

# THE WALL STREET TRANSCRIPT

Questioning Market Leaders For Long Term Investors

A N A L Y S T I N T E R V I E W

## Outlook for Airport Security Stocks

KEVIN B. SKISLOCK — LAGUNA RESEARCH PARTNERS LLC

**KEVIN B. SKISLOCK** has more than 27 years of experience as a Wall Street stock analyst. Nearly half of his career has been spent analyzing stocks for leading buy-side money managers, including Citigroup and Wellington Management Company. On the sell side of Wall Street, he has analyzed stocks for the institutional and retail investment clients of firms including a "research boutique" subsidiary of UBS PaineWebber, Inc. and RBC Dain Rauscher, Inc. Mr. Skislock has been recognized by *Institutional Investor* magazine in their "Best of the Buy-side" rating of Wall Street's buy-side analysts. He has appeared on NBC Nightly News with Tom Brokaw, CNBC's MarketWrap, CNBC's Business Center and The Wall Street Journal Report. Mr. Skislock holds a BS degree from Villanova University and an MBA degree from The University of Chicago. Mr. Skislock remains an active competitor in Masters track and field.

### SECTOR – SECURITY SOFTWARE & SERVICES

**(RAG810) TWST: Can we start out with an overview of how you approach coverage of the homeland defense area, and how airport security fits into that?**

**Mr. Skislock:** To the best of my knowledge, we're the only firm on Wall Street covering homeland defense as an industry per se. The cornerstone of our homeland defense coverage is what we call our Homeland Defense Industry Operating Performance Index. This Index focuses on small and mid-cap companies and is split into two sectors: security and weapons subcontractors. We define the security sector to include companies involved in biometrics, digital asset security, explosives detection, intelli-

gence/surveillance/reconnaissance, also known as ISR, and physical asset security including vehicle armor. Many of the technologies and products included in this sector will be essential to achieving a sustainable improvement in airport security. The weapons subcontractor sector includes military equipment, defense electronics and military-centric information technology companies.

**TWST: And which companies does the Index include?**

**Mr. Skislock:** The total Index currently includes 18 companies. The security sector includes 11 of these and is comprised of **Armor Holdings (AH)**, **Check Point Software Technologies (CHKP)**, **CompuDyne (CDCY)**, **Identix (IDNX)**, **Internet Security Systems (ISSX)**, **InVision Technologies**

(INVN), **L-3 Communications Holdings** (LLL), **OSI Systems** (OSIS), **Symantec** (SYMC), **Viisage Technology** (VISG), and **Zebra Technologies** (ZBRA). The weapons subcontractors sector is comprised of the remaining seven companies and includes **Alliant Techsystems** (ATK), **Anteon International** (ANT), **CAI International** (CAI), **DRS Technologies** (DRS), **Integrated Defense Technologies** (IDE), **ManTech International** (MANT), and **United Defense Industries** (UDI). Year-over-year operating performance for companies in the Index was very strong during the second calendar quarter of 2002. For the group as a whole, all 18 companies, June quarter sales were up 29% and operating profit was up 59%. For the security sector, sales were up 45% while operating profit was up 72%. And for the weapons subcontractors sector, sales were up 15% and operating profit was up 41%. In an economic environment where it's difficult to find double-digit earnings growth rates, this is pretty impressive performance. Over time, we'll be expanding the number of companies in the Index. We're constantly reviewing other companies for possible inclusion.

**TWST: Before we discuss individual companies, can you tell us a little about your outlook for the industry?**

**Mr. Skislock:** In our view, it's fairly obvious that most of these companies will do well during the 2002 through 2003 time frame. Operating perfor-

mance during this period is being driven by huge emergency spending bills directly related to homeland defense, a substantial increase likely in the fiscal 2003 US defense budget, increased military spending among our allies, particularly Britain, and worldwide fears regarding security vulnerabilities. The important question, though, is which of these companies are positioned to generate powerful operating performance *beyond* 2003.

**TWST: And how do you go about determining that? Do you expect that the same growth drivers will be in play?**

**Mr. Skislock:** The key growth drivers will continue to be government spending and advances in technology. As far as government spending is concerned, it's a key growth driver, but it's largely out of the control of company management. It can only

be influenced indirectly via aggressive lobbying. Technology, though, is a different story. It's very much under the direct control of company management, and smart managers are laying the groundwork now for the introduction of disruptive technologies into the post-2003 homeland defense marketplace.

**TWST: And what's your outlook for advances in airport security technology?**

**Mr. Skislock:** We expect that the technology curve for airport security, as well as for port security and inland border security, will be extremely steep. We base this analysis on two key points. First, we believe that threat detection technologies will migrate

### Highlights

*Laguna Research Partners specializes in covering homeland defense as an industry. Its Operating Performance Index for Homeland Defense focuses on small and mid-cap companies and is divided into two segments: security and weapons subcontractors. Kevin B. Skislock defines security to include biometrics, digital asset security, explosives detection, ISR and physical asset security. Operating performance for this year and next is being driven by enormous emergency spending bills directly related to homeland defense, and he reveals which companies are best positioned to generate powerful operating performance beyond 2003. Many companies will need new robust technologies to propel sales and earnings after next year and there are small cap companies that can make important contributions in this area. He believes that 2004 will separate the wheat from the chaff as far as homeland defense companies are concerned. Companies include: *InVision Technologies* (INVN); *Eurotech* (EUO).*

outward from the last possible point of interception, an airport's passenger security checkpoint, for instance, and into airport terminals, into airport parking lots and right to the perimeter of the airport itself. The tremendous burden now being shouldered at traditional passenger security checkpoints will be substantially reduced when cheap, transparent and ubiquitous technologies can intercept threats as they enter the airport perimeter, the parking lot, or pass from the parking lot into the terminal. Ultimately, as form factors shrink and costs decline, we're going to see transparent and ubiquitous threat detection technologies deployed along highways and throughout cities. We've identified some companies that we think can provide that kind of technology.

***"InVision assembles and markets an impressive line of explosives detection systems (these are known as EDS) for different-sized airports. The company appears to be having success migrating customers up to their top-of-the-line CTX 9000, an EDS with superior throughput speeds. So, in our view, they're doing an excellent job of meeting the tremendous surge that we've seen in demand for EDS."***

factors, in a variety of settings and able to detect a wide range of threats, including biological, chemical and nuclear. One of the great weaknesses of current location-specific technologies is that the threat must come to them in order to be detected. Not only do some of these technologies have a poor record for intercepting processed threats in a real-world environment, they're also anything but transparent and are highly avoidable. Even if the intercept rate for these location-specific rigid technologies were to improve, the answer for intended terrorists would simply be, "Don't go there."

**TWST: But an awful lot of what you are talking about here goes contrary to the whole idea of privacy, a citizen's right.**

**Mr. Skislock:** Yes, there are important privacy issues relating to homeland defense that are already being actively debated as we all try to adjust to the realities of high-impact terrorism on US soil. Historically, our free society has always been faced with decisions balancing benefits against loss of privacy. In just the past century or so, as the evolution of technology has accelerated, the frequency of these debates has increased and the potential ramifications of our decisions have expanded tremendously. Back in 1903, when Massachusetts and Missouri enacted the first driver's license laws, people in those states had to ask themselves, "Do I stick with the horse and buggy, or do I give up some of my personal privacy, get a driver's license and buy a car?" The spread of commercial telephone service at the turn of the last century also posed an important benefit versus privacy question. More recently, as the Internet became an integral part of our daily lives, we had to ask ourselves, "Do I stick with snail

**1-Year Daily Chart of InVision Technologies**

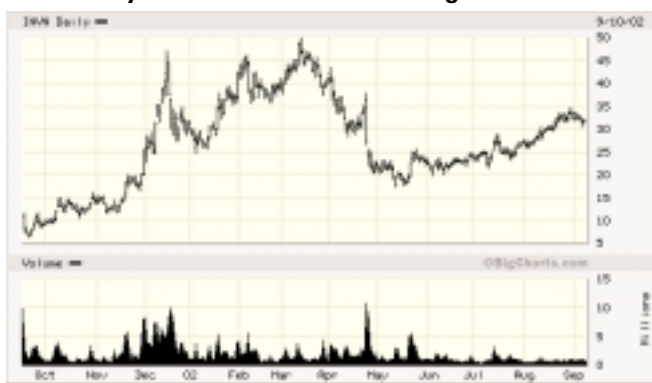


Chart provided by [www.BigCharts.com](http://www.BigCharts.com)

Second, and this goes hand-in-hand with the first point, we expect that threat detection technologies will become less and less "location specific" over time. That is, we believe that the days are numbered for "rigid technologies" that only serve a very specific threat detection role in a very specific setting. The post-2003 future of threat detection, we feel, belongs to companies developing flexible technologies that can be deployed in a variety of form

mail, or go with e-mail and instant messaging? No one can see my snail mail unless they rip open the envelope, but I need to communicate NOW.” And the proliferation of cell phones has faced many of us with the same sort of decision, “Do I stick with a fixed land line telephone, or do I buy a cell phone? My cell phone location for every call is recorded and stored, but I’ve got to stay competitive.” In all of these cases, people have opted for a perceived benefit and surrendered some of their privacy.

The same sort of decision-making process is at work and will continue to be at work with regard to technologies that can improve our chances of countering high-impact terrorism. Achievable benefits will always be weighed against privacy loss. Given the economic risk associated with high-impact terrorism, the significant inconveniences created by current threat detection technologies, and the fact that the threat of high-impact terrorism will never really go away, my instinct is that people will gradually adjust to transparent and ubiquitous threat detection.

**TWST: How soon might we begin to see some of these things happen?**

**Mr. Skislock:** Well, as I mentioned, we expect the technology curve in homeland defense-related threat detection to be pretty steep. A rapid move toward transparent and ubiquitous threat detection, we think, is probably more reality than science fiction. And we expect that the flow of investment dollars into this area will continue to accelerate because the market for low cost, transparent and ubiquitous threat detection technologies is potentially huge. The US/Canadian “Smart Border” plan provides an ex-

cellent view into just how large this market will prove to be. The Plan is comprised of 30 action points including the implementation of biometrics, new permanent resident cards for Canadian immigrants, compatible immigration databases, compatible commercial processing, container targeting at seaports, physical and technology infrastructure improvements at border crossings, infrastructure protection, transponder/GPS-based intelligent transportation systems and aviation security.

**TWST: Where are these advances in technology going to come from? Are they going to come from the companies that are generating strong earnings growth now?**

**Mr. Skislock:** There are a lot of companies likely to generate impressive profit growth during the 2002 through 2003 period. They’ve established excellent distribution channels and are generat-

***“We believe that threat detection technologies will migrate outward from the last possible point of interception, an airport’s passenger security checkpoint, for instance, and into airport terminals, into airport parking lots and right to the perimeter of the airport itself. The tremendous burden now being shouldered at traditional passenger security checkpoints will be substantially reduced when cheap, transparent and ubiquitous technologies can intercept threats as they enter the airport perimeter, the parking lot, or pass from the parking lot into the terminal.”***

ing great cash flow but, in many cases, their post-2003 technology road maps are either unimpressive or somewhat fuzzy. This is particularly true for many companies in the security sector. On the other hand, there are many smaller companies as well as universities that are developing impressive post-2003 threat detection technologies, but they need additional development funds and they need distribution channels to get those technologies to market. We expect that these respective sets of strengths and weaknesses will prove to be very complementary. The most interesting play in homeland defense might prove to be the smaller companies positioned to provide post-2003 revenue and earnings solutions for the larger companies in this space. Many of these smaller companies might reap the benefits of substantial tech-

nology royalty fees, while others might prove to be excellent acquisition candidates.

**TWST: Where does InVision Technologies stand in all of this?**

**Mr. Skislock:** In their most recent earnings release, **InVision** indicated that their products revenue in the second quarter ended June exceeded their products revenue for all of 2001. And that operating strength is reflected in our projections. We see **InVision** earning an estimated \$2.80 in 2002, up 438% from the \$0.52 that the company earned in 2001. But as the market for current explosives detection technologies becomes saturated, we see the company's earnings flattening out in 2003. And in 2004, we're projecting a drop in EPS to the \$1.00 level.

1-Year Daily Chart of Eurotech



Chart provided by [www.BigCharts.com](http://www.BigCharts.com)

Why? Well, two reasons. First, as the market for current technologies becomes saturated, we do not expect the combination of replacement sales plus system upgrades and service calls on the installed base to match the revenue and profit currently being generated by the sale of lots of \$1 million per copy systems. Second, we do not yet feel comfortable with

the company's post-2003 technology road map. We do not think that we are yet seeing the breakthrough technology that will be capable of generating revenue and profit comparable to that being generated by the aggressive placement of the current line of explosives detection systems.

So this is a perfect example of why we are looking beyond 2003 in our industry analysis and trying to identify companies that are developing disruptive technologies for the post-2003 threat detection marketplace. If you were to ask some of the larger companies in the threat detection arena why they are so

focused on the near term, they'd probably tell you, "Look, we are so busy racing to get machines out the door this month and next month, we really don't have a lot of time to focus on post-2003."

**TWST: What is their near-term answer?**

**Mr. Skislock:** **InVision** assembles and markets an impressive line of explosives detection systems (these are known as EDS) for different-sized airports. The company appears to be having success migrating customers up to their top-of-the-line CTX 9000, an EDS with superior throughput speeds. So, in our view, they're doing an excellent job of meeting the tremendous surge that we've seen in demand for EDS. At some point, though, we are going to see the market for the current EDS technology class saturated.

**TWST: Is InVision a current contractor for supplying this type of equipment?**

**Mr. Skislock:** Yes, they are. Right now, we are seeing a lot of first time EDS placements at airports worldwide. As we move through the end of 2003, though, we expect to see the EDS space be-

*"Eurotech, Ltd. is a development stage company that acquires, develops and markets chemical and electronic technologies for the environmental and security markets. In the security sector, Eurotech has come up with an interesting acoustics-based remote sensing threat detection technology called Acoustic Core, or AC. This technology appears to have the flexibility to be applied across all three of the key entry points — airports, container ports and inland border crossings — that might be used by terrorists intent on carrying out high-impact attacks."*

come more of a replacement market, more of an upgrade market and more of a service market. Service revenue is very profitable, but original machine sales carry a price tag of somewhere in the \$1 million per unit range, and they carry a nice profit margin in their own right. So the question in our view is what's going to boost the company's growth potential beyond 2003? We are looking for companies that really do have powerful post-2003 technologies.

**TWST:** When you look out, what are the answers beyond 2003?

**Mr. Skislock:** We believe that the post-2003 earnings power of many of these larger threat detection companies is going to come from smaller companies as well as from universities that, as we speak, are developing highly robust and potentially disruptive technologies for the threat detection market. These technologies could ultimately get to market via license agreement, patent purchase or outright company acquisition. One company that we think is interesting is **Eurotech, Ltd.** (EUO), an AMEX-listed company based in Fairfax, Virginia. It's a development stage company that acquires, develops and markets chemical and electronic technologies for the environmental and security markets. In the security sector, **Eurotech** has come up with an interesting acoustics-based remote sensing threat detection technology called Acoustic Core, or AC. This technology appears to have the flexibility to be applied across all three of the key entry points — airports, container ports and inland border crossings — that might be used by terrorists intent on carrying out high-impact attacks. AC tech-

***"We believe that the post-2003 earnings power of many of these larger threat detection companies is going to come from smaller companies as well as from universities that, as we speak, are developing highly robust and potentially disruptive technologies for the threat detection market."***

***"The post-2003 future of threat detection belongs to companies developing flexible technologies that can be deployed in a variety of form factors, in a variety of settings and able to detect a wide range of threats, including biological, chemical and nuclear. One of the great weaknesses of current location-specific technologies is that the threat must come to them in order to be detected."***

nology can identify the unique acoustic signatures of illicit materials, so management expects that it will be able to develop products that can detect a broad array of explosive, biological, chemical and nuclear threats, all via a single threat detection package.

As an example of some of the outstanding development work being done at the university level, a team led by Michael Sailor at the University of California, San Diego (UCSD), has created a technology labeled "smart dust." Smart dust is made up of silicon dust chips that can remotely sense biological and chemical agents on a real time basis. Sailor's team pulverizes silicon wafers with ultrasound, and layers the resulting particles with an ultra-thin layer of chemically reactive film. These particles can then reflect light at precise wavelengths that are unique to certain biological and chemical agents. Theoretically, the particles can be coated to detect thousands of agents simultaneously. Something so small as a piece of dust that has intelligence built into it has tremendous market potential. As Sailor says, it can be inconspicuously applied to walls in homeland applications and released as dust clouds on military fronts. Right now, the team is developing a laser-based reading device that should be able to read the output of smart dust from a range of up to one kilometer.

I mentioned earlier that this market will move rapidly toward low-cost, transparent and ubiquitous technologies. UCSD's smart dust technology could prove to be the ultimate in this regard. This technology obviously sounds pretty futuristic, but Sailor estimates that it might be no more than a year before it

reaches commercial application. Both Eurotech and UCSD, in our view, provide excellent examples of the kinds of technologies that might benefit larger threat detection companies beyond 2003.

**TWST: As we look at this market, is the reality that the money is being spent or is it still largely talk at this point?**

**Mr. Skislock:** The gab factor has been pretty high and, as we have begun to adjust to the horror of September 11, the political posturing has obviously intensified. If Congress had moved this slowly following Pearl Harbor, we would have been fighting the Japanese in Kansas City long before getting to the Midway Islands. Focusing on the airport security side, it is going to be very tough for airports to meet the December 31<sup>st</sup> deadline for having all checked bags scrutinized by explosives detection systems.

**TWST: It won't be met because the equipment isn't available or the money is not available or the people are not available?**

**Mr. Skislock:** All of the above, to varying degrees. First, it's going to be nearly impossible for EDS companies to get all of the needed machines out the factory door that fast. Remember, we started this race (that is the race to deploy EDS throughout US airports) from a standing start. The placement of EDS in airports was not a high priority issue prior to the attacks. **InVision** management tells me that they were actually laying personnel off on the morning of September 11, 2001. I also understand that the company started calling laid-off personnel back to the company on September 12, 2001. Second, emergency spending bills related to homeland defense have worked their way into law, but that money has been slow in getting allocated to the private sector.

**TWST: So a lot of rhetoric and not a lot of action?**

**Mr. Skislock:** Well, as the earnings performance of many of the companies in our Index shows, increased funding has started reaching many of these companies. The level of rhetoric, though, still considerably exceeds the level of action. We have a long

way to go. The focus in Washington has now turned from emergency spending legislation toward the fiscal 2003 defense budget. Back in February, the White House put a

*"As an example of some of the outstanding development work being done at the university level, a team led by Michael Sailor at the University of California, San Diego (UCSD), has created a technology labeled 'smart dust.'"*

very comprehensive \$369 billion plus \$10 billion defense budget on the table that represents a sharp increase in spending versus the likely level of expenditures in fiscal 2002. In May, the House approved their own \$383 billion defense budget bill. They added the additional \$10 billion in a July vote. It wasn't until August 1, the last possible day before summer recess, that the Senate passed a \$355 billion defense budget bill. The Senate said on August 1 that it would take care of the additional \$10 billion when it returns, so that's not actually done yet. In sum, both of these bills and the Administration's budget all call for huge increases in defense expenditures that will benefit everyone in the homeland defense industry, weapons contractors, weapons subcontractors and security companies, right across the board.

**TWST: So there is a hope?**

**Mr. Skislock:** Emergency spending measures have been signed into law, and money is working its way to the private sector, but at a slower pace than we might have hoped for and anticipated back on the evening of September 11, 2001. In our view, two key factors have worked in favor of the US and its allies during the period since the attacks. First, the multi-pronged allied campaign against al-Qaeda has clearly been effective in disrupting al-Qaeda's com-

mand and control structure. Second, the terrorist war model does not lend itself to sustained aggression. So, while al-Qaeda can exploit the vulnerabilities of a free society, the terrorist war model gives the US and its allies plenty of time to re-group, adapt and counter-attack. Back on the evening of the original attacks, who would have thought that we would reach the first anniversary of those attacks without sustaining a second high-impact attack? But that luck is not going to hold out forever.

**TWST: At some point we have to do something.**

**Mr. Skislock:** Everything that needs to be happening in the private sector is happening. I am very impressed by the way **InVision** is rising to the occasion as far as 2002 and 2003 is concerned. The company is not only getting EDS machines out the door at a rapid pace, but it is doing that in a very profitable way. Cost control at both the cost of sales level and at the operating expense level is excellent. And it is clear that the disruptive technologies needed to stay one step ahead of al-Qaeda in the post-2003 environment are being developed by innovative small cap companies and universities. Hopefully, it won't take another successful high-impact terrorist attack to get the Senate moving at a faster pace on key appropriations bills and on legislation creating a Department of Homeland Security.

**TWST: So the more important question is where do you go from here.**

**Mr. Skislock:** Yes, that's where Laguna Research Partners is focusing its attention and that's where we think we can bring value to Wall Street. As I said earlier, we don't think that the 2002 through 2003 time frame is much of a difficult call. The potential winners are fairly easy to identify. But, after the initial tsunami of government spending actions has finally crested, and once the initial round of security technology deployment has been completed, we

want to help the Street figure out which companies will play a key role following 2003. Yes, we do our best to present current commentary via reports like our Homeland Defense Industry Monthly Reviews. In fact, those reports have been surprisingly popular with our clients who use them as a one-stop read to catch up on everything that's going on with 18 important homeland defense companies in the small and mid-cap arena. But where we are striving to bring high analytical value added to investors is in trying to help them understand how this new industry is evolving, and which companies are going to thrive in the post-2003 environment. That's what we are looking for. There are clearly many large homeland defense companies, particularly in the security sector, that will need new, robust technologies to propel sales and earnings beyond 2003. And there are small cap companies that can make important contributions in this area. We believe that 2004 will be the year in which the wheat will be separated from the chaff as far as homeland defense companies are concerned.

**TWST: In today's environment of full analyst disclosure, does Laguna Research Partners have a relationship with any of the companies that we've discussed today?**

**Mr. Skislock:** Yes, Eurotech has recently joined our client ranks.

**TWST: Thank you. (TM)**

*Note: Opinions and recommendations are as of 9/10/02.*

**KEVIN B. SKISLOCK**

**Partner and Chief Executive Officer  
Laguna Research Partners LLC  
Irvine, CA 92614**

**(949) 651-9053**

**Website: [www.LRPonline.net](http://www.LRPonline.net)**

**e-mail: [skislock@LRPonline.net](mailto:skislock@LRPonline.net)**