering a facility carrying an oversized backpack or a large suitcase. 5. An individual in a facility with no visible company issued identification. 6. An individual who, when challenged by a supervisor or an employee, does not respond or does not provide a reasonable explanation for his/her actions. 7. An unidentified individual asking specific questions about your facility (e.g., security related matters, etc.). 8. An unidentified individual asking questions about key agency personnel (e.g., their normal arrival or departure times, their vehicle, location of their parking space, etc.). 9. An unidentified individual trying to deliver a package or other item to an office or to a specific person. 10. An unidentified individual observed photographing, videotaping and/or sketching the exterior or interior of any state facility. 11. An individual without proper identification entering your facility claiming to be a contractor, law enforcement officer, reporter or a service technician.
1. Two or more unidentified individuals observed loitering near a facility or in the lobby of a facility. 2. Individuals or groups who are uncooperative if challenged by a representative of that company/security or an employee. 3. Individuals or groups who appear at your facility without prior notification or clearance and claim to be contractors or service technicians. 4. Unidentified individuals attempting to deliver packages or other items to an office or to a specific person. 5. Unidentified individuals attempting to remove property from an office or a facility without proper authorization. 6. Unidentified individuals who appear to be conducting surveillance of a facility (e.g., sitting in a vehicle for an extended period of time and/or taking photographs or videotaping, etc.). 7. An unidentified individual observed placing an object or a package outside a facility and departing the area.
1. Any unattended backpacks, boxes, containers, luggage and/or packages in an elevator, hallway, lobby, restroom, snack bar or stairwell of your facility. 2. Any item that could be an improvised explosive device (e.g., items with visible wires, antennas, batteries, timing devices, metal or plastic pipe with each end capped or covered, etc.). NOTE: Untrained personnel should not examine or move a possible improvised explosive device (IED); the immediate area must be cleared pending the arrival of bomb squad personnel. 3. Rental vehicles/trailers parked near a facility, parked at or near the loading dock, or located in the parking lot without prior authorization.

4. Any vehicle that appears to be overloaded or has any substance leaking from it.
5. Any vehicle parked illegally or parked at an unusual location.
6. Any type of vehicle that appears to be abandoned (e.g., inspection sticker expired or missing, registration plate expired or missing, etc.).

THE SOCIOLOGY OF RISK AND CRIMINOLOGY OF DANGER

In the field of criminology, the concept of "danger" has been connected with at least three schools of thought: the *social disorganization* theorists of the 1930s; the *parole success prediction* researchers of the 1950s; and the *labeling theorists* of the 1970s (Walker 1980). In the field of anthropology, the study of "risk" (a term roughly synonymous with danger) is associated with the view that what we fear tells us more about ourselves that the source of our fears (Douglas 1992). In the field of sociology (the sociology of risk), the study of "danger" and study of "risk" involves looking at our postmodern society as a world which forces new kinds of uncertainty and unpredictability upon us (Brown & Pratt 2000). In the field of criminal justice, one might find studies of "danger" in many diverse areas, including the topics of domestic violence, serial killing, interpersonal violence, sex offenders, probation and parole violators, risk assessment in juvenile justice, ex-prisoner recidivism (the velocity of crime or how soon they reoffend), the setting of bail amounts, and pretrial detention. The fact of the matter is that the academic literature on criminal "dangerousness" is very fragmented, and easily confused with the topic of "dangerousness" in mental health settings.

For example, de Becker's (1998) best-selling *Gift of Fear* book, and his follow-up treatise on uncertainty in a time of terrorism (de Becker 2002), is typical of works (e.g., U.S. Marine Corps 2002; Bollinger 2004; Gil & Baron 2004) that rely heavily upon incorporating the criminology of mental illness (e.g., Monahan 1981). In fact, the whole field of profiling suffers from a "pathological bias" where potential offenders are seen as "crazies," psychopaths, or antisocial personalities. To some extent, this is inevitable with the inductive or "hindsight" approach to profiling, where a database of offenses are analyzed retrospectively, and any pre-incident indicators or warnings that should have been noticed take on a pathological slant in retrospect. It's not only retrospection that's the problem, but anticipation as well. Schneier (2003), for example, is a well-respected cryptologist, but like all prognosticators who gaze in their crystal ball toward an uncertain future that can barely be comprehended, he concludes that "people are the worst problem" and that the human dimension is always the weakest security link. This betrays a "compositional bias" (the composition, or make-up, of people in a population) which may have characterized criminology 75 years ago when social disorganization meant personal disorganization, but it's not the best theory-driven science today. Labeling theory, controlology, and environmental criminology (to name a few) all offer better prospects for scientific advancement than disorganization theory. There are also theories outside of criminology which can be helpful, most notably psychology.

In psychology, the middle ground between retrospection and anticipation is context (it all depends on the situation), and context usually provides the knowledge needed to guide perception (Norman 1994). Knowledge comes from two sources: (1) from cues or prompts that are immediately present in a situation; and (2) from memories and experience. This first kind of knowledge makes us think, and the second kind allows us to act without thinking. For example, if you know from experience the relative weight of objects from their size, you do not need to think about how much effort will be needed to lift an object. However, if your knowledge comes from the very act of perceiving, then you will need to think about what you've encountered before you make judgments or predictions about it. *Perception needs to come before knowledge for good situational awareness*. Too much information or too many expectations, and this advance knowledge will bias

your judgment and result in bad prediction. With homeland security, there's also the problem of establishing criteria for when an observer reports, or acts, on the knowledge from their perception.

Signal detection theory (Wickens 2001) in the psychological field of psychophysics offers some promise for studying when people are likely to report something perceived as suspicious. The decision to report is a simple yes-no decision, but often the situational context is ambiguous. Ambiguous situations contain both noise and signal, and the task for every observer in such confusing settings is to sort out the noise as well as the possibilities for false alarm. Sorting out the noise is, in fact, the most time-consuming part of the task. The following diagram illustrates this:

	Report Suspicion?	
	No	*Yes*
Noise	Correct Rejection	False Alarm
Signal	Miss	Hit

If the purpose is to increase successful "hit" rates, or correct perceptions, then more effort needs to be directed toward making people knowledgeable about "noise" and false alarms. This, at least, brings the criminology of it up into the 1970s, when labeling theory was concerned about such matters. To more quickly accomplish better "hit" rates, the best suggestion may be to refocus attention on the subject of what NOT to report, but this is unlikely to be a popular solution, since the practice of turning amateurs into semi-professional terrorist-hunters as the "eyes and ears" of law enforcement is likely to continue. Despite the fact that help is always appreciated, "the people are the police" and all that, it is also a sad fact that most citizens are unable to distinguish between noise and signal.

Professional intelligence analysts, on the other hand, possess a special expertise which provides them the skills needed for making "hits" through signal detection and pattern discovery. Pattern discovery differs from indicator-based approaches and data-mining approaches in that no group of indicators need to reach a certain stage before a warning signal emerges. It is concerned with threats "over the horizon." Also, pattern discovery is best to use when you don't exactly know the nature of a threat via regular risk-based vector methods. Pattern discovery is based on the the idea that discontinuities do not emerge at random, but contain "warning signs" which can also be described as "weak signals," or otherwise factors for change that are hardly perceptible at present, but may (or will) constitute a strong trend in the future or have dramatic consequences. Five stages can be distinguished during which weak signals develop into strong signals:

- **the weak signal emerges**
- **the source of threat becomes known**
- **the shape of threat becomes concrete**
- **the response strategies are understood**
- **the outcome of response can be predicted**

The management of "unknown unknowns" requires weak signal collection and analysis. Intuition and forecasting can be used to identify certain events or developments that could set off alternative dynamics and paths. Other techniques need to be developed for advancing the science of weak signal analysis.

AVERAGE CITIZEN INTUITION

Sometimes, it's the average citizen who overhears something that has vital implications for

homeland security. For example, a grocery clerk might overhear a potential terrorist mumble something like "They're all going to pay soon" when the store is out of their favorite ice cream. Likewise, in ordinary conversation, one might pick up on some "dark humor" or dripping sarcasm by a participant in the conversation. There are few limits to the number of interpersonal situations in which suspicion and intuition are raised. Intuition is a word with many meanings -- for example, some synonyms are: *apprehension, insight, instinct, foresight, inspiration, sensitivity, perceptiveness, premonition, hunch, sense, impression, notion, inkling, funny feeling, gut feeling, and sneaking suspicion*. The root of the word is *tuere*, which means to guard or protect. As de Becker (1998) points out (with the list below), women more than men are willing to rely upon intuition because they have dealt with stalking, domestic violence, and rape, or at least the signal threats for these, which are standard con man tactics easily spotted by someone who is on their guard against the potential for physical violence by an acquaintance or stranger:

Con Man Techniques of Stalkers & Abusers
(1) *Forced Teaming* - use of the word "we" to create the impression "we" are together in some way (2) *Superficial Charm* - a smile, lots of personality, and rapport-building (3) *Too many details* - volunteering just a little too much information or detail (4) *Typecasting* - calling somebody something slightly derogatory to see how you respond (5) *Loan Sharking* - generously offering assistance to unconsciously develop a sense of debt (6) *Unsolicited Promise* - a guarantee of something to convince of one's intent (7) *Discounting the word No* - persistently keeping up at something when its obviously over

It's important for average citizens to know how to protect themselves from fraud. The unfortunate reality is that far too many people are taken in by fraud, and fall victim to more serious crimes. Chuck Whitlock's (1997) ScamSchool and more recent CrimeLine materials provide training for how to recognize the fraudulent activities that often form the foundation of more serious crimes, like stalking, identity theft, and extortion. However, it's NOT often the charm (of a fraudster) that the average citizen has a hunch about, but the anger inside a person instead. More than anything else, interpersonal relations are characterized by the ability of one party to assess how "happy" or "unhappy" another party is, and the perception of unhappiness is sometimes perceived as anger or worry, with the slightest hints of rage or narcissism. What follows is a step-by-step guide to the typical con game process and some assorted terminology.

Typical Con Game Process and Terminology	
1. Making the mark (investigating & locating victims) *2. Playing the con (gaining the victim's confidence* *3. Roping the mark (steering him to the inside man)* *4. Telling the tale (showing him how to make money)* *5. Giving the convincer (permitting him to make a profit)* *6. Having him invest further*	*7. Sending him after more money* *8. Playing him at the big store* *9. Getting him out of the way* *10. Cooling the mark out (having him realize he can't turn to the law)* *11. Putting in the fix (bribing or influencing the law)*
Ace - having "the ace" means authorities have been bribed to keep away	Hush Money - money paid by duped victim in blackmail after the con game

Angle (or Opening or Pitch) - the approach when first contacting the victim
Beef - when a victims complains after losing their money
Big Store - any con game requiring a fake "front" or office
Blowoff - the last move in a con game
Booster - a shill for a con game pretending to be skeptical
Boiler Room (or Bucket Shop) - a "front" made to look like a stock trade room or a telemarketing setup
Build Up - part of the con game which builds trust with the victim
Button - part of a con game in which phony police make a bust
Cannon - a pickpocket
Cardsharp - a cheater who works for the house, always raising the pot
Come On - part of the con game which entices victims to in
Convincer - part of the con game in which the victim wins money
Cool - any method to appease a victim's anger over losing money
Depot Worker - a con man working the bus, train, or plane station
Easy Mark - the ideal victim of a con game; likes to take chances
Finesse (or Shift) - to make the victim look at something else; to distract attention
Fish (or Greenhorn) - the ideal victim of a con game; new in town
Fixer - one who sets up immunity for criminals
Gold Brick - any old, archaic con game
Green Goods - exchanging real money for near-perfect counterfeit money
Grifter (or Hustler) - any con man
Gypsy scam -- any con involving fees for lifting a curse
Hanging Paper - any con game involving checks, money orders, etc.
Hawk (or Prime) - to sell a victim on the idea of participating in a con game
Heat - police or legal suspicion about the con game
Heel - thieves who break into victim's home or hotel room
Hurrah - point in con game in which victim is trapped; has to go on

Inside Man - a con man to whom ropers bring a victim
Lookout - one who keeps an eye on all the players
Lugger - a lookout who keeps an eye on things outside
Make - when a victim recognizes they're being conned
Mark - the victim of a con game
Nut (or Touch) - the amount of money taken in a con game
Parlay - to promote a victim into a larger, more elaborate con game
Point Out - part of a con game in which the victim is introduced to Mr. Big
Queer the deal - anything which frightens off a victim
Red Inking - when a con man threatens or tries to frighten off a victim in order to commit them to greater participation
Roper (or Capper or Steerer) - a shill in a con game pretending to make money
Salt a Mine - to use real money or small items of real value in a con game
Score (or Sting) - successful completion of a con game
Selling Stiffs - any con game involving dead persons
Send - when the victim is sent home to Mama to get more money
Shill (or Plant) - one who lures a victim to a con game by acting like another customer
Squeeze - any con game involving a prize wheel or games of chance
Stall - point in a con game where the victim is temporarily prevented from participating in order to increase desire to participate
Switch -- point in a con game in which the victim is told how the scam operated so to make them think it was his or her idea all along
Tear Up - point in a con game where the victim's check is torn up in front of them to deflect suspicion and build trust
Wire - any operation pretending to have advance or inside information

Advance fee scam -- any up-front fee scam

Nigerian 419 mail fraud -- invitation to help

Advertising scam -- paying for nonexistent ads

Autograph -- getting the victim's signature

Badger scam -- any kind of a setup in which a man is put in a compromising position with a girl or prostitute and then the girl's "father" breaks in and threatens to cause trouble unless payment to keep quiet is made

Bail bond scam -- pretending to need money to get the victim's friend or neighbor out of jail

Bait and switch -- attracting victims with sale items not available

Bank examiner scam -- getting victims to hand over their withdrawals by telling them you're investigating a crooked teller

Block hustle -- selling items on street for fraction of their value

Call-sell operator -- fake long distance phone call time cards

Canister con -- fake canisters for donations to bogus causes

Charity con -- any use of fake charities or good causes

Circle of friends con -- involves friends, relatives, and associates

COD scam -- empty COD package is delivered to victim

Computer repair con -- hacker con to gain computer access

Coupon con -- any scam involving counterfeit coupons

Credit repair con -- creating an unusable new identity for a victim

Damage claim artist -- a professional accident victim

Diary scam -- involves selling the fake diary of a famous person

Diploma mill scam -- any phony college degrees or certificates

Dirt pile scam -- any con game involving real estate

Doctor scam -- any con game involving drugs or treatment

Dummy supply company scam -- phony billing of companies

Employment Agency con -- involves promise of job

Friendship swindle -- involves love or befriending a lonely person

Gold brick scam -- any old-time con (ref: phony gold bricks)

Green goods scam -- any con involving

beneficiary of estate transfer money out of country

Obituary scam -- when swindler pores over newspaper death notices, visits home of bereaved person, and demands payment on a debt owed

Paper accident scam -- any phony insurance claim

Paper pirates (or toner phoners) -- cheap office products

Phantom employee -- nonexistent employee time bill

Phony invoice scam -- legitimate-looking bills

Pidgeon drop -- street swindle where lost wallet or purse is "discovered" a lost wallet or purse. The con man convinces the victim to ask a "lawyer" what to do. The lawyer (another con man) says the victim should put up earnest money while owner is being contacted to negotiate the reward

Ponzi scheme -- any investment racket, pyramid scheme, or chain letter in which operator skims commissions off of deposits made by later investors

Religious scam -- any use of religion in a religious con game

Reload scam -- telemarketing recalls of people on sucker list

Roof repair scam -- fake or shoddy roof repair

Shoulder surfing -- steals numbers or passwords by loitering

Slip and fall -- phony falls and threats of lawsuit

Social engineer -- talking someone out of information

Spanish prisoner scam -- a con in which the victim is convinced that a wealthy prisoner is being held captive without access to his riches, and that if he or she helps bribe the captors, they'll get a reward

Straw man con -- usually a real estate or fake deed scam

Sweepstakes con -- win a prize but pay a fee

Sweetheart scam -- con artist romances the victim

Swoop and squat -- a staged car accident

Trash and dash -- con men pose as janitors to steal valuables

Triple-A con -- pretending to work for AAA

Vanity con -- any use of ego or love of self, like in modeling work or publishing a song

Work-at-home scam -- easy money for things counterfeit money

Home diversion scam -- visiting cons, one distracts, other steals

Hot seat -- convincting victim to put up earnest money

Identity scam -- using a victim's identity in any kind of scam

Inheritance scam -- using a fake inheritance in any kind of scam

Jamaican switch -- convincing victim to help visiting foreigner

Knockoff scam -- any phony, look-alike, designer product

Murphy scam -- any con involving money for drugs, prostitute services, and the like, then skipping out on the victim

Need help scam -- swindler has sick wife or broke car

like stuffing envelopes and product assembly

Worker compensation scams -- false injury claims

Yank down scam -- intentionally pulling display items in stores on top of yourself to file false injury claims

DETECTING ASSASSINS & TERRORISTS

In many ways, it's the perception of narcissism that matters most, especially when intuition is likely to raise the suspicion that someone is planning something big -- like a terrorist attack. This isn't to say that all terrorists are narcissists, or vice-versa, but that they share some psychological characteristics with certain kinds of narcissists. Specifically, a terrorist is different from a workplace violence character in that a terrorist has "*bad me*" paranoia while a workplace violence character has "*poor me*" paranoia. The terrorist suffers no sadness or depression that the workplace violence character suffers from. Instead, terrorist narcissism often takes the form of oppositionalism and grandiosity typical of the assassin. *Assassination is the twin brother of terrorism*, and it's often something that the average citizen might be able to detect, since many more assassination attempts are prevented every year than those which succeed. Like most terrorist attacks, it's not a crime that a person can practice.

Assassination is a much-neglected topic in criminology. There are hardly any books on the subject, and only sources like the *Encyclopedia of Crime and Justice* can be found with short, solicited excerpts on it. In criminal justice, it tends to be studied as a species of political crime with similarities to terrorism, but those similarities and differences are unclear. In the fields of security, only a certain amount of private "lore" exists, most notably by those who protect celebrities and public figures (de Becker 1998) or by those who's job it is to protect politicians (e.g. the U.S. Secret Service). The National Threat Assessment Center at the Secret Service has, in fact, probably done the most research on the topic, but de Becker's (1998) book provides the most public-friendly checklist of what to look for in his intriguing chapter (#13) entitled "*Better to be Wanted by the Police than Not to be Wanted at All.*"

de Becker (1998) states that assassins always study the techniques of other assassins, research their targets, make plans, assemble their weapons, and sometimes write letters to be found after the attack. *They do not fear going to jail; they fear they are going to fail.* Narcissism is a central feature behind every assassin, and they are seeking to feel significant in ways that significance was deprived them in childhood and adolescence. When detecting an assassin, like detecting a terrorist, the intuition that is likely to be triggered will be the mildest of intuitions -- an "uneasy feeling ... that funny feeling ... I just can't put my finger on it ... I can't explain it, but there's just

something ...." The following checklist (for assassins) from de Becker's book was apparently put together by prominent forensic psychologist Park Dietz, and it represents what is perhaps the most subtle set of pre-incident indicators one can create.

Ten Behaviors Common to Modern Assassins (and Terrorists)

1. Displays the slightest hint of some mental disorder
2. Tends to like in-depth research (of potential targets)
3. Keeps a diary, journal, record, or log (usually)
4. Interest in obtaining weapons or dangerous material
5. Communicates inappropriately with some public official (although *not* the one to be attacked)
6. Displays the slightest hint of exaggerated sense of self (grandiosity, narcissism)
7. Exhibits a random travel pattern
8. Identifies with unusual heroes from history (bad guys)
9. Seems to circumvent or be aware of security
10. Makes repeated approaches to target area

INTERNET RESOURCES

A List of Government Reports mentioning Situational Awareness
All About Stalkers & Self Protection
An Amazon Listmania for Books on Situational Awareness
CitizenCorps.gov: FEMA's site
Gonzalez Article on Situational Awareness in SWAT Magazine (pdf)
Integrating Intelligence for Border Security
Introduction to Terrorist Intelligence Analysis
New York State Guide to Terrorism Awareness for Citizens
Passenger Profiling
Potential Swimmer Attack Indicators
Pre-Incident Indicators of Potential Terrorist Activity
Ready.gov: The Department of Homeland Security's site
SA as a Multidimensional Concept in Command and Control
Situational Awareness and the Napoleonic Commander
Techniques of Terrorist Surveillance
Terrorism Awareness and Protection, Inc.
Texas Guide to Terrorism Awareness for Citizens (pdf)
The Chameleon Group, Inc.
Understanding Who Becomes a Terrorist
U.S. Secret Service Article on Assassins & Attackers (pdf)
U.S. Secret Service Article on Social Psychology of Terrorists (pdf)
Warning Methodology and Situational Awareness (ppt)
Wikipedia Article on Assassination

PRINTED RESOURCES

Adams, M. et al. (1995). "Situation awareness and the cognitive management of complex systems." ***Human factors*** **37(1): 85-104.**
Bollinger, M. (2004). ***Recognizing and treating exposure to anthrax, smallpox, nerve gas, radiation, and other likely agents of terrorist attack*****. Boulder, CO: Paladin Press.**
Borum, R., Fein, R., Vossekuil, B. & Berglund, J. (1999). "Threat assessment: Defining an approach for evaluating risk of targeted violence." ***Behavioral Sciences and the Law*** **17:323-405.**
Brown, M. & Pratt, J. (Eds.) (2000). ***Dangerous offenders: Punishment and social order*****. London: Routledge.**

Bullock, J., Haddow, G., Coppola, D., Ergin, E., Westerman, L. & Yeletaysi, S. (2005). *Introduction to homeland security*. Boston: Elsevier.
Bumgarner, J. (2004). *Profiling and criminal justice in America: A reference handbook*. Santa Barbara: ABC-CLIO.
Cannon-Bowers, J. & Salas, E. (1998). *Making decisions under stress*. Washington DC: American Psychological Association.
de Becker, G. (1998). *The gift of fear: And other survival signals that protect us from violence*. NY: Random.
de Becker, G. (2002). *Fear less: Real truth About risk, safety, and security in a time of terrorism*. NY: Little, Brown.
Douglas, M. (1992). *Risk and blame*. London: Routledge.
Dominguez, C., Vidulich, M., Vogel, E. & McMillan, G. (1994). *Situation awareness: Papers and annotated bibliography*. Armstrong Laboratory, Human System Center, ref. AL/CF-TR-1994-0085.
Durso, F. & Gronlund, S. (2000). "Situation awareness," Pp. 283-314 in F. Durso et. al. (eds.) *Handbook of applied cognition*. NY: Wiley.
Dyson, W. (2005). *Terrorism: An investigator's handbook*. Cincinnati: LexisNexis Anderson.
Endsley, M. (1995). "Measurement of situation awareness in dynamic systems." *Human factors* 37 (1): 65-84.
Endsley, M. & Garland, D. (2000). *Situation awareness analysis and measurement*. NY: Lea.
Fracker, M. (1988). "A theory of situation assessment: Implications for measuring situation awareness." *Proceedings of the Human Factors Society*, 32nd Annual Meeting, 102-106.
Fracker, M. (1991). *Measures of situation awareness: Review and future directions* (Rep. No.AL-TR-1991-0128). Wright Patterson Air Force Base, Ohio: Armstrong Laboratories.
Gil, I. & Baron, D. (2004). *The citizen's guide to stopping suicide attackers: Secrets of an Israeli counterterrorist*. Boulder, CO: Paladin Press.
Gonzalez, J. (2004). "Situational awareness," *SWAT Magazine* (January): 18-19.
Hammond, K. (1999). *Judgments under stress*. NY: Oxford Univ. Press.
Harwood, K., Barnett, B., & Wickens, C. (1988). Situational awareness: A conceptual and methodological framework. *Proceedings of the symposium on psychology in the department of defense*.
Kushner, H. & Davis, B. (2004). *Holy war on the home front*. NY: Sentinel Publishing.
Langer, E. (1990). *Mindfulness*. NY: Addison Wesley.
Marquise, R. (2004). "Recognizing terrorist indicators and warning signs." BJA SLATT Program: U.S. DOJ.
Monahan, J. (1981). *Predicting violent behavior: An assessment of clinical techniques*. Beverly Hills: Sage.
Nance, M. (2003). *The terrorist recognition handbook*. NY: Lyons Press.
Norman, D. (1994). *Things that make us smart*. NY: Addison Wesley.
O'Tool, M. (2000). *The school shooter: A threat assessment perspective*. Quantico, VA: NCAVC.
Rising, D. (2003). *A terrorist awareness and preparedness guide*. Raleigh: Lulu Press.
Sarter, N. & Woods, D. (1991). "Situation awareness: A critical but ill-defined phenomenon." *International journal of aviation psychology* 1, 45-57.
Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uUncertain world*. NY: Copernicus.
U.S. Marine Corps. (2002). *The individual's guide for understanding and surviving terrorism*. Boulder, CO: Paladin.
Walker, N. (1980). *Punishment, danger, and stigma*. Oxford: Blackwell.
White, Jonathan. (2004). *Defending the homeland*. Belmont, CA: Wadsworth.
Whitlock, C. (1997). *Chuck Whitlock's scam school*. NY: Macmillan.
Wickens, T. (2001). *Elementary signal detection theory*. NY: Oxford Univ. Press. [sample excerpt]

Last updated: Mar. 29, 2008
Not an official webpage of APSU, copyright restrictions apply, see Megalinks in Criminal Justice
O'Connor, T. (Date of Last Update at bottom of page). In *Part of web cited* (Windows name for file at top of browser), *MegaLinks in Criminal Justice*. Retrieved from http://www.apsu.edu/oconnort/*rest of URL* accessed on *today's date*.