

## 21st Century Blitzkrieg: Winning Investment from the Cyberwar

### *Special Report*

From Sun Tzu to "Stormin' Norman" Schwarzkopf, the goal of every military commander has always been pretty simple: to kill people and break things.

Beat the other guy, and your name will find its way into the history books...

The only thing that changes is the technology. From the longbow to the ballistic missile, the arms race is one that never sleeps.

One of the fastest growing fronts in this struggle is in cyberspace. Today's style of combat is geek versus geek.

But don't believe for a second that it's not just as dangerous...

Because while it doesn't involve tanks or fighter squadrons, cyberwar's ability to disrupt an enemy is just as effective, and often equally destructive.

It's war by other means — one that focuses on using computer code to strike an enemy's Achilles' heel.

#### **Full-scale cyberwar**

The recent discovery of a computer worm called [Stuxnet](#) is a perfect example of the damage a hacker armed with code can create.

Using the "most advanced and aggressive malware in history," cyberwarriors have now set Iran's nuclear ambitions back by two years, according to most estimates. (Not surprisingly, Israel and the United States are at the top of the suspect list.)

The worm itself attacked controllers critical to operations at Natanz, a sprawling enrichment site in Iran's desert. As operators stared blankly at their screens, the bug's centrifuges spun wildly out of control, tearing systems apart.

"This was nearly as effective as a military strike, but even better since there are no fatalities and no full-blown war. From a military perspective, this was a huge success," said Ralph Langer, a top German Security expert.

"It will take two years for Iran to get back on track."

This is only the latest cyber skirmish...

Back in 2007, Estonia fell victim to what *Wired Magazine* dubbed "Web War One".

Hounded by three weeks of digital assaults, Estonia's electronic Maginot Line proved as feeble as the original. The country's firewalls withered as a flood of data sent by the nation's unknown opponents quickly crashed one system after another, crippling numerous vital public services.

Websites of government ministries, banks, and newspapers all fell victim.

And while the rest of the world watched the attacks with a combination of curiosity and indifference, military planners around the globe thought otherwise. They recognized that a long-awaited and long-predicted cyberwar had claimed its first victim.

As with like the Blitzkrieg of old, a new chapter in warfare had begun for all to see.

"We've been lucky to survive this," said the Estonian defense minister.

"If an airport or state infrastructure is attacked by a missile, it's clear war. But if the same result is done by computers, then what do you call it? Is it a state of war? These questions must be addressed."

#### **Cyberwarriors are just warming up**

While there wasn't what you'd call "normal" war carnage during the Estonian attack, governments around the world viewed the attacks with a more critical eye.

They knew full well what this series of cyber attacks showed about their own vulnerabilities — and that warfare of this nature could only get considerably worse, given our increasing dependence on the Internet. That wired backbone creates a rich set of targets of opportunity... not much different than any other wartime objective.

Like a digital Pearl Harbor, targets could include defense networks, the energy sector, emergency preparedness systems, financial services, telecommunications, even the agricultural sector...

In a coordinated cyber attack, no buildings have to fall to weaken us militarily, economically, or politically.

The U.S government takes these threats so seriously that the Department of Defense is prepared, based on the authority of the president, to launch either a cyber counterattack or an actual bombing of the source.

In fact in 2009, President Barack Obama declared America's digital infrastructure to be a "strategic national asset," and later appointed General Keith B. Alexander as head of the new U.S. Cyber Command (USCYBERCOM) to defend American military networks and attack other countries' systems.

By all accounts, General Alexander has his hands full. According to the Pentagon, Department of Defense computers are probed 250,000 times a day, mostly by Chinese hackers.

Joint Chief Chairman Admiral Mike Mullen said earlier this week, "The threat from China is significant, it is an enormously complex and critical area that all of us need to understand a lot better and do a lot more about."

He also warned the impact of a cyber attack on the United States was "substantial" and potentially devastating.

"It's an area with no rules, there are no boundaries, it happens with the speed of light."

### **Cybersecurity Stocks**

Of course, these real-time threats have led to beefed-up budgets to combat them.

A report released in December by Input predicts federal investment in cybersecurity will reach \$13.3 billion by 2015, up from \$8.6 billion in 2010. That's a compound annual growth rate of 9.1% — nearly twice the rate of other government IT spending.

This is going to create a money-making opportunity for investors, as public companies with security expertise begin to win big new government contracts.

In this arena, one of biggest beneficiaries is a diversified technical services company called **SAIC. Inc.** (NYSE: [SAI](#))

Headquartered in McClean, Va., the company's 45,000 employees serve customers in the U.S. Department of Defense, the intelligence community, the U.S. Department of Homeland Security, other U.S. Government civil agencies and selected commercial markets.

At the company's core, SAIC helps governments and companies plan, manage and protect critical public infrastructure.

From ground, marine and air transportation systems to energy distribution and emergency preparedness systems to telecommunications and data networks, SAIC has expertise in securing the critical infrastructure vital to a our national security.

As a result the company wins contract after contract after contract largely from the Federal government.

Here are just a few of them from the last quarter when net business bookings totaled \$2.3 billion. They include:

- **A five-year \$45 million contract from the Navy.**
- **A four-year \$30 million contract from the Marines.**
- **A 30 month \$30 million contract from the San Diego County Regional Airport.**
- **A five-year \$61 million contract from the Army.**
- **A five-year contract with the Department of Veteran Affairs with a ceiling of \$12 billion.**

But that's just the tip of the iceberg for SAIC. Orders like these arrive every month like clockwork.

In fact, the company's backlog of signed business orders at the end of the second quarter of fiscal year 2012 was a whopping \$17.7 billion. As compared to the end of the second quarter of fiscal year 2011, that marked a total backlog increase of 12%.

As for future guidance, the company revealed they expect to produce the following in 2012:

- **Revenues of \$10.6 billion to \$11.0 billion;**
- **Diluted earnings per share from continuing operations of \$1.30 to \$1.40; and**
- **Cash flows from continuing operations at or above \$600 million.**

For investors, the opportunity to purchase SAI at a discount has only improved during the recent sell-off. As for the future downturn in government spending, it is already largely price in.

In other words, this is one that investors do not have to chase leaving little downside as the market pulls back.

What's more, fundamentally SAIC is undervalued trading at a low P/E of 9.19 on forward basis. That is heavily discounted for a company that boasts a return on equity of 23%. At 12.5X 2012 earnings on the low end (\$1.30/share) that makes SAIC easily worth \$16.25/share. On the upside at a \$1.40 SAI is worth \$17.50/share offering investors 37% upside with little downside risk.

- **Buy SAIC Inc. (NYSE: [SAI](#)) under \$13.00/share with a 10% stop/loss.**
- **Price Target: \$17.50**

**But no matter how you decide to play it, one thing is for certain: cyber security is critical to the battlefield of tomorrow.**

After all, war is not something we can simply wish away...

Your bargain-hunting analyst,



Steve Christ, Editor

*Wealth Daily*

You can view the HTML version here: [21st Century Blitzkrieg: Winning Investment from the Cyberwar](#)

[Energy and Capital](#). Copyright © [Angel Publishing LLC](#). All rights reserved. The content of this site may not be redistributed without the express written consent of Angel Publishing. Individual editorials, articles and essays appearing on this site may be republished, but only with full attribution of both the author and Energy and Capital as well as a link to [www.energyandcapital.com](http://www.energyandcapital.com). Your privacy is important to us -- we will never rent or sell your e-mail or personal information. No statement or expression of opinion, or any other matter herein, directly or indirectly, is an offer or the solicitation of an offer to buy or sell the securities or financial instruments mentioned. While we believe the sources of information to be reliable, we in no way represent or guarantee the accuracy of the statements made herein. [Energy and Capital](#) does not provide individual investment counseling, act as an investment advisor, or individually advocate the purchase or sale of any security or investment. The publisher, editors and consultants of Angel Publishing may actively trade in the investments discussed in this publication. They may have substantial positions in the securities recommended and may increase or decrease such positions without notice. Neither the publisher nor the editors are registered investment advisors. Subscribers should not view this publication as offering personalized legal or investment counseling. Investments recommended in this publication should be made only after consulting with your investment advisor and only after reviewing the prospectus or financial statements of the company in question.