

# CSI Roundtable: Information Warfare

*The following remarks were excerpted from a panel discussion at CSI's 25th Annual Conference, November 2-4, 1998, in Chicago, Illinois.*

**Richard Power, CSI:** Let me introduce our panel. They all have real-world experience in the information warfare arena.

Lawrence Dietz is Director of Information Security and Legal Strategies for Current Analysis, a market research firm. He has a diverse background. He is a lawyer, and has spoken on legal issues at many CSI conferences. But when we have lunch, I like to hear about his role as a psychological operations officer in the U.S. Army Reserve. Larry was the Deputy Commander of the NATO Information campaign in Bosnia from July '97 through February '98. He brings insights into an aspect of information warfare that people don't really hear much about.

Keith Rhodes is the Technical Director of the General Accounting Office (GAO) of the Chief Scientist. We met at about 6:30 in the morning in the Russell Office building a few summers ago before the Nunn hearings, which were a pivotal event. And he let me use his laptop. He also provided some very important testimony during those hearings. He has participated in some very vital work—for example, studies on information security at the FAA and the State Department.

Joseph Ruffini is Information Operations Special Projects Program Manager for System Technology Associates (STA). He retired as a non-elite Lieutenant Colonel in 1995. At one point, he was Chief Special Technical Operations for the Commander and Chief United States Space Command, and was appointed the Space Command's first Commanding Control Warfare Officer (later designated as Information Warfare Officer).

Lois Miller is Senior Systems Analyst for Infor-

mation Operations and Information Warfare for STA. She provides information operations and information warfare support for NORAD, the North American Aerospace Defense Command located at Peterson Airforce Base in Colorado.

**Power:** What is Information Warfare or Information Operations in the real world?

**Joseph Ruffini, STA:** There's a lot of different definitions. In it's simplest form, information warfare is protecting one's own information and information systems from attack, from exploitations while attempting to exploit and attack the adversary's information and information systems. There are some subsets to information operation. There's five or six major subsets. There's Computer Network Attack; there's Computer Network Defense; there's Psychological Operations (Psy-Op), Military Deception, Electronic Warfare, Operations Security, Force Protection. A lot of the disciplines that used to be separate, especially in a government organization with respect to protecting information and plans, somehow all roll under Information Operations and Information Warfare. In 1992, it was called Commanding Control Warfare. The term "Information Warfare," was a top-secret term that you didn't use outside the top-secret environment. In 1993 and 1994, we were allowed to use the term Information Warfare and Information Operations openly. The fact that the United States dabbles in computer network attack and the offensive side of IO or IW, was highly classified, beyond "secret." In 1994, it became only "secret" that we did it. Today, if you read through the Air Force Doctrine document 2-5 "Info Ops," it says in unclassified text, we do computer network attack. So we engage in the offensive stuff, that's not a secret now. What our capabilities are --that's the stuff that's in the "Black World."

You hear the terms Black World program, Code Word program, Darth Vader program, etc.

**Lawrence Dietz, Current Analysis:** Information Warfare is the manipulation and corruption of information for the advantage of the adversary. But it's not just hacking networks or jamming signals. Some of the greatest information warfare you can see is broadcast during the final week of the 1998 election campaign! It's no coincidence that the American election is right around Halloween. But that is also part of information warfare. Depending on the desired effect, television is the nuclear weapon in information warfare.

**Ruffini:** The "CNN factor."

**Keith Rhodes, GAO:** You have to understand you're moving a very ancient motivation into the modern environment. You're doing it all for the same reasons. Why would I rob banks where people are professionals when I can hit the VA? They got lots of money, too. They've got more than the banks. Why would rob banks when I can hit Social Security? What we're seeing is that the attacks are more for personal gain—Wild West robbery, somebody wants money, organized crime. There's also a great deal of industrial espionage. People like to hit government sites so they can launch attacks against corporate sites. It's real nice when it looks like the VA is trying to break into Dow Corning because the French want to find out how Dow Corning makes multi-mode fiber optic cable.

**Power:** Not that that ever happens.

**Rhodes:** No, not that that ever happens, right. But the point is that you're still looking at ancient motivations. Computer crimes, computer warfare, info warfare, info operations—if you

remove the words info and computer, you're looking at the same ancient motivations. You're looking at crimes, you're looking at operations. The operations folks in the Joint Staff are going to operate in a multitude of environments, one of which is the information environment. And information environment is as it's been pointed out, not only computer networks, but CNN as well. Planting a crappy story about an opponent, you know, negative campaigning and things like that—that's info ops. You're trying to get the information out, true or false, or at least the story you want told. So the motivations are the same, it's the environment that is different.

**Lois Miller, STA:** Information operations takes something that's been around for a very long time and then adds computer network attack and

—Keith Rhodes

defense into it. It has helped the perpetrator because international law has not kept up. And the plausible deniability that it affords makes it very difficult to find out who exactly is perpetrating the crime. And with the international laws as they are right now, it's difficult to get extradition. It's very expensive and time-consuming. The international ramifications are incredible.

**Ruffini:** What's illegal here is not a punishable offense in a lot of countries. When you go through the consternation at the tax payers' expense to have a computer emergency response team from the federal government actually find that 16 year old kid in Croatia who broke into the Pentagon system, the Croats will simply confiscate his computer. That's about as far as they'll go in some cases.

**Power:** Concerning the "CNN factor" that Joe mentioned, in the November '98 Alert, we did an interview with Terry Lenzner who is a pri-

investigator. He talked about starting to see people spreading disinformation to affect company stock in different ways in the stock trading chatrooms, etc. Some of this activity is individual criminal activity, other activities might be organized by a competitor or other interested entity. So just as with the CNN factor, there are many ways the Internet can be used to manipulate information—not only the information but opinions based on the information.

**Ruffini:** A lot of people are under the impression that you have to have a lot of money and a lot of sophistication to wage info warfare. I'll give you an example of how a very small, relatively untechnical country, Somalia, frankly kicked the United States' butt. What first caused the Americans to lose enthusiasm for our efforts in Somalia? It was when Somalian tribesmen dragged dead bodies of our elite special forces in front of the CNN camera. That's psychological operations at it's best. The Somalians told the truth—you send your best, we kill them; here's the bodies. You want to try again?

You can use CNN for psy-op all over the world. Everybody does. But if you remember it's when we saw the dead bodies of our special forces that we said to the administration, "Hey, if you're not gonna do this right, get out." We ended up pulling out of Somalia. That's a textbook case of the United States getting its butt kicked through psy-ops from some smart tribesmen who knew to put the bodies where the cameras were.

**Dietz:** One of the things that bothers me about some discussions of information warfare or major cyber-crimes is that everybody talks

about catastrophic attacks. If I was a ruthless competitor and I wanted to drive my competitor to the point of distraction, I would probably take a page from Donn Parker, I'd exploit an unknown vulnerability and I'd change some prices of their critical products. And I'd start making their customers really mad! And the company would be totally indignant and would have to deal with all of this and would reduce their momentum in the marketplace. And it would never, ever be attributed to a hostile act—because those computers, they go wrong all the time.

**If I was a ruthless competitor and I wanted to drive my competitor to the point of distraction, I would probably take a page from Donn Parker, I'd exploit an unknown vulnerability and I'd change some prices of their critical products. And I'd start making their customers really mad!**

—Larry Dietz

it's not IW, it's industrial espionage. But if an organized group, whether it's the government or a would-be government, like a separatist group, or some group with a bizarre agenda, for example the AUM cult, some organized entity is pursuing an organized effort to deny, disrupt, destroy, misdirect, misinform, using information systems to get at an adversary—that's information warfare.

**Ruffini:** You're right. You start by putting a grain of sand in your hand, at what point do you have a heap? If I slug it out with someone in a bar fight, that's one thing, but, if Chicago attacks New York, that's another thing. So when do you know that it's warfare? When do you know that you have a dedicated operation against you? In the case of the Rome Labs attack, it took every computer emergency re-

**Power:** Some use the term "information warfare" very loosely, everything is referred to as information warfare. But when somebody is stalking somebody online, or committing identity theft, it's not information warfare, it's computer crime. If a corporation is stealing the trade secrets of another corporation,

sponse expert the Air Force and two prime supporting contractors to investigate that accident. And that took two-and-a-half weeks. We're talking about when 16-18 year old kids do this! It really taxes our assets. God help us the first time a terrorist group, a special interest group, or a nation state decides to actually do a concerted attack across all of the disciplines. But it all goes back to risk analysis.

The hardest question to answer in the information protection business is "What do you want to protect?" Now that may seem like an easy question. Nobody's got all the money and the time to research what do you want to protect. And you sit down with your colleagues at the office and say, "Okay, what's really important in this company? What do we want to protect?" You're not going to decide that in a day. If you decide what you want to protect,

and it's information, then you gotta ask the question, "Okay, where is all this information we're trying to protect?" So, first you have got to decide what you want to protect, then you have got to find out where it is. And most of us can't tell other people where our critical information is because we don't know. It's on CDs; it's on disks; it's in databases; it's on paper; it's in dumpsters.

What is the risk to my company of loss, degradation or compromise? And if that falls outside of the comfort zone, then you go into risk mitigation. "Okay, boss, you know we can subscribe to encryption software. It'll only cost us \$30 bucks a month for x amount of machines. And we think that'll provide us some good protection when we're sending bid rates and marketing plans between Colorado Springs and California." It is all based on risk analysis.

**Power:** Larry was talking about going in to change a few prices on a target's Web site.

**Satellite systems cost a lot of money. When you field the satellite system and then you go back and you try to retrofit security into that systems, you're going to spend billions and billions of dollars.**

**—Joe Ruffini**

Electronic commerce is happening in a very real way. Cisco says it does \$7,000,000 a day in online sales. Charles Schwab says it transacts \$2,000,000 a week in online trade. Amazon.com went down one night on a systems glitch and an analyst estimated they could have lost \$600,000 in online business during that few hours. E-commerce will only grow more essential to businesses in the future. People have not thought through the impact of an attack on their e-commerce service. They are desperate to sell online as fast as they can. There are even people saying they're going to save so much, that what they're gonna lose isn't gonna matter. And that may be right to a lot of people, but it's gonna be wrong for some people in a real way, very soon.

**Rhodes:** You run into that with mobile voice right now. If you can't hijack a cellular phone—you should get out of business. You can do it with a string and a cup. Because the technology is crap. Maybe you don't have the device that locks it out, maybe you get it out of the box and don't even put a four-digit pin on it. But when you talk to the carriers, they're gonna look at you and they're gonna make a corporate decision. What are they going to say? "I'm going to worry in an industry that has 30% growth per year, I'm going to worry about a loss in between the 12% to 18% range? Sorry! Next question, you idiot engineer/security person. You don't understand business and you obviously don't understand money because look at your shoes." (Laughter) You know, that's the way life goes. There's a corporate security decision. Is there a threat? Sure. Some guy and his brother are standing on the bridge swiping calls. Is it critical? It's not critical to the service provider. Risk equals the low threshold

**Power:** Concerning infrastructure attacks, for

many people it's like the "Chicken Little" story, they see it as someone clamoring "the sky is falling." Indeed, some sensationalists and self-promoters have abused this threat. But, on the other hand, it's very real. It occurs to me that the Y2K problem is really illustrative of something that could happen with infrastructure attacks. We've seen the stories about what happens when people are making their Y2K tests. Bank vaults flying open, water systems being polluted, stock exchanges going down all over the world. So if you can get your mind around the damage that can be done to infrastructure through something like the Y2K bug, which was non-intentional, consider the implications of a conscious attack.

**Rhodes:** Well, Y2K is the great penetration test. As Richard points out, it is illustrative of what you're trying to do with security. You have both elevators and stairs in buildings because there's a fire code. Well, unfortunately, there is no quality code for how your software is built or how your systems are designed. The desire has been is for market share, get it out there as fast as possible.

What we're finding in the Year 2000 testing is that people are finally understanding the interconnectiveness. Maybe, maybe it will help us in the security arena because people will be able to say, "You were arguing about a disaster recovery plan for how long? Eleven years? And we never had one and, we did this thing for Y2K and we saw what it could do." They finally figured out what we mean by end-to-end. We mean from the moment the option is let, to the second the money clears through FedWire for the stock transaction. That's the scope of tests on Wall Street. But they are the only ones we've seen who are doing that level of testing.

I am not a psychologist, I'm an engineer. I don't understand why people do the things

they do. I'm not a programming language bigot and I'm not an operating system bigot. And that's very unique in an engineering environment. I don't wear a beret and I don't live for the Macintosh. I don't think Bill Gates is the Anti-Christ. I don't like his code, but I don't think he's the Anti-Christ.

**Power:** People are focused on servers, code, network intrusions and denial of service. But satellites are becoming so important—not only in broadcast media, but in business communications. There's extraordinary amount of vulnerability there. We just saw a recent satellite pager meltdown. These are things people should be thinking about in regard to information warfare, right?

—Joe Ruffini

**Miller:** The last time the Leonid meteor shower came through, there were 50 satellites in space. There are now over 500. The chance that they're gonna get hit with something is probably pretty good. When that pager system went out of control, it rendered gas pumps unable to pump because part of their system was carried on that satellite. It had a profound effect on quite a few people.

**Ruffini:** There's so much that people don't realize rides on satellites. We deal with satellite experts in the Space Command all the time. Take someone that works for the United States Air Force that's an expert in Space System and Satellite System, and say, "What exactly rides on this satellite? What exactly are all the functions that are performed on this satellite?" They would have to refer to their databases, there's so much that goes on.

One of the problems you have with satellite systems, not only as an operator but as a taxpayer is that when you deploy a satellite, you deploy a satellite system. The system is the satellite, plus the up link, the down link, the

**The up links, down links and cross links are targets for information warriors. It's relatively unsophisticated to jam or corrupt a UHL up link. It's child's play.**

cross link, and the controlling ground stations. Satellite systems cost a lot of money. When you field the satellite system and then you go back and you try to retrofit security into that systems, you're going to spend billions and billions of dollars.

One of the things that satellite systems designers have not looked at closely enough in the past twenty years is what the threat is going to be to our systems? And do we have the money and the skills to design the protection up front?

We've got a lot of satellite systems that are very vulnerable. Global positioning and communication satellites are not hardened. The up links, down links and cross links are targets for information warriors. It's relatively unsophisticated to jam or corrupt a UHL up link. It's child's play.

If you were to bring all the experts into the room and say, "Would you list all the vulnerabilities of your satellite system, given what we know to be the current information operations technology?" You could start writing on this wall and go all the way around and we'd be moving to the next room. Frankly, when you really get into this at the classified level, and start peeling back the onion skins, right now there doesn't seem to be a lot of hard solutions to the vulnerabilities in our infrastructure, because it takes time, and most of all it takes money.

**Dietz:** Does everybody know the difference between a fairy tale and a war story? One starts "Once upon a time," the other starts, "This is no ca ca." (Laughter)

In Bosnia, there's a bunch of TV antennas that go across the top of the country. This is no ca ca. One day, persons unknown took the

equipment out of one of those TV towers, which meant that all the TV towers below it didn't get any signal, which meant that the people who lived in the Southern part of the country couldn't watch "Cassandra."

What's "Cassandra?" Well, it's a pirated Venezuelan soap opera. These people were rioting in the streets because they couldn't watch "Cassandra."

What does this have to do with satellites? Well, the office of a high representative rented a Harris satellite up link and down link to replace this power that was out of commission, at about \$250,000 bucks a move. The point is that the satellites can sometimes be a cure for a problem when you have a denial of service. And don't deny people their television, it makes them really mad!

—Lois Miller

**We have to determine whether it's a 16 year old that has planted logic bombs, or it's a patterned attack. This is very important, especially in the defense industry, because if it is, indeed, a patterned attack, if it is state-sponsored, it could be considered an act of war.**

**Power:** We've talked

for 45 minutes about information warfare and we haven't mentioned HERF guns yet.

**Dietz:** I don't know what that is. (Laughter)

**Power:** Well, he still works for the government part time, so he might have to deny it. High Energy Radio Frequency weapons. What are their significance, and do you think that they pose a real threat?

**Dietz:** Frankly, I'd rather have a generator mechanic who could knock out the power.

**Miller:** I would worry more about precision guided software conditions.

**Power:** Precision guided software condition. You want to elaborate on that?

**Ruffini:** That's Lois' term for computer viruses. Precision guided software condition., NORAD has picked up that term now. They like it.

**Rhodes:** I would just rather have stable code. I worry a lot more about tracking bugs than somebody trying to drive by the data center in a van or hide a HERF gun in their pocket and walk by and do my disk. In the days of Tempest, when we were all working behind shields and all that stuff. Yeah, because we were running one big computer. And somebody could steal our emanations.

I just really want to have a stable release out of Microsoft. (Laughter) That's all! I don't want to have Service Pack Two be a catastrophic failure so they have to deliver me the Service Pack Two dis-install. Because in reality what they sent me was crap code.

**Power:** Just to summarize the panel's responses on the threat from HERF attacks, Larry's more concerned about generator mechanics, Lois is more concerned about computer viruses, and Keith is more concerned about bad code from Microsoft.

**Conference Attendee:** During the conference, we've heard a lot about a new and growing phenomena of automated hacking. Where it used to be you needed time, motive, and knowledge, now you only need time and motive to do real major hacking job. How does this exacerbate the problem of determining the risk?

**Miller:** We have to determine whether it's a 16 year old that has planted logic bombs, or it's a patterned attack. This is very important, especially in the defense industry, because if it is, indeed, a patterned attack, if it is state-spon-

sored, it could be considered an act of war.

**Dietz:** The net on this is that the skill level to render harm is much lower than it ever was. And one of the things that I've heard as a recurring theme during the conference is that most of the failures come from implementation and policy shortfalls. And they are known problems. The message to take home is to check on the basics. Do the basics.

**I break encrypted systems in the government all the time. And I don't have to worry about the encryption. I go into the system itself and discover, "Oh, you know, the administrator has no password."**

**—Keith Rhodes**

**Rhodes:** When you get your firewall, you buy it from Company X, you have to set up your firewall because it usually comes to you in one of two modes—it's either a fire hose or a fire brick. That is, everything's turned off or everything's turned on. You have to go

through and do the settings because most of the vendors don't want to, and can't do the work of coming out and establishing a security program inside your organization so that you understand what you want and do not want to do with your firewall. That's up to you. You have to bring up the administrative functions. You have to figure out whether this product running on NT is actually going to be secure enough, or somebody's going to be able to crack the VPN.

**Conference Attendee:** What is the threat posed from lack of preparedness vis-a-vis the Y2K bug in the Asian nations that are struggling economically and as well in less developed nations? For example, is there a danger from their missile systems, etc.? And what are the information warfare implications? Can the problem be exploited?

**Dietz:** Well, in regard to many of the countries in Asia, even though there has been financial difficulty, their militaries are probably insulated

cessful little business all by themselves. I'm not so much concerned about military side, because their budgets are immune. What that might concern me are the large bureaucracies—particularly chaebols or keiretsu—where everybody is intertwined and nobody is gonna tell anybody if something is kafluzzed until something bad really happens and it's already obvious.

**Rhodes:** I'll give you one example from looking at the banking community and Wall Street. The U.S. banking community, Wall Street, the clearing houses, SWIFT and FedWire are all doing integrated tests. They're not working the code anymore. They're actually in test mode. They've gone through Beta. The situation, though, is that even with as good a test structure as they have, they are seriously trying to figure out how they can firewall themselves off from Europe. Because 40% of Europe is not going to be ready on January 1, '99 for the Euro. Germany is taking a wait and see attitude toward Y2K. They're very concerned to whether the Bank of Japan is going to be able to play in the clearinghouse tests. There are six countries out there that they really want to clear with. It's nice to be sitting here in an English-speaking country because Australia and New Zealand, and Canada, and the U.K. and the U.S. are ahead of the game. But all that means is that you're on a pile of dog crap and you get to be on top of it. And that's about it. Yeah, there are people desperately trying to figure out right now, how do you firewall yourself off from a global economy. You have people like Ed Yarden saying the rest of the world is gonna be toast. How far do you have to scrape until you find what's left of the bread?

**Conference Attendee:** Wouldn't the information warfare threat be reduced significantly if the U.S. government lifted its export ban on strong cryptography?

**Rhodes:** If I made more Stradivarius violins, would there be better violinists? No. The overwhelming preponderance of the security problems are people are just not fixing the regular holes; not changing the defaults. The use of secure encryption is good, and I personally think the government's policy is total ca ca. But I don't think it's the big problem.

**Ruffini:** No, it's not the big problem. But I personally would like to see us share a lot more of encryption technology and other defensive capabilities with our allies. I would like to see an international relation very similar to the one we had during the Cold War. An attack against one is an attack against all. If you have nukes and want to be considered the good guys, come on in, be on the team. There's strength in numbers. In the information warfare game, eventually you'll see those international liaisons. But I don't think it's gonna come much before 2004 or 2005.

**Rhodes:** I break encrypted systems in the government all the time. And I don't have to worry about the encryption. I go into the system itself and discover, "Oh, you know, the administrator has no password." (Laughter) So I climb inside the system. In certain systems, the key during VPN is stored in the swap space. So you steal the swap space and you hijack the session.

Because I have the key, I don't have to do the math. I've got it already because you've got an encryption link between somebody sleeping on a park bench and somebody living in a cardboard box. But, oh man, that session is tight! Right up until you kick the cardboard box open or hit the guy on the park bench in the feet with a nightstick.

**Ruffini:** If we find and kill everybody as smart as Keith, a lot of the info war problem would go away. That's one way to do it, speaking as an Italian American. (Laughter)