



**ÆGIS** journal

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

Volume 9 Number 5, May 2006

From the case files of

**LUBRINCO**

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

and

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

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

**Business in Bogotá or other high-threat areas? Call us!**

**This month's features:**

• **Special Announcement**

- 1. Asset Location and Due Diligence — Gaming the system using customer complaints**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — How Usama bin Laden made the world safe for spies**
- 3. Executive Protection — Decapitation *à la* America: How China might invade Taiwan**
- 4. Technical Issues — Nokia 6270**
- 5. Real Stories from the Field — Who might live in a pandemic**
- 6. Book and Product Reviews — *The Law and Economics of Cybersecurity***
- 7. Subscription/Unsubscription/Copyright Information**

## **1. Asset Location and Due Diligence — Gaming the system using customer complaints**

A company that specialized in motivation and life skill training had had over 15,000 student / customers since it was founded many years ago. The program averaged about one or two refunds per year, and no civil complaints to the state Attorney General's office. In 2005 they noticed an abrupt upswing in refund requests, and over 80 complaints were sent to the Attorney General's office in their state. The business model had not changed, and the same people were running the business the same way they always had. They were at a loss to describe what was happening.

Having misunderstood what was actually happening, they approached (with counsel) the AG office and quite rightly voiced the opinion that 80 complaints from 15,000 students/ customers was not an unreasonable amount, just over one half of one percent. While this seemed reasonable from a statistical perspective, the AG's office decided to pursue the claims. Their attorney suggested that they just refund the money, so they did. Inexplicably, this seemed to accelerate the number of refund requests, rather than solving the problem, as if they were adding gasoline to a fire.

One afternoon a senior manager for the company's IT group was running the normal searches on the Internet to make sure that the money they were spending on certain search terms was in fact in place. What he found was a "paid for" advertisement on Google that came up when you searched for the name of his company. The ad very clearly bad-mouthed the company, and gave specific instruction on how to demand a refund, and how to file a complaint with that state's AG's office.

The first thought was to look for the location of the advertiser, but they were well camouflaged. The second was to call Google to see what the heck they were doing allowing something like that to occur. They got it right with Google, and learned that the ads were being paid for by one of the company's competitors in another county.

Back at the AG's office, even the new fledging attorney handling the case wondered why all of the complaints looked the same. Nonetheless, it was an easy win, so he moved forward toward an enforcement action. In the end the client paid both the AG's office a fine and the actually-satisfied-with-the-

program customers their refunds. This added up to several hundreds of thousands of dollars.

So let's recap what happened. A cunning competitor purchased an adword (a word or phrase that would point to your Web site in a search), designed to show up each time the victim company's name was searched, that told how to get refunds from the company and file complaints with an AG's office. The AG took the bait, and even knowing something was wrong, effectively enacted a state-sponsored class action suit against the company.

When asked what would have happened if the company were not based in his county, the AG said there would have been nothing his office could have done. Being no fools, the victim company let go over 200 employees, and moved its headquarters offshore.

This story is an interesting illustration of a competitive strategy: gaming the system, and the system responding mindlessly. The competitor won a small victory. The AG won a hollow victory. Two hundred jobs left the US in one week, not because of raw economics, but to avoid economic victimization by the state.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — How Usama bin Laden made the world safe for spies**

For a brief period of time after the Cold War ended it looked as if some effort would be put forth to address economic espionage. This was not because economic espionage represented a real threat to American business (which it did), or because lack of a common enemy (Russia) emboldened us to confront our allies who were targeting our economic interests (which they were), or even because the end of the Cold War had allowed foreign intelligence collection agencies to shift from military intelligence to economic intelligence (which it had). Rather, it was because, with the Cold War over, and with no Russian enemy, we had to either find something for our intelligence and counterintelligence people to do, or send them home.

During this heady period, we saw the passage of the Economic Espionage Act of 1996, and a commitment on the part of a number of federal law enforcement agencies to address this \$300 billion dollar annual drain on American industry. It was, however, even then clear that nobody's heart was in it. After all, it seemed something of a comedown to go from stopping the Red Menace to protecting Avery Dennison's stickum. Nonetheless, resources were moved to begin, however grudgingly, to seriously address what was then – and is now – a serious threat.

Unfortunately for American business interests, the world of intelligence went back to normal on 11 September 2001. With the fall of the Twin Towers, which we had the misfortune to watch out of our office window, there was an immediate refocusing of our national intelligence and law enforcement efforts away from economic espionage.

Thus, Usama bin Laden single handedly eliminated the emphasis on dealing with economic espionage, and made the world again safe for spies.

We race to point out, however, that while the intelligence and law enforcement communities may have lost interest in economic espionage, the SEC, which understands the implications of our \$300 billion annual loss, has not lost sight of the threat to American industry.

Thus, you still have an explicit responsibility under Sarbanes-Oxley to have internal controls in place to track, account for, and deal with losses from economic espionage, competitive intelligence, and theft.

### **3. Executive Protection — Decapitation *à la* America: How China might invade Taiwan**

**Max Hirsch** ([hirsch@taipeitimes.com](mailto:hirsch@taipeitimes.com)) is 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 specializes in kidnap victim recovery. Contributed articles do not necessarily reflect the viewpoint of AEGIS.

#### ***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 E.U. (trade disputes and the usual diplomatic spats notwithstanding).<sup>1</sup> 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.<sup>2</sup>

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.<sup>3</sup> 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).<sup>4</sup> 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

---

<sup>1</sup> China's Foreign Minister Li Zhaoxing commented on March 7<sup>th</sup> 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.)

<sup>2</sup> See my last AEGIS 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.

<sup>3</sup> 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.

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

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.<sup>5</sup> (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,<sup>6</sup> 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.

---

<sup>5</sup> Bishop, Mac William (29 May 2005). “Japan to station advanced fighters on Okinawa.” Taipei Times, front page.

<sup>6</sup> 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.

In light of recent tensions and China's military buildup,<sup>7</sup> 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?<sup>8</sup>

### **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 their technological capabilities.<sup>9</sup> Given that the PLA is actively internalizing

---

<sup>7</sup> 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).

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

<sup>9</sup> Shambaugh discusses 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).

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*.<sup>10</sup> 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.<sup>11</sup>

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

---

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 attaché 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>.

<sup>10</sup> 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.

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

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.<sup>12</sup>

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 *à la* America deliver China into a quagmire *à 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

---

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

fervor; it is difficult to imagine the PLA meeting much resistance from the citizenry north of the Choshui River.<sup>13</sup> 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<sup>14</sup> 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.<sup>15</sup>

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

---

<sup>13</sup> 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-unification 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>).

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

<sup>15</sup> 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.

taught in textbooks that their “sovereignty” includes three million square kilometers of oceans and seas...<sup>16</sup>

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...<sup>17</sup>

The idea behind these maritime forays seems to be to conduct hydrographic/oceanographic surveys to map the ocean floor and pinpoint certain thermal

---

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

<sup>17</sup> 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>).

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 the case on the Muzha Line and the Danshui Line from its Minquan East Road stop to the Danshui stop), 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. Neihu District, where numerous high-tech companies are based, would also be especially vulnerable. This is because Taiwan’s “NORAD” is located somewhere in the mountains adjacent to the district. The command center would be a prime target in a first-wave attack by China.

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 (<https://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.

#### **4. Technical Issues — Nokia 6270**

On 31 July 2001 the first GSM 850 call was made, and soon a number of countries in the Western hemisphere (Antigua & Barbuda, Argentina, Cayman Islands, Colombia, Dominica, Ecuador, Grenada, Montserrat, Panama, Paraguay, St Kitts & Nevis, St Lucia, St Vincent & The Grenadines, and, most recently, Canada and the United States) implemented 850 MHz GSM systems. In five of these countries, GSM 850 is the only frequency available. The addition of GSM 850 rendered 900/1800/1900 handsets obsolete as worldphones, and most definitely as worldphones for use in the Americas: Now you need 850/900/1800/1900.

Half a decade after tri-band terminals became obsolete, three years after NEC introduced its 515 quad-band GSM handset, and two years after Motorola introduced its V600 quad-band GSM handset, Nokia has finally introduced a quad-band handset: Their model 6270.

First the bad news.

- The handset is not aimed at the international business traveler, who, experience has taught us, cannot carry a camera phone.<sup>18</sup> While there is a lot of virtue to widespread availability of cameras in every form – we urge you to go to <http://www.witness.org/> to see what can be done for the common good with cameras – cameraphones are simply not a good fit for business travelers. We therefore consider that a handset appropriate for international business travelers must minimally be a camera-free quad-band device.
- The 6270 sells for between \$300 and \$450 on eBay, which is a lot of money if your goal is to make phone calls. We would guess from its feature set (camera, flash, video, stereo speakers, MP3 player, FM radio...) that it is aimed at the affluent teen and college market.
- While the user interface on the 6270 is as good as we have come to expect from Nokia, the device we tested was unable to hold a signal when walking between the Ninth and Tenth avenue entrances in the Port

---

<sup>18</sup> When we tested the Motorola V-600 cameraphone, it was vouchered 11 times in the fortnight we had it: We had to carry a second handset with us and switch the SIM when this happened.

Authority Bus Terminal here in Gotham (our highly-standardized and very accurate albeit non-scientific test of real-world RF ability).

- No American service provider – at least at the time we write this – is planning to carry the 6270.
- It has a SAR of 0.74 (we prefer it to be under 0.5).

Now the good news!

The good news is not the 6270 itself. It is, rather, that the 6270 demonstrates that Nokia is finally moving into the quad-band world. For those who prefer the Nokia user interface (which we prefer above all others), this hopefully this means that they will, in the near future, run through their supply of outdated tri-band chipsets, and start producing quad-band terminals instead.

Nokia has, in the past, produced some of the world's best GSM handsets. The 6150, the 6190, and the 8310 all come to mind. For the business traveler, the Nokia 6310i handset (arguably among the best GSM terminals ever made) was flawed only by the puzzling lack of the 850 MHz band. The 6310i had good RF, the great Nokia user interface, the very useful wallet feature (which allowed you to store information with password protection), Bluetooth, IR, wonderful use of internal memory, and a great selection of batteries. Indeed, the 6310i is so well thought of that it still sells on eBay, outdated as it be, for up to \$250. While we will never see a quad-band version of the 6310i (they have long abandoned that form factor), we hope that at some point in the near future Nokia will again have its design staff address the needs of the international business traveler.

## **5. Real Stories from the Field —Who might live in a pandemic**

A lot of odd things happen within humanity. For example, if you have direct forebears who had the plague and survived, you likely inherited a strand of DNA which makes you virtually immune to AIDS.

While an interesting factoid, what does this have to do with a pandemic? In order to understand this, you have to understand how an influenza pandemic differs from normal flu. In an average year roughly 36,000 Americans die of the flu, and roughly 200,000 Americans are hospitalized because of the flu. Most of those who die are the young, the old, and the infirm, whose immune systems are too weak to mobilize to fight the virus.

Death in a pandemic is different. In a pandemic the majority of those who die are the healthy, not the less-healthy. Why is this? Because in a pandemic your body looks at the unfamiliar virus, realizes it doesn't know how to deal

with it, and throws every defense it can muster at dealing with it. If you die from your lungs filling with liquid, it is your immune system that has killed you, not the virus.

But what happens if your immune system is weak from being young, or old, or from an immune system disease such as AIDS? It is posited that people with deficient immune systems may die from the flu in roughly the same numbers as if it were not a pandemic. Those who are healthy, however, and who would normally recover, are likely to die during a pandemic, and to die at a much higher rate.

We like to think that there will be no influenza pandemic.

Failing that, we like to think that there will be a flu shot available that will help ameliorate the effect of any pandemic. We know that, even with 65,000 dead from flu in a normal year, vaccines are not a high priority, but in FY 2006, the President announced an emergency budget request of \$7.1 billion, of which \$6.7 billion was for HHS pandemic influenza activities. The goals are to:

- Produce a course of pandemic influenza vaccine for every American within six months of an outbreak;
- Provide enough antiviral drugs and other medical supplies to treat 25 percent of the U.S. population; and
- Ensure a domestic and international public health capacity to detect and respond to a potential pandemic.

While not tied to the \$7.1 billion request, a collateral goal was to stockpile enough pre-pandemic influenza vaccine for 20 million persons.

Failing that, we like to think that medicine has progressed enough in the last century that our public health infrastructure will be able to handle a pandemic.

## **6. Book and Product Reviews**

*The Law and Economics of Cybersecurity*

Edited by Mark F. Grady and Francesco Parisi

Cambridge University Press ISBN 0-521-85527-6 320 pages \$75

<http://www.cambridge.org/catalogue/catalogue.asp?isbn=0521855276>

The book contains the following eight very thoughtful papers about computer security in a networked environment. And let's face it if you are connected to the Internet, you're in a networked environment.

1. Private versus social incentives in cybersecurity, law and economics  
Bruce K. Kobayashi
2. A model for when disclosure helps security: what is different about  
computer and network security? by Peter Swire
3. Peer production of survivable critical infrastructures by Yochai Benkler
4. Cyber security: of heterogeneity and autarchy by Randal C. Picker
5. Network responses to network threats: the evolution into private  
cyber-security associations by Amitai Aviram
6. The dark side of private ordering for cybersecurity by Neal K. Katyal
7. Holding Internet Service Providers accountable, Doug Lichtman and  
Eric P. Posner
8. Global cyberterrorism, jurisdiction, and international organization by  
Joel T. Trachtman.

Not one of the papers offers the solution, but, rather, engages the reader in some very thought provoking exercises and what might work depending upon the different environments and the users' different incentives. For example the type of security features, even the choice between open sources and proprietary security features, can very much depend upon the environment in which you operate. For example, most of us out surfing the Web have found that known suppliers and methods of protecting ourselves against mischief has been the best way. Why? It is tried, tested, and fixed as a result of the shear volume of security breach attempts, past success, and re-engineered defense after a method of breaching the security has been found. However, operating in a military environment, this manner of testing your security and sharing with the world your success and failures may not be as prudent. Based upon the user's environment, the papers dissect in economic terms tradeoffs in security, regulation, and punishment to deal with the complex issues of choosing an optimal collection of models for private and public sector applications and environments.

There are two shortcomings to the book. One regrettable feature is the manner in which several of the papers deal with crime. We, having worked against criminals, studied criminals, and spent *way* too much time with criminals. Our empirical knowledge tells us that the lens or filter used to deal with the economics of criminal behavior over the internet is naive. The second shortcoming, which we hope the editors will contemplate (we are encouraging this) is the need for a shorter edition of the book in layman's terms. While the editors of *ÆGIS* are collectively well versed in programming,

math, models, and econometrics, the book reviewed presents sufficiently relevant information that it should be shared with those less conversant.

Valuable information? Yes. Worth the \$75.00? Yes.

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

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2006 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@feeinc.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.

- **Sarbanes-Oxley Section 404 OPSEC compliance.**
  1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
  2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, and information theft.
    - LUBRINCO provides private sector access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, and information theft.
- **International asset location and due diligence.**
  - Location of concealed assets in fraud, theft, and divorce.
  - Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, the Caribbean.
  - Financial fraud and anti-money laundering program development and training for compliance with the US *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the EU *Revised Money Laundering Directive of 2001*.
- **Protection of management, staff, and families.**
  - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
  - When traveling and living overseas.

- When transporting items of substantial value.

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

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

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

To sign up for a **complimentary subscription** to **ÆGIS** or the **ÆGIS** PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to [aegis@lubrinco.com](mailto:aegis@lubrinco.com).

To subscribe to our AvantGo channel, go to [http://avantgo.com/channels/\\_add\\_channel.pl?cha\\_id=1773](http://avantgo.com/channels/_add_channel.pl?cha_id=1773)

To be removed from the subscription list, follow the instructions on the mailing you received, or send an e-mail to [aegis@lubrinco.com](mailto:aegis@lubrinco.com).

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

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

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

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

*Article Title*, from the May 2006 **ÆGIS** (© 2006 **LUBRINCO** & FEE), to be found at <http://www.lubrinco.com/>.

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

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

Please be safe, and be smart.