



**ÆGIS** journal

***Addressing threats that affect your bottom line***

Volume 14 Number 2, February 2011

From the case files of

**LUBRINCO**

<http://www.lubrinco.com/>  
**1-212-695-1759** and

**FE&E** CLARITY FROM COMPLEXITY  
Financial Examinations & Evaluations, Inc.

<http://www.feeinc.com/>  
**1-480-838-1728**

- 1. Asset Location and Due Diligence - Words vs. Deeds**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence - China turns it spy's on Business.**
- 3. Executive Protection - Egypt and the January ÆGIS Journal Issue.**
- 4. Technical Issues - Telecoms to Come Under AML Laws**
- 5. Real Stories from the Field - Fun with Security Codes and Cards**
- 6. Book and Product Reviews - February Snow Brings April Insurance Claims**
- 7. Subscription/Unsubscription/Copyright Information**

**Announcements:**

**Due Diligence for The Financial Professional – by L. Burke Files**  
**Now available at Aegis Journal and Amazon, 480 pages.**

[http://www.amazon.com/Diligence-Financial-Professional-Burke-Files/dp/0982372337/ref=sr\\_1\\_1?s=gateway&ie=UTF8&qid=1285712297&sr=8-1](http://www.amazon.com/Diligence-Financial-Professional-Burke-Files/dp/0982372337/ref=sr_1_1?s=gateway&ie=UTF8&qid=1285712297&sr=8-1)

**Offshore Alert Conference - April 4 - 6th, Miami Ritz Carlton**  
<http://www.offshorealertconference.com/2011/home.asp>

**Credit Card Fraud in Abu Dhabi on April 11th and 12th.**  
<http://www.pulsarft.com/upcoming-events.htm>

## **1. Asset Location and Due Diligence - Words vs. Deeds**

*“Words have no relation to action - otherwise what kind of diplomacy is it? Words are one thing: actions another. Good words are a mask for concealment of bad deeds. Sincere diplomacy is no more possible than dry water or wooden iron.”*

When assessing a company or a man data nothing can be more misleading than words. We are never better than when we are on paper, and we are never more convincing than when making a presentation.

I remember a recent conversation with an entrepreneur, as he recalled his big deals.

*It was going to be great, a real moneymaker, but someone with more money and clout stepped in.*

*It was all set up for sale and my partners dropped the ball.*

*I know I was a defendant, and I lost, it was just lucky lawyering on the other guy's part.*

I know this man, and he has made a lot of money over the years on many different projects, so when he asked for help, I took a look. As I did my homework on the entities he controlled, reviewing the decisions and errors that were made, they all landed right in his lap. Yet, despite overwhelming evidence, he still maintained that it was someone else's fault. Take two. I set him and his new project up with an audience. His presentation goes well and everybody's questions were answered. He gave a convincing presentation, including many facts, and he embellished by stating that he was the only person who could make this project work. He dwelled on compliance and accounting issues, and how everything had to be just right. But I knew there was a problem -- he hadn't filed personal tax returns in over ten years.

He kept repeating the need for compliance, compliance, and compliance – and he

never once added, oh, and by the way, I'm not compliant. A clear division between words and deeds.

The problem was twofold – his plan was a complex engineering project that required real management skills and multiple disciplines to pull off. A real management team was never assembled, and no help was recruited -- because the people he needed were too expensive, and he could do it himself. Maybe he *could* do both the work and the science himself -- but there are only so many days in a week, and he had filled all eleven of them. Thus, another forced split between words and deeds, over-promise and under-deliver.

I did help him, but from within the context of what I knew. I put together a proposal that included outside funding, external experts, additional management, and a review process. His answer to the proposal was "You're stealing my project from me." The assembled team and I sat in numb silence.

We failed to realize the fatal flaw from the beginning. His words and deeds were incongruent. Upon this realization, we should have stopped.

The quote at the beginning? V.I. Lenin

## **2. OPSEC, Economic Espionage, and Competitive Intelligence - China turns it spies on Business.**

If you have been reading the FT, WSJ, New Straits Times or The Standard, you will have noticed the comments of several business owners who are giving up on China – giving up altogether. Their comments might lead you to believe that their decisions involve human rights violations, the economy, or low cost labor available in other countries -- and you would be partially right, but there are substantial forces influencing these decisions that are not being reported.

China is incapable of, or unwilling to protect these corporations Intellectual Property and Critical Information (IPCI). The Chinese government has upped the ante, so to speak, to stay in the game. China has retasked methods used for military espionage to business purposes, and is now employing these methods on a grand scale. It is a full blown economic war. I know this is a strong statement, but it's also very accurate.

If you add the pressure of corporate espionage on top of China's structurally asymmetric rules for foreign firms, the negative affects of Chinese commercial espionage is weighing heavily in many firms decisions to leave, and is having a similar influence on other firms plans to relocate. In a candid moment, a functionary with the AmCham in China said "It is economically, more or less, impossible for companies to work and operate in China, particularly innovation firms, without the almost certainty of a complete compromise and loss of their IPCI," adding that, to his knowledge, not one of their members has ever made money in China. A potent point

made.

You will also read that many of the major innovative giants of the U.S. - like Google, Intel, Motorola, and AMD have experienced aggressive attacks on their networks, and these attacks all had a reasonable amount of success. It is all part of the Chinese government's stated goal of aiding Chinese-owned firms by using state power to cull information from a variety of sectors they deem valuable. The Chinese have made it very clear that they have a set of national commercial objectives and that those objectives will be promoted. Whether it is a state enterprise or simply one that has the favored status of the state -- it doesn't matter.

Many outsiders are simply sick and disgusted with the one-way economic attitude of the Chinese government, and their history of allowing foreign companies in and then aiding in the appropriation of their technologies for the benefit of domestic businesses. Many firms are allowed in for such a short period of time, all they experience is an opportunity to lose their competitive edge, educate their competition, and lose tens of millions of dollars before they are sent packing.

Why is it this bad? The Chinese government fears that the rebellions happening all over the middle-east may spread to their streets. Their desire for full employment is a high priority, and they are willing to do anything to achieve it. Unemployed people are restless and dangerous. There are regular demonstrations in China, but they are not covered in the news for fear that the coverage will foment further unrest. They've seen the contagion -- it has hit them in the face. Their monitoring of Internet and social media sites has taught them that many of the subjects do not like them one bit -- not one bit at all. Their response was censoring the web and the establishment of Internet "retraining camps".

Why do they target Western IP/C and technology? The idea of "property rights" is part of Western culture. It is so much a part of our culture that we forget to think about the fact that China is not a Western civilization. The idea of property rights goes back to Thomas Aquinas in *Summa Theologica*, Thomas Hobbes, James Harrington, John Locke, Pope Leo the XIII, David Hume, and even Karl Marx. Property rights are not part of their culture! Oh, I almost forgot to mention - they are still the world's largest communist nation. Their reasons to steal Western technology are twofold. China's current culture does not produce great innovators -- failure is shunned and even punished in Chinese culture. Innovation only occurs after a long string of "failures" (learning what does not work). The second reason is that we make stealing so unbelievably easy. There is no consequence for the theft of Western business models, patents, technologies, or customer lists.

How bad is it? How does China, within a period of thirty years, go from a period of isolation and technological stagnation to a nation with a space program and a stealth fighter? *Hint: Both look remarkably like U.S. spaceships and aircraft.*

How do we know that the Chinese are using state sponsored spy-craft to bolster the economics of their nation's business? First, the persistent attacks on commercial enterprises, both cyber attacks and traditional HumInt penetrations directed at

firms with little or no military value. Second, the UK's domestic intelligence service MI5 sent a letter to most of the major technology firms warning them of state-sponsored economic cyber espionage attacks coming from China.

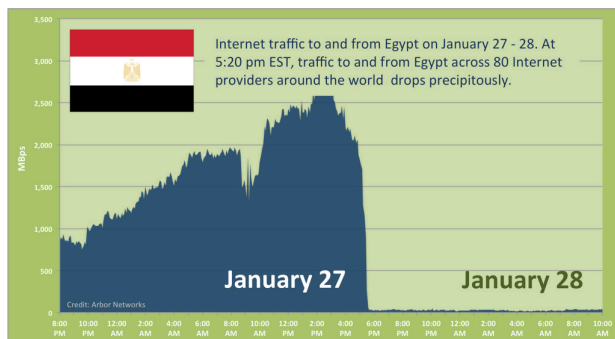
So what to do? It's really your choice.

We performed a vulnerability assessment for a company with offices and factories in China. The result was frightening -- but in reality, they were doing better than most at protecting information.

The CEO made some interesting decisions. As soon as he was aware that a manufacturing line was compromised, he fired everyone on the line and told them why. A competitor had stolen the technology from his factory and began producing cheaper. So sorry, no need to have you here – you're fired. They did not abandon the line or the market; they set up manufacturing in another country with lower wages. The terminations went all the way up the management chain, and affected the bonuses any retained employees received. While this action slowed the losses, it did not stem them. In the end, the decision was made that sensitive items were not to be manufactured in China, and there was no expansion of operations in China. Among the actions taken, all Chinese IP address (except those from his company) were blocked. The important lesson is to be aware of your vulnerabilities, not blind to them.

### 3. Executive Protection - Egypt and the January *ÆGIS* Journal Issue.

We warned you to be prepared last month, and now we have an example.



Government regulation and control of Internet and phone systems is a threat to open communications! When the government goes upside down, the people are in the streets, and you need *real* communication links more than ever -- you are toast. You must expect this. You and your charges are YOYO

(you're on your own). You have no web, no dial tone, no cell signal, international lines are cut, local lines are restricted, no twitter, and no texting. You're down to satellite phones, ham radios, and soup cans with string ...

If you are not prepared, you will have a few red-faced moments.

Info lifted from a wonderful Wired article.

<http://www.wired.com/threatlevel/2011/01/egypt-isp-shutdown>

And a follow-up article.

<http://www.wired.com/threatlevel/2011/01/egypt-isp-shuttered/>

#### **4. Technical Issues - Telecoms to Come Under AML Laws**

The World Bank has called for Central Bank regulation of telecommunication companies that offer money transfer and mobile banking services — a move that will raise customer charges owing to increased compliance costs. Increased cost should be no surprise. Telecom companies will, in classic form, pile whatever fees they can on the consumer – even if \$1 in cost only prevents \$.05 in fraud.

Mobile technology offers an opportunity for an estimated three billion low-income earners to gain access to financial services -- primarily in Africa and Asia. The World Bank says that the line differentiating financial providers in banking, telecom, credit card, and mobile commerce has become increasingly blurred -- yet no robust regulations to guard against money laundering have been passed.

“Distinctive risks concern observers in affected service markets,” said the World Bank. “These perceptions merit urgent attention because mobile financial service providers may fall outside anti-money laundering and combating the financing of terrorism controls generally adhered to by traditional financial institutions.” Huh?

The transactions being handled, for a large part, are small transactions. Among the big players behind the scene are banks, once again being disintermediated in the payment process because of their cost structure. The reason for the popularity of mobile payment systems is that the cost of a transaction is very low -- when the cost of transactions goes down, opportunities appear and volume goes up. It appears to me banks do not understand that the transactions micro-payments replace are currently being serviced in the local cash economy, because people who use these systems are not banked, and are not likely to be banked.

Mobile phone operators are not banks -- they are in the business of communications, and the small segment of the market represented by mobile payment systems are nothing more than a differentiating feature providers want to offer their clients. It's a simple way to store a few dollars and settle transactions through a trusted channel.

Banks would like to limit consumer's options, and whatever costs these limitations impose, will be borne by consumers ... as always.

#### **5. Real Stories from the Field - Fun with Security Codes and Cards**

One of the investigators with our group likes to eat, but he doesn't like to cook. He's a delivery or takeout type of guy. He was recounting a story when on a particularly

cold day in Phoenix (45 degrees) he thought it best to order in. When he called for the Chinese food delivery, he offered to give the delivery driver the pin number for the gate, so that the driver could enter without calling. The delivery driver stated, in a polite but dismissive tone, that he didn't need to call, as he had the universal code for the fire department, and that he could go in and out of any complex as he needed.

Traveling to yet another fair city, I picked up my trusty rental car and charge off in an unknown maze of freeways and by-ways. I spent three days working in the fair city, and then headed back to the airport rental car return. Being a child of depression era parents, I always top off the tank myself. I spotted a gas station, pulled in and then began the "find the filler cover release Macarena". While executing the moves with some sense of style, I found a "gate key" card that I assumed was left by a previous renter. I put the card in my pocket with the full intent of turning it in at the counter. I arrived at the airport, and was literally handed a receipt for the car within 20 seconds -- and forgot about the card. Back at home, it rode around in my backpack for months. When chauffeuring some of the offspring to a party at their friend's home, I was required to have the invitation that contained the gate key code -- right, that's back at the house. Calling the house, neither the nine year old, my wife, or the dog could find the invite. Then, in a moment of both desperation and curiosity -- I remembered the gate card key in the backpack, placed it in the slot, and viola! The gate opened. This was cool. I continue to use the gate key with great fanfare, especially with impressionable kids in the car, since this is exactly what an investigator should have -- a magic gate key. It works in most every residential community gate I have tried.

I asked a security professional, "What's the magic?" She told me it is one of two errors. It is a master key lost by a security company, or more likely, looking at the key it contained not just the master program, but also the local complex's key program. Same problem with the pin code for gate access. It seems that for several companies, the default and master key are the same. For a secure system, the default is for "boot up" and should require that a new master code be installed. Either way, I am keeping it and will continue to deploy the card (and now the pin code since I have that too) -- always with great fanfare when I deliver my charges to their festivities.

As for our family, we do not live in a gated community, and frankly, I don't think many of them would have us.

*Note to security people: remove default settings, create a new master code, and to one in particular -- thank you for the card. I will use it for good and not evil.*

## **6. Book and Product Reviews - February Snow Brings April Insurance Claims**

There are several forecasts predicting severe flooding for the central Midwest and east. The snow has fallen and has not melted, thus no gradual dispersion of water.

All prediction are for an early spring and a rapid melt off of the winter snows. Floods are the deadliest weather phenomena in the U.S. — claiming an average of 100 lives annually. Many of these deaths occur in automobiles and are preventable. If confronted with a water-covered road on foot or in an automobile, play it safe. Floods are also the most disruptive for business continuity issues.

[http://www.noaaneews.noaa.gov/stories2010/20100316\\_springoutlook.html](http://www.noaaneews.noaa.gov/stories2010/20100316_springoutlook.html)

<http://water.weather.gov/ahps/index.php?stage=2>

## **7. Subscription/Unsubscription/Copyright Information**

•• ÆGIS is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2011 by The Aegis Journal, LLC. It is edited jointly by L. Burke Files ([LBFiles@feeinc.com](mailto:LBFiles@feeinc.com)), Gregg Lowney ([greg@feeinc.com](mailto:greg@feeinc.com)) and Shaun Hassett ([SHassett@lubrinco.com](mailto:SHassett@lubrinco.com)).

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

- **International asset location and due diligence.**
- **Anti-money laundering, financial fraud, and anti-corruption program development and training.**
- **Risk Assessment and statutorily mandated AML independent examinations and program reviews for financial institutions and gatekeepers.**
- **Investigation and location of missing or concealed assets, related to fraud, theft, and divorce.**
- **Due Diligence to prevent fraud and loss, as well as validate potential business partners, counterparties or potential business acquisition or merger targets. LUBRINCO has significant expertise in performing Due Diligence in China, Central and Eastern Europe, Central and Southern Asia, the offshore financial centers, Latin America, and the Caribbean.**
- **Identification, valuation, and protection of intellectual assets and critical information.**
- **American businesses lose more than \$300 billion in revenues annually to competitive intelligence, economic espionage, inappropriate disclosure, and information theft.**
- **LUBRINCO provides private sector consulting access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information.**
- **Implementing an OPSEC program is likely to increase revenues for an at-risk operating group by \$75 million.**
- **Protection of executive management, staff, and families.**
- **In the high-threat environments of Latin America, Africa, the Mid-East, and**

## **Southeast Asia.**

- **When traveling or living overseas**
- **When transporting items of substantial value.**

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

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

Subscription to **ÆGIS** is available for \$15 per year in North America and \$25 per year outside of North America.

To sign up to receive a **complimentary subscription** to **ÆGIS** or the **ÆGIS** PDF notification list, send an email to [subscribe@aegisjournal.com](mailto:subscribe@aegisjournal.com).

To be removed from the subscription list, send an e-mail to [unsubscribe@aegisjournal.com](mailto:unsubscribe@aegisjournal.com).

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

If there is a topic that you would like to know more about, please send your request to [editor@aegisjournal.com](mailto:editor@aegisjournal.com) and the editors will consider it as the topic for an article in an upcoming issue.

### ***We welcome readers who wish to submit a short article for publication in ÆGIS:***

If you would like to submit an article for publication in **ÆGIS**, please send it as an attachment to an e-mail to [editor@aegisjournal.com](mailto:editor@aegisjournal.com).

Submission of an article for publishing consideration certifies that:

(a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted.

The submission of materials for publication in **ÆGIS** constitutes a license to **LUBRINCO**, and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

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

**ÆGIS** is a forum for the exchange of information, ideas, operating styles, theories,

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

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

Please be safe, and be smart.