



**NCIX**  
NATIONAL COUNTERINTELLIGENCE EXECUTIVE

---

**THE AFCEA COUNTERINTELLIGENCE CONFERENCE**

**Sunnyvale, CA**

**December 4, 2007**

**Remarks by Joel F. Brenner**

**National Counterintelligence Executive**

***“Counterintelligence in the 21<sup>st</sup> Century:  
Not Just a Government Problem”***

[Acknowledgments]

Globalization is a fact of life in the twenty-first century. But you know that already. So what I’m going to talk about is how the fact of globalization and the speed of communication are affecting the intelligence business in general and counterintelligence in particular. And by “counterintelligence” I mean something much broader than traditional espionage against governments. Nowadays counterintelligence is no longer a government problem. It’s a problem for any firm that has valuable secrets to keep, regardless of whether those secrets may be classified. And

it's a problem for any business that uses electronic communications devices – which means every business, all the time.

We now live in a world in which the United States can no longer assume it has a qualitative technological advantage over friends and adversaries. The world has gotten flatter – a lot flatter. Moreover, the dirty world of stolen information has become increasingly economically rational. Thieves who were incapable of exploiting information they knew how to steal have now figured out how to sell it. There's a robust market for your secrets, and the sellers in that market include amateur hackers, criminal syndicates, and foreign intelligence services.

In the past 20-or-so years the economies of the advanced industrialized nations have enjoyed astonishing productivity advances based on the rapid deployment of fast-moving information technology. Those advances have greatly outweighed the cost of the vulnerabilities that technology has created. That balance is changing, and I believe that we are approaching the point when the actual, incurred cost of the vulnerabilities, and the risk of still greater losses, will be unacceptable to government and private firms

alike. It is therefore time we got our houses in order – all of us, government and private sector alike.

### Behavior

The challenges we face are both technological and behavioral, and between these two, the more difficult is behavior. We Americans like our convenience; we're accustomed to instant gratification. We have driven our technology to do many things more easily, cheaper, and faster, but our impatience is often our Achilles Heel. I know of a case in which a guy (a contract employee, by the way) nearly brought down an entire intelligence agency's unclassified systems when he decided he was too smart to use the equipment issued to him; it was too slow, he thought; he had better stuff at home, he thought. So he brought it in and hooked it up to the agency's network. And what do you know? It was infected. Straightening that out cost millions in real dollars, and more millions in lost productivity.

A few weeks ago I learned of another smart guy who, after taking his PDA to a foreign country well known for cyber intrusions, synched it up to his firm's networks. This is actually normal behavior, but given who he was and the

country he was in, the risk that he has infected his agency's servers with a "phone home" vulnerability approaches 100%. But gosh, not being able to synch your personal calendar and contacts with your office systems is a real pain in the neck... By the way, the first guy was a relatively low level contract employee. The second was the CEO of his company. If we want to manage this problem, we can't just point fingers downward. We have to look in the mirror.

Persuading even well-educated people that real vulnerabilities exist when they can't see them, and when avoiding the vulnerabilities is inconvenient, is like trying to persuade uneducated peasants about the reality of microbes. Can't seem 'em? Then they don't exist.

When convenience butts heads with security, convenience wins – hands down, every time. And when you add stupidity, malice, and carelessness to the mix – and I'm afraid we find those qualities in some measure in every organization, public or private -- you have the makings of serious IT management problems.

If you want to make your self less vulnerable to identity theft, you need to choose strong passwords, keep them secret, and change them periodically. You also need to encrypt what's on your computer, apply software patches as soon as they become available, install strong firewalls, and so forth. How many of you do that?

You don't have to raise your hands. We already know the answer: always much less than half the audience.

Businesses and governments have to do these same things — only more of them and at industrial strength — and our record, and their record, are mixed at best, to put it mildly. We don't manage our systems and the people who use them as well as we could, and we don't do it consistently. We need to change that. This includes patch management — which must be automated to be effective — and monitoring bad behavior on our systems.

### Cyber Attack Warning

When it comes to external threats from remote attacks, I will tell you frankly that we in government can do a better job of helping you handle cyber vulnerabilities through a

better warning system. Specifically, our rules for what we can tell you (our “cooperation model,” if I may put it that way) is a function of our classification model. That is, if you’re doing classified work, we can provide you with information about actual or potential attacks on your system that we generally have not been willing to provide if you’re not working on a classified contract. The problem with this cooperation model is that it assumes that the criticality of your systems depends on whether you’re doing classified work – which generally means defense-intelligence work. This assumption is antiquated. So we are re-thinking it.

The Critical Infrastructures Protection Act of 2001 defines “critical infrastructure” to mean “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”<sup>1</sup> And the Homeland Security Act of 2002 defines “key resource” to mean “publicly or privately controlled resources essential to the minimal

---

<sup>1</sup> 42 USC § 5195c(e).

operations of the economy and government.”<sup>2</sup> These definitions have nothing to do with the system for classifying information – nor should they. So we’ve got work to do here.

### Acquisition Risk

When I came into my current job about 15 months ago, I quickly identified two new counterintelligence risks. One of them was the cyber network vulnerabilities I’ve been talking about. The other was acquisition risk.

Businesses and government, including intelligence agencies, buy communications and other equipment in the open international market. What are we buying? What does “Made in USA” mean when components come from overseas and the software in the electronics may have been written by God-only-knows-whom? Unknown or sketchy provenance raises the risk that a foreign government or organization could program vulnerabilities into our most sensitive information systems. This risk is not a fantasy of an over-active imagination, but it is extremely difficult to police, because finding an intentionally inserted line of malicious code in a million lines of code is nearly impossible.

---

<sup>2</sup> 6 USC § 101(10).

So we look at where the stuff comes from. We are putting more resources against this problem, and we are getting much more rigorous in our analytic approach to it. It may be appropriate that different agencies or businesses have different tolerances for acquisition risk, but it is not appropriate that, under the guise of managing risk, we kid ourselves about what the risk really is. Risk management is not risk acceptance. Which is why we must employ a consistent risk assessment methodology across the intelligence community and, eventually across the entire federal government.

Doing rigorous and consistent analysis is only part of the problem, however. Behavior is again the problem.

Let me share with you the unfortunate case of a well-known US company negotiating a contract in a country I won't name but which is on the other side of the Pacific Ocean and is growing very fast and has a lot of people in it. And the executives of this American company realize in mid-negotiation that their counterparts know their bottom line positions on every issue on the table. They also realize that the only way this could have happened is that host-country

operators have hacked into the firm's networks and exfiltrated their negotiating secrets.

This could have happened in lots of ways: by sophisticated remote attack, whether or not aided by an insider; through use of a thumb drive to download the contents of a laptop while going through customs, or during the surreptitious entry into a hotel room; or through a bug inserted into a PDA while passing through an airport.

Countering the risk of penetration of cell phones and PDAs would be worth our discussing later this morning. For the moment, let me just say that if you do not understand that this is the environment you live in, you are asking to have your company electronically undressed. These devices are controlled by software. Anything done in software can be undone in software. And these changes can be done remotely, on the fly, in an instant. Of course, if you're Aunt Nellie in Dubuque, you're probably nobody's target and probably have nothing to worry about. But as senior executives of major firms doing business with the federal government, you're not Aunt Nellie. You're targets.

## The Beijing Olympics

In August next year, thousands of American businessmen will descend on the People's Republic of China for the Summer Olympic Games and conduct their business affairs just as if they were sitting in Sunnyvale or Baltimore. Of course, for most companies, China is a great place to do business. It's a place where you're welcome and where you can get returns on investment of 20% - 50%. That's some sort of paradise, right? And it's interesting too. But while you are making money, you need to know that in many cases you are in danger of having your pockets picked of your intellectual property. Foreign intelligence services from all over the world will be operating there.

An acquaintance of mine whose business is communications security for large financial firms counted five beacons popped into his PDA between the time he got off his plane in Beijing and the time he got to his hotel room.

The danger here is not merely that information on your device can be stripped out. The more serious danger is that your device will be corrupted with malicious software that takes only a second or two to download – and you will not

know it – and that can be transferred to your home server when you collect your email. Phones are easy to deal with. If you take one to a hostile environment, take a throw-away and know you are communicating in the open. Wireless privacy is an oxymoron; there's no such thing. You just have to understand that. But PDAs are harder to deal with because the damage is likely to be done while you are there. Ultimately, firms can probably manage this risk only through a solution that involves their server architecture. You figure out what secrets you really can't afford to lose, and you just do not permit them to be communicated through the same server that handles your ordinary communications.

### Global Trends

Beyond the Olympics, there are longer term global trends affecting the intelligence community which I would like to discuss, because inevitably they will also affect those of you that contract with us. There are two trends underway in the business world that will affect the way intelligence practitioners work in the future. They are not specific to counterintelligence, but they are bound to affect us along with the rest of the community. One relates to the “unbundling” of activities that were bundled or aggregated

earlier in our history. The other involves the “disintermediation” of activities, how goods and services are more directly delivered today than in times past. These are two big waves that the intelligence community has mostly ducked – *so far*.

“Unbundling” means separating once-aggregated activities into separately priced components. Think back to the way telephone service was delivered before the late 1970s when the Bell System was broken up. There was one phone company, and that company sold you equipment, wiring and installation services, local phone service, and long distance service too. When that cozy world fell apart, it was a big nuisance for consumers. People had to make choices and didn’t always like it. “Telephone service,” conceived as a unitary product, got unbundled, and suddenly we bought different pieces of it from different firms. The benefits of the resulting competition have been dramatic, and without that competition, we would not have had the telecommunications explosion of the last few decades – or rather, the US would not have led that explosion.

We could multiply examples: hospital care, banking, energy generation and transmission, and so on. Unbundling pushes competition (and therefore efficiency) deeper into the economy. It would not surprise me if some of the several distinct parts of the business of intelligence got unbundled too, particularly on the analytic side. In fact, it would surprise me if this did not happen.

“Disintermediation” means taking the middle man out of the market. You want shoes? You don’t have to visit the shoe store any more. You can buy them online. The same goes for clothes, financial securities, books, automobiles, and lots of other products. Electronic transactions are displacing specialized brokers in the financial services industry. In news delivery, there is a proliferation of sources of unfiltered information, blurring the very definition of journalist. You want information? Who needs a newspaper anymore? (I think I do, but plummeting circulations tell us that lots of people don’t. And as for me, I don’t need the *whole* newspaper; I can pick and choose pieces from this one or that one, and I do.)

This trend is bound to affect intelligence – again, particularly on the analytic side.

Who's the middle man in the delivery of intelligence to policy makers? Analysts. What's the difference between an analyst and a journalist or editor? Why should we think that the market and social forces that are transforming journalism will leave intelligence analysis alone? They won't. The role of "finished" intelligence has begun to diminish as analytic and other intelligence activities are disaggregated and provided more directly to consumers. Look at the internet and you can see the world moving toward raw intelligence and away from established or finished intelligence products.

The world is also moving toward *private* intelligence. The corporate world creates, commissions, and buying intelligence analysis to a degree that would surprise many of our colleagues. And one reason they can do it is that governments no longer have a monopoly on world-class collection vehicles, like satellites, and world-class communications equipment. On a long historical view, beyond the last century, private intelligence is not new. In 1815, the best intelligence on the results of the Battle of

Waterloo belonged to the Rothschilds – a system of beacons from Belgium, across the Channel, up to London. That's how they learned of Napoleon's defeat before anybody else, including the government, and made a fortune on Consols (the British equivalents of Treasuries).

The pressure on collection will be slightly different. If you're on a watch floor and you learn from a secret source about a sudden event in, say, Kabul, and then 25 minutes later a report of that event appears on CNN, how many tens of millions are you willing to pay for that secret source? A rational answer should depend on two factors: (1) The dependability of open sources, and (2) whether you can do something significant with the information in the 25 minutes before everyone else knows about it (as Rothschild did). To an increasing degree, I suspect we are going to be unwilling to make that investment. But whether we do or not, I predict that in the future, the critical factor in more and more (though not all!) situations will be speed rather than secrecy.

This will sound strange to those of us in intelligence that spend much of their time dealing with truly, deeply secret material. So don't misunderstand me. There is always

going to be secret material. What I'm saying is that less and less will be secret and that much of it won't stay secret for very long, and that the speed at which information is moved and acted on will be the coin of the realm.

Unbundling and disintermediation are happening whether we like it or not, and these forces will shape the future. The conversation about the right use of the private sector by the intelligence agencies will continue. Adjustments will be made from time to time. But in my view, the relationship is destined to become stronger, not weaker, because we cannot do without your brains and your agility. Managing you, on the other hand, won't get any easier.

Let's leave it at that and start a conversation. I'd very much like to know what's on your minds.