INTELLENET NEWS

June 2006

Table of Contents

Carino's Corner

Jim is recuperating from his latest medical problems and was not able to provide his usual input for this Newsletter.

Therefore, in desperation and although I am not a Jim Carino, I thought I would add a few comments of my own. These comments are not to be blamed on Jim.

I repeatedly see requests on the Intellenet Listserv wanting to know if there is an investigator in a particular area, looking for a specific investigative skill, or wanting to know where a lab can be contacted in connection with an investigation or "where can I get insurance?"

Remember that the Intellenet website Membership List can provide you with information on your investigator requests. When was the last time you looked at Intellenet Supplemental Support List on the website? There are many individuals and organizations on the Supplemental Support List to meet many of your needs.

Using the Intellenet membership and Supplemental Support List should be one of the first places you look for assistance. It will also reduce the number of requests on the Listserv and save individual time responding too many of your requests.

Bill Blake

Clem was hired by an old farmer to help out during the harvest season. To make it easier for him to find his way to the field each day, the farmer suggested that Clem pick out a landmark to remember the tricky turnoff from the main road. Things went well the first two days on the job, but on the third trip, Clem got lost and arrived late.

"Didn't you pick out a landmark to help you remember where to turn?" asked the farmer.

"Sure did," replied Clem. "But the cows moved.

Know Your Fellow Members

Rick Johnson
President
Rick Johnson & Associates of Colorado
Denver, Colorado

Rick Johnson is a former investigator for the Denver County and Jefferson County District Attorneys' Offices, where he specialized in complex white collar crimes. He also served as grand jury investigator.

Rick started his private practice in Colorado in 1987. His first major investigation in 1987 was a probe of political kickbacks conducted on behalf of the Denver Elections Commission that determined that 50 of 51 candidates broke the law. After his investigation, Denver changed the Election Law. He since has maintained a specialty in governmental misconduct, including investigations into alleged misconduct by the police chiefs of four Colorado municipalities, all of whom resigned following Rick's investigations.

In 2002, Rick was called upon by the Arapahoe Board of County Commissioners to investigate the activities of County Clerk Tracy Baker and allegations of favoritism toward a female employee with whom he was having a sexual relationship. This situation generated a lawsuit by another female employee alleging discrimination and hostile work environment. His investigation uncovered hundreds of Emails, text messages, and phone conversations made on county equipment during business hours between Baker and his female employee, most of a personal and grossly sexual nature. Baker promoted the favored woman from motor vehicle clerk with a salary of $22,800 to deputy clerk with a salary of $63,100 during the relationship. Baker refused to resign. A recall election was held. Baker lost.

Rick also has specialized in domestic relations and child custody matters, including parental kidnapping, grandparents' rights, matters of visitation, and related issues, including the recovery and return of minor children to parents in Colorado and in other states, who have primary legal custody.

Rick also maintains a substantial litigation support effort on behalf of attorneys in Colorado and across the country. He recently was called upon by a California law firm to locate a potential witness known only by initials and a possible past residence in Boulder, Colorado. Rick found the woman in Scotland.

Along with major corporate, law, and governmental clients, Rick has maintained a long-standing obligation to the problems of individuals. In 2005, he responded to a plea from a mother whose daughter was engaged in an on-line and text-messaging relationship with a man via one of the most popular on-line dating sites. Photos and personal information were exchanged, but never by voice telephone. Repeated arrangements to meet were mysteriously cancelled by the man, but only after the daughter arrived at the arranged time and place.

Rick's investigation revealed that the man actually was a woman posing as a man, using photos taken from the Internet to present her image as a man and secretly stalking the daughter, even joining her health club. Rick identified the woman, her employer, the man whose photos she was using, and much of her personal history. He then arranged to confront the poser, and put an immediate end to the charade.

Rick is in his second term as president of the Professional Private Investigators Association of Colorado, Inc., (PPIAC.) Colorado is one of a handful of states that do not license or otherwise regulate private investigators. This year, Rick is leading a major PPIAC effort to obtain licensing, first via a proposal and model legislation submitted to the Colorado Department of Regulatory Agencies, which must rule on the need for licensing, and then, once that hurdle is passed, an effort in the Colorado Legislature to pass the enabling legislation.

Because Colorado does not regulate private investigators, Rick is the founder and president of the Private Investigators Academy of the Rockies, a school for new and prospective investigators. It's an introductory but comprehensive 18-hour course focusing on everything from how to set up and run a business to the major components of typical investigations, with an emphasis throughout the course on the law and ethics.

Rick is proud to be a member of Intellenet, an association for which knowledge, skill, and expertise are not just standards to be met, but paramount requirements. Intellenet truly is an organization in service to the world. He greatly appreciates all of the support he has received from the organization.

CID—The US Army Detectives

The U.S. Army Criminal Investigation Command was organized as a major command of the Army to provide investigative services to all levels of the Army. Using modern investigative techniques, equipment and systems, USACIDC concerns itself with every level of the Army throughout the world in which criminal activity can or has occurred. Unrestricted, CID searches out the full facts of a situation, organizes the facts into a logical summary of investigative data, and presents this data to the responsible command or a United States attorney as appropriate. The responsible command or the U.S. attorney then determines what action will be taken. Ultimately, the commander of USACIDC answers only to the Chief of Staff of the Army and the Secretary of the Army.

In 1775, the "regular" soldiers of the Continental Army received extensive training based upon the Prussian manual of arms. This training was designed to instill military discipline in the "Continentals" who would then be augmented by volunteer and militia units. The result would be a fighting unit which would instantly obey commanders during the heat of battle. This training would also help reinforce the maintenance of discipline within the ranks during periods when combat was not imminent. Failure to maintain discipline during bivouac and battle could destroy the Army and, with it, the new nation.

The emphasis on enforcing discipline within the Army continued until 1863, when the emphasis shifted to enforcement of a new law passed during the nation's Civil War.

As the Civil War dragged on and casualty lists proliferated, Congress passed the Enrollment Act which was designed to provide conscripts for the Union Army. It was the first draft law and was highly unpopular. Because riots often erupted in protest of the new draft law, Secretary of War Edwin Stanton felt that a police force was needed to enforce the new and unpopular law. In March 1863, the Provost Marshal General's Bureau was established to administer and enforce the draft law and to arrest deserters.

During the war, investigations of criminal acts within the Army, such as payroll thefts or murders, were conducted by private agencies such as the Pinkerton Detective Agency. Ultimately, Major Alan Pinkerton was commissioned by MG George McClellan to create the first criminal investigation division.

After the Civil War, the Provost Marshal General's Bureau remained largely unchanged until the American Expeditionary Forces entered France during World War I in 1917. As the number of American soldiers in France increased, so too did the need for additional police services. In October 1917, the Military Police Corps was established; from this corps, today's Military Police Corps evolved. Although this new corps functioned well in its role as uniformed policemen during World War

I, crime rates mounted and a legitimate need for a detective element became apparent.

In November 1918, Gen. John Pershing directed the Provost Marshal General of his American Expeditionary Forces to organize a criminal investigation division within the Military Police Corps for the purpose of detecting and preventing crimes within the territory occupied by the American Expeditionary Forces. The Criminal Investigation Division (CID) was headed by a division chief who served as the CID advisor to the Provost Marshal General on all matters (administrative and technical) pertinent to criminal investigation. Operational control of CID, however, remained with individual provost marshals. There was no central control of investigative efforts within CID and the individual investigators were hampered by a lack of investigative training and experience. Investigators consisted of personnel selected from military police units within each command.

Crimes committed by American soldiers and crimes committed by other nationals against the Allies were reported through channels similar to those of a civilian police force. CID personnel acted as detectives as they investigated crimes or suspected crimes.

CID effectiveness, although hampered by some shortcomings, produced favorable results in the recovery of stolen government and personal property. However, the absence of central direction and control, and the lack of investigative training and experience among personnel, kept CID from achieving its full capability.

Between World Wars I and II, the Army was reduced to a small peacetime organization where there was little need of a criminal investigative element.

The American entry into World War II in December 1941 changed the Army almost overnight from a small peacetime organization of professionals into a force of millions. Because the Army was a community within itself, and this community had grown so rapidly, there was again a need for some type of law enforcement system.

In early 1942, investigations of crimes committed by military personnel were considered to be a "command function" to be conducted by local military police personnel. The delegation of criminal investigations to a command function meant that each commander was responsible for seeing that crime committed within the commander's realm of responsibility was investigated. The Office of The Provost Marshal General felt that the agents in the Investigations Department were not trained for criminal investigations per se, nor did it anticipate their being used in that capacity. The only investigations being conducted at this time were "loyalty" investigations into the backgrounds of persons hired for employment in defense related industries.

As the Army expanded, so too did the crime rate. Criminal investigations failed to keep abreast of the expanding crime rate. Commanders did not have the personnel or the funds to conduct adequate investigations. In December 1943, The Provost Marshal General was charged with providing staff supervision over all criminal investigations.

The Criminal Investigation Division of The Provost Marshal General's Office was established in January 1944. The Provost Marshal General rendered staff supervision over criminal investigation activities, coordinated investigations between commands, dictated plans and policies and set standards for investigators.

Following World War II, the CID was centralized at the theater Army level. Control of criminal investigation personnel was decentralized to area commands during the 1950s and then down to the installation level during the early 1960s. While The Provost Marshal General still had overall supervision of criminal investigation activities, the operations were conducted at the local level.

A Department of Defense study in 1964 called "Project Security Shield" made clear that complete centralization of the Army's criminal investigative effort was needed in order to produce a more efficient and responsive worldwide capability.

In 1965, the Army took the first step towards centralizing command and control of CID elements.

Elements were organized into CID groups corresponding to the Army areas in the United States. The following year, the concept was introduced to units in Europe and the Far East.

This group arrangement did not totally solve identified problems and in September 1969, at the direction of the Army Chief of Staff, the U.S. Army Criminal Investigation Agency was established under the direction of The Provost Marshal General. The agency was to supervise all CID operations and to provide guidance to CID elements around the world.

However, the agency did not have command authority. It was only chartered to provide direction to the criminal investigation effort.

In March 1971, Secretary of Defense Melvin Laird directed the Secretary of the Army to form a CID command with command and control authority over all Army-wide CID assets.

On September 17, 1971, the U.S. Army Criminal Investigation Command was established as a major Army command. The CID Command was vested with command and control of all Army criminal investigation activities and resources worldwide. Granting major command status to the CID facilitated CID communications with all levels of the military and civilian governments while providing a centralized controlling authority over the Army's investigative resources and activities. The Commander of CID is directly responsible to the Chief of Staff of the Army and the Secretary of the Army. The organization of the CID command brought to an end the 50-year-old problem of how to administer the CID.

CID has the authority to investigate felony crime affecting the Army anytime, anyplace in the world.

During its history, CID has undergone considerable change, both in organization and its approach to the problem of detecting and preventing crime. Throughout the changes, however, run the threads of common purpose and principle that link yesterday's years of success by individual CID special agents investigating crime within the Army and today's agents. As the Army's responsibilities have grown and changed, CID has responded to every change by continuing to provide the timely, second-to-none investigative service that has become its trademark.

Regardless of the type of crimes investigated by CID, be it counter-narcotic, procurement fraud, property crimes or crimes of violence, CID's performance has invariably been at or above the standards of its nationwide law enforcement agency peers.

Today, the Criminal Investigation Command headquarters is located at Fort Belvoir, Va. Its position in the Army organization and its location at the seat of national government ensures the CID has a positive direction and remains responsive to the Army's needs. It is an organization that has successfully lived up to its motto:

Federal Air Marshals? – Don't 'Assume the Position' – The TSA circus continues

David Forbes
BoydForbes Security, Evergreen, CO

It was something of a surprise when I saw Steve Elson in the Fox News' Washington DC studio on December 8, with me sitting in Fox News Denver. The producer in New York had wanted opposing views on the Miami Air Marshal shooting incident. So we were probably something of a disappointment. Steve and I share much common ground on aviation security issues, and afterward we exchanged views with our frustrations - yet again the media preferred to spend seconds barely scratching the surface when it merits much more time and examination.

Speculation now abounds as to the true depth and impartiality of the investigation into the shooting death of American Airlines passenger Rigoberto Alpizar on December 7. But our interest does not necessarily focus on the actions of individual air marshals.

We are more concerned about the overall 'health' of the Federal Air Marshal Service [FAMS]. This agency, again under the management misdirection

of **T**he **S**ycophants **A**nonymous, is a troubled entity. BoydForbes has asked Steve Elson, a renowned Security Red Team exponent with US Navy Seals and FAA Security experience and tactical skills, to respond to three important questions. But before hearing from Steve, here are some other vital questions that members of congress and the public should be seeking answers to from the FAMS…..but don't hold your breath folks, as Steve will tell you, openness, honesty and accountability is far from the strong suit of TSA/FAM management.

1. What type of ammunition was authorized and used during the incident? An anonymous source has said that the [former Secret Service] managers of the FAMS have forced the marshals to use the type of .357 SIG rounds that have such penetration capabilities they would threaten the safety of an aircraft and its passengers. Anyone know if this is so?

2. Isn't it the case that the attrition rate of the FAMS is horrendously high, more than 40% turnover, with consequently fewer marshals deployed than the [approximately five thousand] target number announced in 2003?

3. The indicators are that at least two thousand air marshals have left the service in the past three years, and several hundred more are believed to be leaving, returning to the Border Patrol. What is the effect on air marshal morale and training with this high turnover, and what is being done about it and about the underlying cause of it – poor management?

4. What is the percentage of supervisory personnel in the FAMS – one suggestion, not confirmed officially, is that the service has somewhere near one supervisor of GS-14 rank to every three operational air marshals – how can this be? Anyone looking at the actual cost versus budget performance of FAMS?

5. How many air marshals have been recruited this year and is that number anywhere near the 2005 recruitment target?

6. The TSA/FAM circus last week shot itself in the foot when it put its Viper Teams into municipal transit systems without broad consultation and consensus with local law enforcement, then had to hastily withdraw. What might have happened if a local police officer was forced to confront an air marshal in a crowded subway transit system? A polite flashing of badges, or a rapid exchange, a volley of high velocity rounds?

Now: The Steve Elson Interview

BoydForbes: *Based upon the recent incident in Miami, your own Special Forces operational history and your experience with FAA Security Red Teams, what concerns do you have with the FAM program, as we know it today?*

Steve Elson: The old adage "train as you fight" is germane. Air Marshal training is static rather than dynamic and the stress conditions (long boring hours; screaming/yelling in a panicked cabin, etc, under which air marshals may be called into service are not in any way approximated during training. FAMS are unprepared for what is likely to occur in the real world. The Miami incident is an anomaly and should be discounted vis-à-vis FAM actions; air marshals are for the air, not the ground unless taxiing.

More critical is the fact that, unlike SOF and SWAT teams, these air marshals do not train together. Many have never met until they meet up for a flight. Thus they don't really know each other, each other's personality, each other's skills, each other's moves, etc. They lack good operational communications and they are spread so thin, they are likely to be more of a hazard in a stress situation (real or perceived) than a benefit.

BoydForbes: Why should we not believe, and why should we be worried about, the management of FAMS and TSA when, through spokespersons and public announcements, they are constantly giving

us reassurances about the quality of FAM training and deployment?

Steve Elson: The more accurate, salient, and factual question is: "why should we believe anything TSA/Air Marshal management says?" TSA/Air Marshal management has repeatedly been caught lying and this is only the tip of the proverbial iceberg. Air marshals who have quit reveal the fallacious nature of TSA/Air Marshal management announcements. Of course they are going to lie. One reason may be deterrence, but more likely is the fact that, like other organizations, TSA/Air Marshal management isn't going to announce that they have wasted billions to make matters worse. Bureaucracies are devoted to aggrandizement, self-promotion, and above all -- **protecting management**; fulfilling their stated mission is purely coincidental. Perfect examples can be found in the fact the FAA damn well knew the vulnerabilities of aviation pre 9/11 and did nothing; a more recent example of government lies and betrayal is evinced in the hurricane Katrina debacle. The army corps of engineers and Louisiana politicians (local, state, and federal) knew the levies in New Orleans were not capable of withstanding their advertised strength, but did nothing. And failures of Michael Brown/FEMA need no further elaboration. Most of the senior managers of the federal government agencies were selected for purely political reasons, not competence or character. TSA/Air Marshal management exemplifies the worst of these political appointees. They betray not only the public but also the operational air marshals who do want and try to do a good job.

BoydForbes: If you were given the authority opportunity and a responsible level of funding to change the FAM program for the better, what fundamentals would you adopt and what should the American public reasonably <u>expect</u> ***as an outcome from your recommendations?***

Steve Elson:

<u>Fundamentals</u> (in priority order)

1. **<u>Leadership</u>**. Strong/competent/moral leadership with true and harsh **accountability** at the core of the organization. The political managers of the current air marshal organization would be immediately fired. They should be prosecuted.

(a) Corollary. Leaders of the air marshals would seek, listen to, and act upon the recommendations of the operational air marshals/field agents.

2. **<u>Training</u>**. Realistic dynamic training that stresses real situations would be employed. Teams which trained and worked together, would be deployed on selected flights. If the government would actually harden the cockpit and place a secondary door aft of the cockpit so pilots could egress to use the lavatory, there would be <u>no need</u> for air marshals or guns on most planes. Now that we finally understand the concept of "acceptable losses," we don't need air marshals for most flights. If the "bad guys" can't access the cockpit, they can't take over and control the plane. FAMS would deploy on certain "high vulnerability" flights, not just scattered across the airline industry to make an ignorant public "feel good."

3. **Operational security (OPSEC).** TSA/Air Marshal managers run their collective mouths too much. It is way too easy to game the marshals aboard a plane, elicit responses from the air marshals, and learn how to beat them. **Faaaaar too easy!** The managers have put out enough information to help a terrorist group defeat the FAMS aboard aircraft. Currently TSA/Air Marshal management tries to put out information to fool the public into believing they have a significant counter terrorism capability. In the end, they give away critical information.

<u>What should the American public reasonably expect</u>?

Strong moral **leadership**; common sense; fiscal responsibility; well-trained and competent air marshal teams who work together and know each other; and **accountability**.

In-Home Service Provider Safety Tips

Bill Blake
Blake and Associates, Inc.
Littleton, Colorado

In today's society, many different types of service providers routinely enter the customer's residence. These people include babysitters, cleaners, and repair persons. Unfortunately, not all of these visits have a favorable outcome--some result in death, injury, or loss of property. A few simple actions can reduce the possibility of an adverse occurrence.

Prior to allowing a service person entry to your residence:

1. Know your service provider and reputation, i.e., well known business versus unsolicited neighborhood contacts.
2. Contact Better Business Bureau to identify past complaints.
3. Ask the vendor if he/she is insured and bonded?
4. Is the service person an employee or sub-contractor?
5. Does the service vendor require insurance and bonding of sub-contactors?
6. Does the vendor conduct employee background investigations?
7. Who will be the service person and will they have company identification?
8. Check national, state and local registered sex offender lists.
9. If necessary, for babysitters and other repeat visitors, conduct your own criminal records check through local law enforcement.
10. When in doubt, use another service provider.

While service person is in residence:

1. Verify the identity of service person.
2. Have more than one adult in residence, i.e., coffee with neighbor, relative.
3. Constant checking on service person's activities--moving throughout work area at random.
4. If you feel uncomfortable about the service person during the work period, immediately go to a safe area, i.e., out of the residence, into a locked room or into a locked vehicle.
5. CALL POLICE FOR ASSISTANCE.
6. Carry a portable or cellular phone with you at all times.
7. If attacked, make as much noise as possible to summons assistance.

After the service person has left the residence:

1. Report unacceptable conduct/actions to the vendor and if necessary, to the police
2. Report the incident to Better Business Bureau.

Pay Stub Extreme Income Makeover: Better Than an Amex Platinum Card Stapled To Your Forehead

Ægis, March 2006, The Lubrinco Group
Reprinted with Permission

Several Internet companies are offering "novelty pay check stubs" for, of course, entertainment purposes only.

For $89.95 you can buy a fake paycheck stub on-line that will fool anyone, according to the company that sells them. The paychecks are realistic enough to include the trademark of ADP, a major provider of payroll services to employers. ADP is ticked off to say the least. In fact, ADP has sued the site for trademark infringement in a San Jose, California court. The Associated Press and a number of newspapers have written about the suit.

The fake pay stub site has also drawn complaints from industry watchdogs who aren't buying the company's claim that its fake paychecks are meant merely to fool your spouse, or impress your neighbors, or for a looser to get a fake paycheck stub to impress a date. We can just hear the mope now: "Hiya babe. Wanna see my stub?"

Unfortunately, that same loser is going to use that same fake paycheck stub to get credit and rip-off the credit grantor, and will use it as proof of gainful employment to rent an apartment, and will use it to prove to their probation officer that they are making a real living (while still selling illegal Canadian Lipitor in retirement centers.

While the Tampa-based Internet business mentioned in the article may not last long, imitators will spring up all over the world. According to statistics we found, there were an average of over 15,000 daily click-throughs to the order page in November, December, and January. Now that's the type of traffic that can generate a real, attractive pay sub!

The only real protection against fraud involving fake paychecks is direct contact with the employer that supposedly issued the paycheck.

Federal Buildings Must Meet Standards

Government-Owned Property Balances Security and Public Need

Joanne Friedrick

Security Director News

Reprinted with Permission

It is a major balancing act: Putting the proper security measures into place in the nation's more than three billion square feet of government owned and leased office space vs. keeping these buildings accessible to their tenants and the public.

The Interagency Security Committee, which was created by executive order of President Clinton in 1995, has established minimum security standards for federally owned and leased properties, according to Steven Smith, program manager for the building security technology program of the General Services Administration. In 2004, the ISC began a review of various physical security plans related to critical infrastructure and resources. An updated set of security design criteria was released in September 2004, establishing requirements for construction of new buildings as well as modernization of existing federal buildings. There is also a set of security standards that apply to leased properties.

Meeting on a quarterly basis, Smith said the ISC uses risk-based criteria to establish the design basic tactics for each locale. Every two years, said Smith, each building receives a risk assessment through the Department of Homeland Security's Federal Protective Service. Smith said that organization has access to crime statistics and other information that is employed to assess risk.

"Then we can establish design basic tactics," he explained. For example, he said, a design basis tactic may be to protect against a bomb blast. The building security committee decides the specifics, he said, such as what type of protection to take against a certain type of bomb.

What can end up happening, said Smith, is the establishment of both physical and operational security measures, ranging from the erection of bollards around a building to changing out the glass in the windows to putting more guards in place.

While the GSA has minimum security standards for both owned and leased spaced based on ISC standards, Smith said each agency has its own needs and can make a case for more than the minimum.

Buildings are ranked ranging from I to IV for leased space and I through V for owned units. The highest level of owned space is typically reserved for facilities tied to national security, such as the Pentagon and CIA headquarters.

Otherwise, both leased and owned space operates on similar criteria based on number of federal employees, square footage of space and degree of public contact.

According to GSA's Security Standards for Leased Buildings, a Level II building, which has from 11 to 150 personnel with a moderate volume of public contact and occupies 2,5000 to 80,000 square feet, would require, at minimum, reserved government parking, exterior lighting, window film, entry locks, secured utility areas, emergency power, secured mechanical and roof, restricted building information, non-disclosure of tenants, shutdown procedures, an occupancy emergency plan, background checks on employees as laid out under Homeland Security President Directive 12, a 20-foot setback and blast-resistant façade as established under the ISC Security Design Criteria.

Higher levels incur more security, including systems such as intrusion detection devices, CCTV,

magnetometers, visitor management systems and fire alarms with voice communications.

Smith said much of the emphasis for federal buildings is on protecting the perimeter so public access can be restricted as little as possible. "The further we can keep the vulnerability away," he said, "the better off we can be."

Improvements to security, said Smith, are based on need and availability of funds. If an agency has an immediate need, he noted, they may use their own funds to help mitigate the risk.

———————————————

The Escaped Convict

An escaped convict broke into a house and tied up a young couple who had been sleeping in the bedroom.

As soon as he had a chance, the husband turned to his voluptuous young wife, bound up on the bed in a skimpy nightgown, and whispered, "Honey, this guy hasn't seen a woman in years. Just cooperate with anything he wants. If he wants to have sex with you, just go along with it and pretend you like it. Our lives depend on it."

"Dear," the wife hissed, spitting out her gag, "I'm so relieved you feel that way, because he just told me he thinks you are really cute!"

———————————————

The PI as Marriage Counselor

Domestic Investigations—Expect to be Surprised

Rick Johnson
Johnson & Associates of Colorado, Inc.
Denver, Colorado
Reprinted with Permission

It was a day like any day and a case like any other case, or so I thought. It started with a call from a husband concerned about his wife. He had questions that had been brewing for a while, apparently, and thought surveillance on his wife this night would provide the answers. This night was key for him, because his wife was to be at a bar with friends from work. She apparently has an affinity for poker, and the bar was sponsoring a small Texas Hold'em tournament. And he suspected that one of the men from work was the culprit in his fears about his wife's conduct.

Where… and when… it became something well beyond the normal expectations for a domestic relations case was at the conclusion, when the wife, in response to a telephone call from the husband that was made without my knowledge during a break in our meeting, not only… and surprisingly… invited herself to my meeting with her husband… but ended up paying the balance on the invoice, as well.

Clearly, this was a situation that could get out of hand, that even could be dangerous to either one of them or to me. I recognized the risk, of course, but my thought was that, if both were together in my office, my presence could serve to diffuse the situation.

As it turned out, in between her arrival and her paying the bill, I found myself forced into the role of a marriage counselor, as the wife, who clearly admitted that our report of her conduct was accurate, challenged her husband's conduct toward her, conduct that she asserted was at the root of her disaffection.

It's important to note that we observed the wife embracing and kissing an associate from work at the bar and again later on the street as they walked to where his car was parked. We observed the man and woman drive away in separate cars to an apartment complex, where her employer maintained a corporate apartment. But we saw the man drive away from that location after a few minutes to another, separate entrance to the complex, where he apparently maintained an apartment. We could not see whether the wife was in the car. In fact, given the darkness and the rain that had been falling steadily, we couldn't see into the man's car at all.

So, beyond the affection shown by the two, we saw nothing definitive as to how far along the relationship had progressed.

To that point, the wife was adamant, admitting the affectionate conduct, but denying that it went any further. In fact, she had called her husband and informed him that she had been drinking and was going to stay at the corporate apartment. The timeframe she quoted, in fact, coincided with the times that we recorded during the surveillance.

In any case, the details of the odd negotiations that went on in my office at the presentation and discussion of the report is really a sidebar to the position we investigators often must assume in accepting any case involving domestic surveillance.

That responsibility starts with the initial telephone call asking for help.

I don't think I've ever heard enough in that first call to merely and routinely accept a domestic surveillance case. In fact, I often aggressively challenge the prospective client on the need or even the potential value of the effort. In states where divorce laws provide for a "No-Fault" process, surveillance often is of no value. The clear exception, of course, is where children are involved and potentially at risk because of the conduct of one spouse or the other.

And all too often, the people who call me for help already have enough information to determine a next course of action… counseling, separation, divorce. As we talk, they frequently realize that any evidence from surveillance is just expensive frosting.

Of course, there is the understandable desire of a wronged spouse to obtain hard evidence that can be used to beat up on the other party, but a smart investigator has to recognize that the intensity of that desire to hit back can be a red flag. I think we all remember the Texas case, where the investigators outside a hotel where the husband was meeting a girlfriend stupidly notified the wife, who promptly drove to the location and used a Mercedes to repeatedly run over and kill her husband.

It has long been my policy to identify a second party, if possible, but I rarely can be convinced to pass that information on to the wronged client who hired me. An attorney may require that information, but many of the people who call me for domestic surveillance haven't consulted, let alone hired, an attorney—again, another reason for considered caution. Surveillance is profitable, but it is not without risks to both the client and to the investigator.

I regularly require a face-to-face meeting with a prospective domestic surveillance client. It's important for me to obtain a strong feeling about the client and the client's initial desires and goals. It's just as important for the client to gauge my experience and capabilities. And it gives both of us a much more effective chance to really evaluate the need for surveillance… not to mention, again, the mental and emotional state of the prospective client. The lesson is clear: domestic relations cases are never a matter of routine.

Husbands kill wives. Wives kill husbands. Innocent people often get caught in the crossfire. An investigator who merely takes a domestic relations case at face value is running a clear risk, both to himself and to the client and the wayward spouse.

Not many cases will end up with the extracurricular wife paying the bill.

Websites? Are They Worth The Cost?

Bill Blake
Blake and Associates, Inc.
Littleton, Colorado

Whether or not you have a website for your business is a choice individually made based on many factors. My personal experience with my website, www.blakeassociates.com, has been very good. I have received business and information requests from all sections of the United States and sectors of the business community through the website.

The business leads have been generated through various search engines reflecting the services provided and the security related articles I have authored. This is particularly important when attorneys are attempting to locate individuals who can provide litigation support. While membership in various legal databases such as Martindale.com

and Lexis-Nexis can be productive, they are costly, but the search engines have a very minimal cost.

The value of writing articles for your website cannot be truly appreciated until you get requests for assistance or information from webcrawlers who are potential customers. Not only does it provide marketing exposure for you, in many cases requests have been received from other businesses to link to your website, greatly increasing your exposure through their links.

I have received requests for information or permission to reproduce my website articles from academics. When the academic world reviews and reproduces your articles, they are verifying your professionalism and competency.

Over the years I have viewed numerous websites of our competitors and have developed recommended criteria for a viable website. One of the most disappointing things for me is to visit a good website and not be able to find a "contact us" section. It is amazing how many of these sites exist. This is contrary to the theory of a viable website: why advertise your business and not tell people how to contact you? As a minimum, the mailing, e-mail, telephone and fax contacts should be listed.

The secret to a viable website is not how many "gimmicks" can be incorporated. Personally, I get turned off by websites with the "flash" introductions that take forever to load. I'm not interested in the "gimmicks", only the content. When the "gimmicks" appear, I move on to another website.

The usual hyperbole of "how great I am" needs to be tempered with Jack Webb's "just the facts." Many websites concentrate on the organizations the individuals have been a member of or for whom they have provided services. By stating that you were employed by the XYZ agency does not tell me if you were an active general investigator, an administrative assistant or a lab specialist. This is primarily a "name dropping" exercise. As a prospective client, I'm not interested in your past employment affiliations, I want to know what you did during this employment and how it can be of value to me.

I often hear the comment—"I'm not a writer and cannot put together a good article." As the Intellenet Newsletter editor, I find this hard to believe. Many of the articles I have received for publication or have viewed on various websites are excellent. If you question your writing skills, there are several alternatives available to you.

1. Use a ghost writer who can accurately record your thoughts.

2. Do what I do—write an article and submit it to someone else for review and critique. Believe me, your spouse, teenager or office staff will not hesitate to correct you!

Is a website worth the cost? Yes, it is! For a minimum amount of money and effort, your business can increase dramatically. One good referral through your website will pay for the costs many times over.

Congratulations

On Wednesday, April 12, 2006, Robert E. Dudash, son of Robert and Brenda Dudash, Omaha, NE was inducted into the Delta Phi Alpha German Honorary Society, Theta Beta Chapter in recognition for his scholastic achievements as a German student at the University of Nebraska at Omaha. In order to qualify for membership, a student must have a minimum GPA of 3.25 in German and an overall GPA of 3.0 or higher. Robert is second from the

left and is pictured with other students also being inducted.

The Stockholm Syndrome

Mayer Nudell, CSC
N. Hollywood, California

Periodically, it is useful to take a look back to ensure that we understand the origins of phenomena that occur today. Sometimes, these origins go back far enough that the essential nature of a phenomenon is taken for granted, but not really understood. Given the incidence of kidnapping and hostage-taking in the world today, perhaps it is useful to take another look at the well-known, but not always well-understood Stockholm Syndrome and how it can affect the outcome of a kidnapping or hostage-taking.

The Stockholm Syndrome derives its name from a 1973 incident which occurred in the Swedish capital. After an attempted bank robbery was foiled by the rapid arrival of police, the hapless criminal retreated into the bank's vault with a number of bank employees and customers as hostages. During the ensuing six-day negotiations, which resulted in the would-be bank robber's surrender, a number of surprising developments occurred.

The criminal and the hostages established a cooperative relationship which complicated every action of the police. Hostages provided their captor with suggestions and acted as lookouts for him, even while he was asleep. When his surrender took place, the hostages formed a human wall around him out of fear that the police might shoot him. One of the hostages (a school teacher) even hugged and kissed him before he was taken away by police and professed her love for him. She married him while he was still in prison.

Puzzled by this, psychologists studied this case in considerable detail and ultimately determined that a type of transference, or bonding, took place between the hostage-taker and the hostages. Later cases have demonstrated that transference of this type can be encouraged by negotiators and can contribute to a peaceful and successful resolution of hostage and/or barricade situations.

This important phenomenon can be a two-edged sword. In some critical ways it can complicate the resolution of an incident. At the same time, its manifestation is a key asset in securing the safe release of hostages. The Stockholm Syndrome has three components. First, there are positive feelings on the part of the hostage(s) toward their captor(s). Second, there are negative feelings on the part of the hostage(s) toward the police and other authorities. Third, there are positive feelings on the part of the hostage-taker toward his captive(s).

Upon examination, none of these three factors is surprising. Positive feelings about one's captors are simply a manifestation of dependence. After all, the hostage is completely dependent upon the hostage-taker for everything from food and the performance of bodily functions to his very life. In such a case, it is natural that the hostage will begin to seek ways to build an alliance with his captor and to focus on the positive in doing so. This is a form of bonding similar to that which occurs between an infant and his mother. The complete dependence of the hostage promotes gratitude (for not being harmed) and a positive affiliation with the captor in much the same way that nursing promotes the development of love between a baby and his mother. Because the infant-mother bond represents the most basic form of security as well as dependence, some experts have suggested that this facet of the Stockholm Syndrome represents a form of psychological regression by the hostage.

The development of negative feelings toward the authorities by a hostage is, in many ways, a logical extension of the first component of the Stockholm Syndrome. As the positive affiliation with his captor occurs, the hostage comes to blame the authorities for his predicament. After all, if the police would just let the captor go, if the government would just agree to the terrorist's demands, everyone could go home. When this is coupled with a realization that the police may come through the door shooting, the hostage comes to believe that the **real** danger to his life is the action of the authorities outside rather that any threat from his captor inside.

The last part of the Stockholm Syndrome, positive identification with the hostage-taker by the hostage, also has a readily understandable basis. As an incident begins, the hostage has no personality for the hostage-taker. Hostages are merely leverage to be used with the authorities during the negotiations process. However, as events unfold, the close proximity between captor and hostage as they share the crisis forces them to see each other as human beings. This changes the hostage from an impersonal symbol to a living, breathing person. This makes it much harder for a terrorist or any hostage-taker or kidnapper to harm the hostage.

The hostage negotiator has no control over the development of the first two components of the Stockholm Syndrome. However, he can and should do everything possible to encourage the development of the third component. In fact, a skilled negotiator may be able to extend this third factor into a positive relationship between himself and the hostage-taker. Time is often a factor in this process, but the negotiator can assist by emphasizing the hostages' human qualities, by frequently inquiring about their well-being, and by creating tasks which the hostage-takers and the hostage must perform as a group (for example, the distribution of bulk foods and clothing.)

The important thing to remember is that, while the development of the Stockholm Syndrome is a positive sign in terms of the ultimate resolution of an incident, the close identification between hostages and their captors must be kept in mind as the incident unfolds. This places an additional burden on the authorities during any rescue or surrender, as they cannot be certain of the extent to which this identification may prompt unexpected and dangerous actions by the hostages. For example, in the original Stockholm incident, the hostages formed a human barrier between their captors and the police.

Understanding the dynamics of the Stockholm Syndrome is an important asset, not only for negotiators, but also for preparing potential victims for kidnapping and hostage situations.

The two good ole boys were sitting at the bar having a couple of cold ones and discussing Southern women.

"I do believe that women in the South are the prettiest in the county," declared the first. The other man nodded in agreement. "And you know why? "Cause they win all the beauty contests."

The other man looked at him quizzically. "They don't like group sex?"

"Nope. Too many thank you notes."

Executive Protection — Executive Protection - Decapitation *la* America: How China might invade Taiwan

Ægis, April 2006
The Lubrinco Group
New York, New York
Reprinted with Permission

Contributed by **Max Hirsch** (hirsch@taipeitimes.com), a former translator in the Ministry of Economic Affairs in the Taiwanese government. He is currently a reporter at the Taipei Times, Taiwan's premier English-language newspaper, and conducts research for the Ackerman Group, a Miami-based risk consulting and investigative company that specialize in kidnap victim recovery.

What's China waiting for?

Despite decades of saber rattling in the Taiwan Strait, geopolitical analysts are generally in agreement that the "opportunity cost" of an all-out invasion or blockade of Taiwan by China is exorbitant. That is, China simply has too much to risk by staging such maneuvers, particularly in this era of globalization, they argue. However, the *possibility* of an invasion or blockade in the near future - although increasingly slim - still exists and to a great extent influences regional players' behavior. This paper briefly explores invasion scenarios, focusing on probable methods of attack

and offering safety tips to multinationals on Taiwan.

The consensus among analysts that China is very unlikely to invade Taiwan in the short-term, at least before the 2008 Olympics, is sound. Since Deng Xiaoping's liberalization reforms in 1978, China's highest priority has been economic development, the preconditions for which include domestic and regional stability. As such, China's foreign policies have largely focused on fostering constructive relations with its neighbors. As China continues to integrate itself with the rules-based global community, it will also increasingly lay emphasis on maintaining *basically* healthy bilateral relations with the U.S. and EU. (trade disputes and the usual diplomatic spats notwithstanding).[1] A sudden, violent takeover of Taiwan by China would undoubtedly alarm and anger the international community, destabilizing the region and setting off an economic backlash that China might not be able to withstand. Furthermore, the range and enormity of China's domestic problems are staggering; experts are quick to point out that China is still too beleaguered by domestic troubles to stage the kind of military campaign required to successfully integrate Taiwan. [2]

Economically, cross-strait integration is *already* a reality. Taiwan presently enjoys a US$23.56 billion trade surplus with China, its largest export market. China, meanwhile, has benefited tremendously from the US$100 billion that Taiwanese investors have pumped into its economy to date. [3] To be sure, many vital, deeply entrenched production and supply chains in the Asia Pacific region and elsewhere would become severed or disrupted in the event of a war or blockade, devastating China's economy *and* the world's.

The consequences of attacking Taiwan could also include a swift U.S. response in kind. Although America is keen to preserve the status quo and avoid jeopardizing relations with China, it also has a track record for intervening in cross-strait flare-ups. In 1996, for example, the U.S. deployed the largest armada to the region since the Vietnam War in response to Chinese missile tests in the Strait (Chinese missiles had splashed down alarmingly close to Taiwan). [4] Also, U.S. arms sales to the island are extensive. Analysts are increasingly skeptical that the U.S. is willing to wage a full-blown war - or even a limited war - with China to protect Taiwan. Nonetheless, given these examples and President Bush's vow to use any and all means to safeguard the island, the possibility of a strong U.S. response to a Chinese attack on or blockade of Taiwan still serves as a strong deterrent.

In February 2005, Japan issued a joint statement with the U.S. in which Taiwan is referred to as an area of "mutual concern." The Secretary-General of the Liberal Democratic Party - Japan's ruling party - commented that the U.S. and Japan would absolutely not tolerate a Chinese military invasion of Taiwan. Japan later announced in May 2005 that it would deploy 24 of its most advanced fighter aircraft (F-15J) to Okinawa by 2009, significantly boosting its ability to respond to a crisis in the Strait. [5] (Recent backsliding in Sino-Japanese relations has empowered hardliners in the Japanese government, resulting in Japan's committing more military resources to the protection of Taiwan.) As long as the status quo and a containment of China serve U.S. and Japanese interests, [6] China must factor in the possibility of waging war against these countries in a campaign to forcefully annex Taiwan.

New tensions, old risks

These and many other deterrents explain why China has yet to yank Taiwan into its administrative fold, in spite of all its bluster and brinkmanship. However, recent provocations by Taiwanese president Chen Shui-bian and other pro-independence elements have thrown a spotlight once again on the threat of a cross-strait war. In late February 2006, Chen terminated a domestic advisory council charged with overseeing unification with rival China (against the advice of the U.S.). He has also reiterated his intention to draft a new constitution before the end of his second term, and is trying to steer Taiwanese investment and trade away from China. China views such actions as precursors to declaring formal independence. The U.S., for its part, seeks to rein in Chen before he goes too far in *his* brinkmanship.

In light of recent tensions and China's military buildup, [7] speculation regarding a Chinese invasion of Taiwan deserves revisiting here. As I have tried to demonstrate, China is poised to invade Taiwan, but has been held back by numerous cogent disincentives. These are edgy circumstances in which misunderstandings or false moves could precipitate a war. Indeed, a recent "scenario study" conducted by a major faction within Taiwan's ruling party (the pro-independence Democratic Progressive Party [DPP]) concluded that there exists a high probability of China and Taiwan misjudging each other's actions, and that such miscalculation could lead to major cross-strait conflict. According to a report by Taiwan's Central News Agency, the study explores two scenarios:

The first [scenario] was set in 2007, with China using a major oil find in the western half of the Taiwan Strait to launch an offensive against Taiwan. The second scenario was set in 2015 when a nuclear plant explodes in Qinhuangdao on China's eastern coast, creating major domestic turmoil. The question poised was: Would China invade Taiwan to divert public attention from the disaster? [8]

Anatomy of attack

Assuming that a war did erupt, how would it play out? How would China invade and then integrate Taiwan? According to David Shambaugh's authoritative *Modernizing China's Military: Progress, Problems, and Prospects*, China is taking its cues more and more from the U.S. in this regard. That is, America's (and NATO's) technological and tactical prowess on the battlefield has inspired Chinese war planners. The PLA has observed the U.S. military and NATO closely in their operations, admiring their "decapitation" of command and control targets in recent conflicts, as well as their technological capabilities. [9] Given that the PLA is actively internalizing American standards of warfare, it is fair to assume that a Chinese invasion of Taiwan would be reminiscent of America's overall style of attack since at least the first Gulf War. *Jane's Defence Weekly's* Taiwan correspondent, Wendell Minnick, spells out precisely what a PLA invasion of Taiwan would look like in his article, *The year to fear for Taiwan: 2006*[10] The opening paragraph of the article reads:

If China ever makes the decision to invade Taiwan it is unlikely to be a large-scale Normandy-style amphibious assault. The reality is that China is more likely to use a decapitation strategy. Decapitation strategies short-circuit command and control systems, wipe out nationwide nerve centers, and leave the opponent hopelessly lost. As the old saying goes, "Kill the head and the body dies." All China needs to do is seize the center of power, the capital and its leaders. [11]

Minnick then portrays a hellish takeover scenario beginning with an airborne assault comprised of sudden, massive airdrops of Chinese paratroopers directly on Taipei and other strategic points. Preempting claims that China currently lacks the resources to be able to execute this initial airborne assault, Minnick notes, "intelligence reports have indicated that China was able to airlift one airborne division to Tibet in less than 48 hours in 1988. Today, China's ability to transport troops has greatly improved. China is expected to be able to deliver twice that number - 22,000 - in two days." According to the article, a more clandestine offensive perpetrated by Chinese spies and assassins would precede the airborne assault:

Pre-positioned special forces, smuggled into Taiwan months before, would assassinate key leaders, and attack radar and communication facilities around Taiwan a few hours before the attack. Infiltrators might receive some assistance from sympathetic elements within Taiwan's military and police, who are believed to be at least 75 percent pro-Kuomintang (KMT), and hence, pro-unification. Many could use taxis to move about the city unnoticed. Mainland Chinese prostitutes, already in abundance in Taiwan, could be recruited by Chinese intelligence to serve as *femme fatales*, supplying critical intelligence on the locations of key government and military leaders at odd hours of the night; death is the ultimate aphrodisiac.

China's offensive, according to Minnick, would quickly overwhelm Taiwan's military, which he represents as wholly ineffective in protecting the island against a hypothetical Chinese attack.

Taiwan's air force, for example, is believed to have only enough munitions to hold out for two days in a war with China. [12]

With regard to post-war political integration, Minnick writes:

Once Taipei was captured, a new government chosen by Beijing would be sworn into office. There would be plenty of Taiwanese politicians to choose from. It is well known there are many pro-China legislators who have investments in China and more than a few who have had private meetings with Beijing officials. The inauguration would be conducted in the spotlight of the international media There would be too many pro-China people in the State Department - privately relieved the Taiwan issue was finally settled - to say anything in Taiwan's defense. With the new government inaugurated, the new president would declare an end to all hostilities with China With pro-China sentiments running high in the Taiwan military, it is likely that most would grudgingly accept the new president.

What about a guerilla insurgency? Would a high-tech, strategic offensive *la* America deliver China into a quagmire *la* America in Vietnam, or America in Iraq? Taiwan's mountainous terrain, subtropical jungles, and coastal urban sprawl would certainly serve as an ideal backdrop for a nasty guerilla war. Such a grass-roots insurgency is possible but very unlikely. Guns, for instance, are almost unheard of among Taiwanese citizens (except among aborigines and triad members). Moreover, it would be very difficult to funnel weapons to Taiwan after a Chinese invasion - Taiwan is, after all, a fairly small island that China would no doubt surround and seal off in an invasion or blockade.

How willing ordinary Taiwanese are to fight back is another issue. Northern Taiwanese are known for their political ambiguity and lack of nationalistic fervor; it is difficult to imagine the PLA meeting much resistance from the citizenry north of the Choshui River. [13] Southern Taiwanese, on the other hand, are typically much more nationalistic, and would be ideal candidates to wage an underground resistance. However, citizens' lack of weaponry and the fact that the PLA's greatest asset is its sheer number of troops[14] bode ill for potential insurgents. Also, the cultural and linguistic sameness between the Taiwanese and Chinese would make it that much easier for the former to eventually accept the latter as the island's new stewards.

Some analysts assert that a no-holds-barred military offensive is unnecessary; China need only blockade the island with its growing arsenal of destroyers, submarines, and other vessels. A trade-oriented island economy like Taiwan's would quickly collapse. Even cross-strait across-the-board trade sanctions, imposed by China *without* a blockade, would "force Taiwan to its knees in a week," according to Hu An'gang, a prominent Chinese economist. [15]

China's need for naval supremacy to pull off a successful invasion and/or blockade of Taiwan is obvious - especially if China is to discourage the U.S. and possibly Japan from militarily intervening - and accounts for a certain doctrinal shift in the PLA as well as some spooky occurrences in the Pacific theater lately. Shambaugh does well to illustrate China's paradigmatic evolution in the context of naval warfare:

China's claimed strategic frontiers now extend beyond its immediate borders into its regional periphery. The principle [doctrinal] shift was from continental to maritime and national to regional definitions. They also include defined spheres under the sea and in space. A redefinition of China's maritime interests has been cultivated, and Chinese are now told to develop a "conception of sea as territory" Chinese are now regularly taught in textbooks that their "sovereignty" includes three million square kilometers of oceans and seas[16]

The launching of China's next generation nuclear attack submarine, as well as new indigenous and newly bought diesel submarines from Russia have gone hand in hand with occasional intrusions of Chinese vessels into Taiwan's and Japan's maritime zones. A Chinese submarine's bold expedition in Japanese waters in November 2004 is perhaps the most egregious example. However, stealthy incursions of Chinese scientific ships into Taiwanese and Japanese maritime territories are more common. A 2005 paper published by the

Brookings Institution, a prominent American think tank, cites Japan's 2004 defense white paper in reiterating the suspicions of military experts that such "activities have been conducted in order for the Chinese navy to better map the ocean floor and gather specific data needed for their submarines to exit into the Pacific without being detected by U.S.-Japan reconnaissance capabilities.":

In recent years, China has been expanding the scope of its maritime operations. Chinese vessels have carried out activities that seem to be oceanographic research, mainly in the exclusive economic zone (EEZ) of Japan. Japan and China, to settle the issue, formulated a framework for mutual prior notification on scientific oceanographic research activities in areas close to each country in the East China Sea However, Chinese oceanographic research activities without notification or inconsistent with notification under the framework have been observed. Furthermore, Chinese activities have been conducted even in Japan's territorial waters, without Japan's consent. Chinese warships have often navigated in waters near Japan. Chinese naval vessels that seemed to conduct some exercises or be engaged in intelligence [gathering] or maritime research have been observed. In June 2003, a Chinese Navy icebreaking and survey and research ship was observed stopping dead in the ocean south of Iriomote Island. In November 2003, a Ming-class submarine was seen surfacing in the Osumi Strait of Kyushi Island[17]

The idea behind these maritime forays seems to be to conduct hydrographic/ oceanographic surveys to map the ocean floor and pinpoint certain thermal levels below which Chinese subs can operate with impunity, undetected. Such stealth would give China the option of dispatching a diesel-electric submarine fleet (diesel subs are quieter than nuclear ones) to lie in wait for American vessels before the actual invasion or blockade is staged. Chinese subs could then surface and checkmate incoming enemy vessels before they are near enough to assist Taiwan. One-upping the U.S. on the high seas would create a window of opportunity for China to employ its missiles, air force, special forces, and IT-based weapons and systems to snatch the democratic life right out of Taiwan. The Chinese offensive would be fast and surgical, severing the Achilles' heel that is Taiwan's command and control infrastructure.

Executive protection

So, what is the bottom line for multinationals on Taiwan? Whether or not China will use "non-peaceful means" to seize the island in the foreseeable future is an inexhaustible debate that exceeds the scope of this paper. What it all boils down to, however, is this: an invasion or blockade is unlikely but possible.

The next question, then, is what should multinationals do in the event of a Chinese offensive? Obviously, multinationals should flee the island as soon as possible; however, chances are the attack would be so abrupt and swift that they would not get that chance. So, if multinationals unwittingly find themselves with ringside seats to a full-blown invasion, what then?

Firstly, for those in Taipei, where the vast majority of foreigners are on Taiwan, it would be imperative to stay out of the subway system, known as the MRT (Mass Rail Transit). A main metro artery - the Danshui and Xindian lines - snakes right through the nexus of the federal government, situated near the Chiang Kai-shek Memorial Hall and National Taiwan University Hospital stations. Errant missiles and other ordnance slamming into the streets could easily collapse the metro tunnels and stations in that area. A citywide blackout is also likely, so imagine if you will, getting trapped 100 feet below the surface in pitch blackness (or high above the city as would be case on the Muzha line), possibly in throngs of panicking people. Another especially dangerous MRT line to be on would be the Xiaonanmen Line - Taiwan's Ministry of National Defense and its Procurement Bureau are just opposite of Xiaonanmen Station. Aboveground in the Zhong Zheng District in the heart of Taipei, where most federal buildings are concentrated, would not be any safer. If missiles do not rain down on this area, PLA paratroopers will, and they will probably be met with stiff resistance by Taiwanese paramilitary personnel. Street combat would be intense here, so give it wide berth. Fleeing the city via Yangmingshan (or Yangming

Mountain), is ill-advised. The National Security Bureau - Taiwan's CIA - is right on Yang De Boulevard (No. 110), the main road up Yangmingshan. The Bureau is an eerie green-tiled fortress surrounded by jungle, barbed wire, and cameras, and is surprisingly close to the street. Stay away from this compound. In fact, stay away from Yangmingshan altogether - the whole mountain is peppered with signals intelligence (SIGINT) installations, and is likely to get hit hard.

The American Institute in Taiwan (AIT: the de facto U.S. embassy), like other U.S. embassies worldwide, employs the Warden Notification System or "warden system" to alert and advise Americans in Taiwan in the event of a crisis. American citizens should register with the American Citizen Services section at AIT in person or online (travelregistration.state.gov/ibrs/home.asp) to receive warden system services. Once registered, Americans will be assigned a "warden" based on the location of their residence on the island. Wardens are American volunteers who are charged with contacting and assembling U.S. citizens per AIT's instructions in the event of a crisis that may necessitate their evacuation. Other multinationals' home countries' missions are likely to implement a similar plan; signing up for it is a good idea. U.S. Regional Security Officers (RSOs) and other security personnel have been known to don Kevlar and arm themselves with assault rifles, and hit the streets to round up Americans in some emergencies. It would be wise to register a working cellular phone with the warden system and keep it on your person, and follow the instructions of the warden or RSO. In the event that cell and landline phones are out, try to be at your home address as registered with your warden. Of course, if you are in the Zheng Zhong District, take cover or flee from that area - on foot if you have to. For Americans, AIT may *not* be the safest place to go to, especially if the U.S. decides to assist Taiwan in defending itself. (The PLA may very well obliterate AIT much like U.S.-led NATO forces "mistakenly" blew up the Chinese embassy in Kosovo in 1999.)

Westerners are not likely to be targeted - individually - in a Chinese assault, so lying low and being contactable by one's embassy or mission is the best plan. Moreover, it is in China's best interests to minimize civilian casualties and other collateral damage, and allow foreigners to exit Taiwan once major hostilities have ceased. It is recommended that expatriates on the island formulate at least a ballpark exit strategy that encompasses not only themselves but also their financial assets.

1. China's Foreign Minister Li Zhaoxing commented on March 7th during the 2006 annual session of parliament that China's ascendancy will *benefit*, not threaten, its neighbors. He also called for better relations with the U.S. (China has consistently portrayed its rising power as beneficial to the international community.)

2. See my last ÆGIS article: "China Syndrome: Staving Off Social Meltdown in Rural China" (March 2006). In it I discuss China's struggle to maintain social order in its countryside. Indeed, corruption, environmental degradation, poverty, inadequate health care, and land disputes are some factors that have destabilized Chinese rural communities. China's top leaders are scrambling to address these problems and head off a nationwide implosion.

3. Lim, Benjamin Kang (2006, March 9). "Leading China economist says trade war can break Taiwan." Reuters. Published in *The China Post* on 03/09/2006, page 1.

4. Lasater, Martin L. The Taiwan Conundrum in US China Policy. Boulder, Co.: Westview Press, 2000 (page 261).

5. Bishop, Mac William (29 May 2005). "Japan to station advanced fighters on Okinawa." Taipei Times, front page.

6. Control of regional shipping lanes, especially in the Taiwan and Bashi Straits, and the Strait of Malacca, is potentially an extremely contentious (and a less talked about) issue due to the sheer tonnage of cargo that passes through these straits. In this era of globalization and trade, and especially as energy competition heats up, the U.S. needs regional partners like Taiwan in maintaining control of key waterways amid China's awesome military buildup.

7. On 7 March 2006, Taiwan's Ministry of National Defense reported that China now has more than 800 ballistic missiles pointed at the island. China's People's Liberation Army (PLA) staged high-tech exercises in early March, serving as a warning to Chen just after he terminated Taiwan's National Unification Council and Guidelines. Additionally, China announced on 4 March 2006 that it would increase its military budget 14.7% to US$35 billion (China's true military spending is widely believed to be many times the official figure).

8. 23 January 2006. "New Tide worrying about cross-strait miscalculation." Central News Agency (CNA). Reprinted in Taipei Times on 01/23/2006, front page.

9. Shambaugh discussed in depth the PLA's ongoing attempts to emulate the U.S. in its modernization, admiring and fearing America's and NATO's prowess in waging a "limited war under high- technology conditions," particularly in the Introduction and Doctrine and Training chapters of his book, *Modernizing China's Military: Progress, Problems, and Prospects* (Berkeley, CA: University of California Press, 2004).

Another seminal publication regarding China's military modernization is former US Air Force Colonel Mark Stokes' study entitled, *China's Strategic Modernization: Implications for the United States* (Carlisle Barracks, Pa.: U.S. Army War College Strategic Studies Institute, 1999). Stokes was a U.S. defense attach at the U.S. embassy in Beijing and the American Institute in Taiwan (AIT). The study is downloadable in its entirety at http://www.fas.org/nuke/guide/china/doctrine/chinamod.pdf and at http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=74.

10. Although Minnick would now probably withdraw his prediction that an invasion is likely in 2006, his depiction of how a Chinese invasion of Taiwan would be, is still very incisive and relevant.

11. Minnick, Wendell (10 April 2004). "The year to fear for Taiwan: 2006." Asia Times Online (see http://www.atimes.com/atimes/China/FD10Ad02.html).

12. Minnick, Wendell (25 May 2005). "Taiwan's military will fire blanks." Taipei Times, page 8.

13. The Choshui River is known in Taiwanese politics as the geographic line that roughly divides voters into northern and southern blocks. Northern constituents statistically tend to support pro-independence or pro-status quo parties and policies; southern constituents tend to back pro-independence parties and policies.

A recent study conducted at Taiwan's Academia Sinica suggests that although Taiwanese are fostering a stronger sense of identity with their island, their nationalism is as lukewarm as ever (see http://www.taipeitimes.com/News/taiwan/archives/2006/03/12/2003296948).

14. China boasts the largest military in the world, with a staggering 3.25 million members (that figure includes active paramilitary personnel).

15. Lim, Benjamin Kang (2006, March 9). "Leading China economist says trade war can break Taiwan." Reuters. Published in *The China Post* on 03/09/2006, page 1.

16. Shambaugh, David. *Modernizing China's Military: Progress, Problems, and Prospects*. Berkeley, CA: University of California Press, 2004 (pp. 66-67).

17. Tomohiko, Taniguchi. "Whither Japan? New Constitution and Defense Buildup." Brookings Institution, Washington, D.C.: May 2005 (pp 25-26) (see http://www.brookings.edu/fp/cnaps/papers/taniguchi20050530.pdf).

EVERYTHING CHANGES SOMETIME

Frederick A Bornhofen, CPP, CFE, VSM, AAFS
Bornhofen & Associates
Elverson, Pennsylvania

The Commonwealth of Pennsylvania is moving toward changing the state law concerning private investigators. Presently, the law enacted in 1953, allow us that the a judge may issue or deny a license which is recognized throughout the Commonwealth. It was interesting to reflect on the issues that form the basis for the 1953 enabling act and what actually did the private investigators do for living in 1953.

From the literature but it would seem that most private investigators spent their time in domestic cases and high-stakes homicide cases. In the public's mind, this is how they acted hide their time. With the advent of television, we saw a private investigator almost exclusively solving homicides which the police could not possibly understand. Every TV private investigator had a favorite Lieutenant or Sergeant who regularly shared private police information with him.

When the people in TV land saw that this was successful, they developed program after program based on their ideas of what a private investigator did for a living. We saw a single private investigator hero, married Private investigators, private investigator partnerships of two males, three females and even and "A Team" of paramilitary do-gooders. We saw investigators over every race, some of whom were very young and some of whom were very old, some who were crippled, blind and most recently, neurotic. Wire tapping, opening the mail, black bags jobs and even assaults by the investigator were commonly depicted.

The public changed their opinion of private investigators from a domestic snoop to the crime fighter who had no scruples and one who never let the law get in his way to enforce the law.

What we saw was private investigators solving the unsolvable, sometimes breaking the law of the land, but what we never saw was any one write a report, attempt to market the services to a client, testify in court or being held accountable for his many transgressions.

Many things have changed since 1953 including the mission of the licensed private investigator. Although domestic investigations occur, with no-fault laws, they become few and far between. Most private investigators would not know how to start a homicide investigation and no reasonable client could afford to pay for the time involved to properly developed the case, and make it suitable for prosecution.

It is difficult to make an overall general statement about all private investigators but it's safe to say that private investigators conduct those investigations that law enforcement has no time or interest in investigating. The bigger venues are conducting background investigations, criminal defense work, trademark protection, finding missing heirs, school residency investigations, accident and arson investigations and of course, insurance fraud investigations. The authors of the 1953 enabling act for the Commonwealth of Pennsylvania could not have imagined that in the intervening years, on the job description of the private investigator would change so dramatically.

It will be interesting to reflect upon how the job description of the private investigator will change in the next 50 years. Unfortunately the public still looks at the private investigator on TV land and never considers the meaningful work that we all do.

After Momma gave birth to twelve of us kids, we put her up on a pedestal. It was mostly to keep Daddy away from her.

Dolly Parton

DHS Announces Federal Regulations to Improve Worksite Enforcement and Asks Congress to Approve Social Security "No Match" Data Sharing

President Bush recently announced that the Federal government would make it easier for employers to verify employment eligibility and continue to hold them to account for the workers they hire. To that end, the Department of Homeland Security (DHS) announced today the release of two Federal regulations to help businesses comply with current legal hiring requirements intended to reduce the employment of unauthorized aliens.

The first proposal would permit U.S. businesses to digitize their I-9 employment forms, which are used to verify eligibility to work in the United States. The other proposed regulation would set forth guidance for U.S. businesses when handling no-match letters from the Social Security Administration (SSA) concerning submitted employee Social Security numbers or from DHS concerning documents submitted by employees during the I-9 process.

"Most businesses want to do the right thing when it comes to employing legal workers," said Homeland Security Secretary Michael Chertoff. "These new regulations will give U.S. businesses the necessary tools to increase the likelihood that they are employing workers consistent with our laws. They also help us to identify and prosecute employers who are blatantly abusing our immigration system."

Typically, when a worker's Social Security number does not match the worker's name on tax or employment eligibility documents, the Federal government sends out a "no-match" letter asking them to resolve the discrepancy. In fact, out of 250 million wage reports the Social Security Administration (SSA) receives each year, as many as ten percent belong to employees whose names don't match their Social Security numbers.

Employers have also expressed their frustration with being required to keep paper forms or to store the forms on microfilm or microfiche when all other aspects of their record-keeping have been computerized. The interim regulation would give employers the option to sign and store Forms I-9 electronically. It is expected that many employers will experience cost savings by storing these forms electronically rather than using conventional filing and storage methods. In addition, because of the automated way in which electronic forms are completed and retained, they are less likely to contain errors. Finally, electronically retained forms are more easily searchable, which is important for verification, quality assurance and inspection purposes.

The "no match" regulation reviews the legal obligations of an employer, under current immigration law, when the employer receives a no-match letter from the SSA or DHS. It also describes "safe-harbor" procedures for employers to use in dealing with such a letter. If followed in good faith, these procedures would provide certainty that DHS will not find, based on a receipt of a "no-match" letter, the employer in violation of their legal obligations.

These proposed regulations are now subject to a 60-day public comment period, although the I-9 regulation will become effective on an interim basis as soon as it is published.

As Congress continues to consider comprehensive immigration reform, DHS continues to urge them to increase the authority of the SSA to share information about Social Security "no match" letters with DHS worksite enforcement agents. This information would allow DHS to learn which employers had received "no match" letters from SSA. It also assists investigators in identifying companies with the highest rate of immigration fraud.

"Identifying businesses that are habitually flagged for submitting mismatched Social Security numbers would bolster our worksite enforcement efforts," added Secretary Chertoff. "Congressional approval of this legislation is critical to ensuring that U.S. businesses hire legal workers."

Chertoff also noted that fixing the problem of illegal immigration requires a comprehensive solution that must include a temporary worker program. A temporary worker program would replace illegal workers with lawful taxpayers, help us hold employers accountable, and let us know who is in our country and why they are here.