

Aerospace & Defense

Fall 2010

Cyber Security Growth and Its Impact on M&A Activity

As information technology continues to quickly become a pervasive aspect of modern warfare, cyber security has recently risen in importance for federal, state, and local governments as well as the private sector.¹ Cyber security represents the strategic initiatives taking place to secure the nation's cyber infrastructure, which includes thousands of interconnected computer servers, routers, switches, and fiber optic cables that allow both public and private organizations' critical infrastructures to operate.² President Obama has declared cyber security as one of the most serious economic and national security threats for the United States and is allocating an unprecedented amount of attention and resources to cyber security matters.³

Increasingly, the nation's critical infrastructure is becoming the target of hackers. During 2008, there were 54,640 total cyber attacks against the U.S. Department of Defense (DoD). The number of attacks increased significantly in 2009 resulting in 43,785 reported cyber incidents targeting the DoD in just the first half of 2009 (latest available results).⁴ In 2008 and 2009, the United States ranked as the top country to fall victim to malicious cyber activity according to Symantec Corporation.⁵

The private sector is also coming under cyber attack as global conglomerate Siemens AG recently discovered a

computer virus designed to attack the industrial control systems it makes to help monitor power grids and other key infrastructure. The virus, first detected in July 2010, marked the first large-scale attack on industrial computer systems that are used to monitor controls for large automated factories, utilities, nuclear power plants, and water treatment systems, according to those close to the situation. The virus attack is likely to result in additional pressure on Siemens and other makers of industrial control systems, such as GE and Emerson Electric to reevaluate and boost safeguards to such systems, many of which were engineered at least 10 to 15 years ago.⁶ Additionally, Intel Corporation, a provider of integrated circuits for computing and communications industries, was recently hit by a "sophisticated" cyber attack in January 2010, around the same time Google Inc., a Web technology company, said hackers attacked its systems, resulting in the loss of intellectual property.⁷

In an effort to address the threats to the nation's cyber infrastructure, the federal government has increasingly allocated more funds to fighting cyber terrorism. In February 2010, the Obama administration released its fiscal year 2011 Department of Homeland Security (DHS) budget of US\$56.3 billion, which represents a 2 percent increase from fiscal year 2010, of which over US\$400 million has been allocated to increase

the resiliency and security of private and public sector cyber infrastructure.⁸ According to the Office of Management and Budget, the U.S. government spent approximately US\$6 billion on cyber security in 2009. The Homeland Security Research Corporation estimates that, in addition to the federal spending, the entire U.S. homeland security market, which includes federal, state, and local governments, intelligence agencies, and the private sector, will grow from US\$69 billion in 2010 to US\$85 billion by 2014,⁹ of which an increasingly larger portion is expected to be allocated to cyber-related defense.

Among the numerous initiatives being undertaken, one of the most notable is the DHS's establishment of the National Cyber Security Division (NCS) in 2004 under the authority of Homeland Security Presidential Directive-7, which establishes a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. The NCS oversees the Federal Network Security (FNS) branch, which serves as

¹ Alexander, John B. "The Changing Nature of Warfare, the factors Mediating Future Conflict, and Implications for SOF" Joint Special Operations University, November 2005.

² *The National Strategy to Secure Cyberspace*, Department of Homeland Security, February 2003.

³ Gorman, Siobhan. "U.S. Hampered in Fighting Cyber Security Attacks, Report Says," *The Wall Street Journal*, June 16, 2010.

⁴ *U.S.-China Economic and Security Review Commission*.

⁵ *Symantec Global Internet Security Threat Report, Trends for 2009*, Volume XV.

⁶ *Siemens AG Press Release*, April 2010.

⁷ Dicolò, Jerry. "Intel Says It Was Target of Cyber Attack," *The Wall Street Journal*, February 23, 2010.

⁸ *Budget-in-Brief FY 2011*, Department of Homeland Security.

⁹ *U.S. Homeland Security - Homeland Defense (HLS-HLD) Markets - 2010 - 2014*, Homeland Security Research Corporation.

the single, accountable focal point for achieving an enterprise model dedicated to federal cyber infrastructure security and Cyber-Risk Management Programs, which include a National Outreach Awareness Month.⁹ In April 2009, the White House announced the creation of a position called the “Cyber Security Coordinator” (known colloquially as the Cyber Czar), who will manage a more centralized and “top-down” approach to the U.S. government’s interagency cyber security process and make recommendations for the nation’s cyber policies and standards.¹⁰ More recently, The National Security Agency (NSA) announced the launch of a program dubbed “Perfect Citizen” in July 2010 to detect cyber assaults on private companies and government agencies running such critical infrastructure as the electricity grid and nuclear-power plants. The surveillance by the NSA would rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack.¹¹

Further example of cyber security’s importance is the announcement in October 2009 by the DHS that the agency has been cleared to hire at least 1,000 new cyber security professionals over the next three years to fill critical cyber security roles. The positions include cyber analysts, developers, and engineers in the areas of cyber risk and strategic analysis, cyber incident response, vulnerability detection and assessment, intelligence and investigation, and network and systems engineering.¹² These positions will be hard to fill as qualified professionals are few and far between. According to a newly published report from the Center for Strategic and International Studies, “the current professional certification regime (for cyber security professionals) is not merely inadequate; it creates a dangerously false sense of security.” This trend has emerged because individuals and employers are

spending scarce resources on credentials that don’t demonstrably improve the ability to address security-related risks; credentials are currently focused on demonstrating expertise in documenting compliance with policy and statutes, rather than expertise in actually reducing risk through identification, prevention, and intervention.¹³

Large security contracts are being awarded as a result of the increased focus on cyber security. The Federal Bureau of Investigation (FBI) awarded a five-year, US\$99.5 million cyber security contract to Fairfax, VA-based ManTech International, a provider of solutions for national security programs.¹⁴ Northrop Grumman Corporation, a provider of defense products and solutions, won a contract for the Defense Advanced Research Projects Agency’s (DARPA) National Cyber Range (NCR), which will provide an environment to test and analyze new concepts and technologies to protect against modern cyber threats.¹⁵

The recent attention on cyber security already has and is expected to continue to have a significant impact on merger & acquisition activity in the sector. The federal government has made it increasingly clear that the new procurement standards will call for companies to work to lower costs and risks given the current economic budgetary constraints. Progressively more, the federal government and the DoD are moving away from large procurements of major weaponry and vehicular systems in favor of investing in high-tech equipment in C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance) to combat terrorism both on domestic and foreign lands and America’s cyberspace. As a result, the traditional strategic defense players and financial buyers are looking towards acquisitions to get exposure to the new directives coming from Washington. Representative transactions include IT services provider CGI Group, Inc.’s

recent acquisition of Stanley, Inc., a provider of information technology services and solutions to the United States defense, intelligence, and federal civilian government agencies, for an implied enterprise value of US\$1.1 billion and a valuation of 1.2x revenue and 11.6x EBITDA.¹⁶

The Stanley acquisition represents a major push by IT technology companies to get exposure to defense technology. Additionally, CACI International Inc., a provider of IT services to the government, completed the acquisition of SystemWare Inc., a cyber security company, in January 2010 for an undisclosed sum. The acquisition comes as the federal government steps up its focus on cyber security. SystemWare’s clientele includes the DoD, federal agencies, and members of the intelligence community. The company makes systems that help users monitor and detect cyber security and physical security issues. It recorded US\$16 million in revenue during 2009.¹⁷

Raytheon Company acquired Oakley Networks, a provider of military-grade and infrastructure solutions for protecting data assets, intellectual property, and infrastructure to federal and commercial customers, in 2007¹⁸ and subsequently SI Government Solutions, Inc., a provider of custom information-security solutions for intelligence and defense communities, in 2008.¹⁹

Other active acquirers of cyber security assets include Boeing, which acquired Narus, Inc., a provider of software solutions for the protection and management of Internet protocol networks, in July 2010,²⁰ and SAIC,

¹⁰ U.S.-China Economic and Security Review Commission.

¹¹ “U.S. Plans Cyber Shield for Utilities, Companies,” *The Wall Street Journal*, July 8, 2010.

¹² Krebs, Brian. “DHS Seeking 1,000 Cyber Security Experts,” *Security Fix*, October 1, 2009.

¹³ DePompa, Barbara. “A Cybersecurity Crisis Looms,” *Government Computer News*.

¹⁴ *Mantech International Corporation Press Release*, August 16, 2010.

¹⁵ *Northrop Grumman Corporation Press Release*, January 13, 2009.

¹⁶ Cole, August. “Defense Firms Pursue Cyber Security-Work,” *The Wall Street Journal*, March 2009.

¹⁷ *CACI International, Inc. Press Release*, February 1, 2010.

¹⁸ *Raytheon Company Press Release*, October 23, 2007.

¹⁹ *Raytheon Company Press Release*, April 18, 2007.

²⁰ *Narus, Inc. Press Release*, July 7, 2010.

Inc., which acquired CloudShield Technologies, a provider of IP service control and infrastructure protection solutions, in February 2010 for an implied enterprise value of US\$140 million.²¹

Foreign firms are also trying to edge into the marketplace. Europe's biggest defense contractor by revenue, BAE Systems PLC, acquired information security firm Detica Group PLC for

US\$1.06 billion in July 2008. BAE also recently hired a top Bush White House cyber security official, Marie O'Neill Sciarrone.²²

It is clear that cyber security will continue to be a top priority for federal, state, and local governments and private companies as cyber security attacks increase and the need to address vulnerabilities becomes paramount. Given the increased resources being allocated to

cyber security, companies will continue to expand organically and through strategic acquisitions to better position themselves to win future cyber security work. Moreover, federal, state, and local governments will continue to rely on the private sector to service its aging IT infrastructure and help position the nation to fight and win the future battles in cyberspace.

²¹ CloudShield Technologies, Inc. Press Release, February 9, 2010.

²² Cole, August. "Defense Firms Pursue Cyber Security-Work," The Wall Street Journal, March 2009.

Market Snapshot										
Company	Market Cap ^{1,4}	Share Price ¹	52 Wk Low	52 Wk High	1 Mo Price % Change	1 Yr Price % Change	Debt to TC	Price to BV	EV ² /Sales	EV ² /EBITDA ³
S&P 500										
BOEING CO.	51,820.1	70.6	47.3	76.0	6.2%	47.8%	73.2%	11.6	0.8	7.7
GENERAL DYNAMICS CORP.	25,731.9	68.1	55.5	79.0	8.5%	8.6%	19.1%	1.9	0.9	6.2
GOODRICH CORP.	10,289.5	82.1	53.9	83.0	11.3%	51.0%	44.0%	3.1	1.7	9.4
HONEYWELL INTERNATIONAL INC.	36,754.0	47.1	35.6	48.6	7.2%	31.3%	40.9%	3.6	1.3	9.9
LOCKHEED MARTIN CORPORATION	25,673.6	71.3	67.9	87.2	0.0%	3.6%	56.2%	6.6	0.6	5.1
NORTHROP GRUMMAN CORPORATION	18,459.5	63.2	49.6	69.8	4.3%	26.1%	24.2%	1.4	0.6	5.5
RAYTHEON CO.	16,798.1	46.1	42.7	60.1	0.8%	1.8%	18.5%	1.7	0.7	5.8
ROCKWELL COLLINS INC.	9,512.1	60.5	47.2	68.0	3.9%	20.1%	27.0%	6.5	2.1	9.9
UNITED TECHNOLOGIES CORP.	69,043.1	74.8	61.4	77.1	5.0%	21.7%	35.3%	3.2	1.4	8.0
S&P 500 Mean					5.2%	23.6%	38%	4.4	1.1	7.5
S&P 500 Median					5.0%	21.7%	35%	3.2	0.9	7.7
OTHER PRIMES/SYSTEMS SUPPLIERS										
BAE SYSTEMS PLC	18,805.5	5.5	4.6	6.2	2.6%	7.1%	61.9%	2.9	0.6	3.9
BOMBARDIER, INC.	8,600.6	5.0	4.2	6.1	1.9%	22.6%	54.9%	2.5	0.6	7.0
EUROPEAN AERONAUTIC DEFENCE	21,299.6	26.3	15.9	27.4	5.7%	39.9%	47.0%	3.0	0.2	16.6
EMBRAER - EMPRESA BRASILEIRA	5,219.4	28.9	19.1	29.7	1.6%	42.5%	38.6%	1.8	1.0	11.8
FINMECCANICA SPA	8,050.9	14.0	10.7	16.8	17.8%	-29.9%	49.3%	0.9	0.6	6.0
THALES	7,960.6	40.8	34.8	50.0	11.9%	-16.0%	32.2%	1.5	0.5	10.1
Other Primes/Systems Suppliers Mean					6.9%	11.0%	47%	2.1	0.6	9.2
Other Primes/Systems Suppliers Median					4.2%	14.8%	48%	2.1	0.6	8.6
AVIONICS/ELECTRONICS										
ALLIANT TECHSYSTEMS INC.	2,530.9	76.2	60.1	90.8	1.1%	-2.0%	59.8%	2.9	0.8	5.9
DRS DATA & RESEARCH SERVICES PLC	11.0	0.3	0.2	0.4	0.7%	36.8%	32.0%	1.4	0.3	3.8
HARRIS CORP.	5,796.9	45.2	40.2	54.5	2.0%	8.3%	38.8%	2.5	1.3	5.8
HERLEY INDUSTRIES INC.	229.1	16.6	10.1	17.0	0.7%	46.9%	7.1%	1.4	1.1	7.4
L-3 COMMUNICATIONS HOLDINGS INC.	8,262.4	72.2	66.1	97.8	-0.1%	-0.2%	37.2%	1.2	0.8	6.1
CAE INC.	2,880.7	11.2	8.2	11.5	9.1%	43.8%	29.4%	2.5	2.1	9.3
ULTRA ELECTRONICS HOLDINGS PLC	2,043.5	29.8	19.2	30.3	11.3%	37.8%	27.3%	6.3	1.9	11.7
Avionics/Electronics Mean					3.5%	24.5%	33%	2.6	1.2	7.1
Avionics/Electronics Median					1.1%	36.8%	32%	2.5	1.1	6.1
COMPONENTS (LARGE CAP)										
COBHAM PLC	4,279.6	3.7	3.3	4.5	2.2%	3.0%	42.2%	2.8	1.6	7.6
CURTISS-WRIGHT CORP.	1,422.7	30.9	26.1	37.5	1.9%	3.6%	31.8%	1.3	1.0	7.1
ESTERLINE TECHNOLOGIES CORP.	1,817.9	60.4	36.8	61.0	5.6%	43.5%	29.0%	1.4	1.4	8.5
MEGGITT PLC	3,666.8	5.3	3.7	5.3	13.6%	31.6%	39.4%	1.7	2.8	11.2
MOOG INC.	1,705.9	37.6	24.3	40.2	5.9%	106.7%	41.2%	1.5	1.2	9.0
PRECISION CASTPARTS CORP.	19,427.8	136.6	93.0	141.2	7.2%	611.7%	3.9%	3.2	3.4	12.1
ROLLS ROYCE GROUP PLC	19,217.2	10.4	7.0	10.5	9.3%	-48.7%	38.5%	3.8	1.0	8.2
SMITHS GROUP PLC	7,461.6	19.1	14.2	20.8	-0.4%	-10.0%	47.9%	4.2	2.0	9.7
TEXTRON INC.	5,723.4	20.8	15.9	25.3	1.3%	-6.2%	68.1%	1.9	1.1	12.6
ZODIAC AEROSPACE SA	3,738.9	70.6	30.9	74.3	11.7%	108.8%	35.0%	2.0	1.6	13.2
Components (Large Cap) Mean					5.8%	84.4%	38%	2.4	1.7	9.9
Components (Large Cap) Median					5.7%	17.6%	39%	2.0	1.5	9.4
COMPONENTS (MID CAP)										
DUCOMMUN INC.	225.4	21.5	16.0	24.3	-1.4%	26.1%	7.9%	0.9	0.6	5.3
HEROUX-DEVTEK INC.	176.5	5.9	4.8	6.1	-1.5%	26.2%	31.9%	0.8	0.8	5.4
MAGELLAN AEROSPACE CORP.	49.0	2.7	1.2	3.2	4.8%	118.3%	48.5%	0.2	0.4	4.1
TRIUMPH GROUP INC.	2,022.2	83.6	46.2	84.3	12.1%	78.6%	47.7%	1.5	2.4	14.8
Components (Mid Cap) Mean					3.5%	62.3%	34%	0.9	1.1	7.4
Components (Mid Cap) Median					1.7%	52.4%	40%	0.9	0.7	5.4
MRO/AFTERMARKET SERVICES										
AAR CORP.	865.4	22.0	14.9	26.1	18.1%	12.4%	37.0%	2.3	0.9	8.3
HEICO CORP.	1,389.4	49.8	29.6	50.8	9.1%	63.6%	7.4%	7.3	2.6	12.9
MRO/Aftermarkets Services Mean					13.6%	38.0%	22%	4.8	1.8	10.6
MRO/Aftermarkets Services Median					13.6%	38.0%	22%	4.8	1.8	10.6
TOTAL AEROSPACE INDUSTRY MEAN										
TOTAL AEROSPACE INDUSTRY MEDIAN										
					5.6%	42.6%	37%	2.8	1.2	8.5
					4.9%	26.1%	38%	2.1	1.0	8.1
1	Market Capitalization amounts are in millions, based on closing Share Prices as of October 31, 2010									
2	Enterprise Value (EV) equals Market Capitalization plus Debt, Preferred Equity, and Minority Interest, minus Cash and Cash Equivalents									
3	EBITDA equals Earnings before Interest, Taxes, Depreciation, and Amortization									
4	Market Capitalization and Share Prices are based on foreign exchange listed securities and converted to US\$									

Select Aerospace & Defense Transactions

- June 30, 2010 – **Boeing Co.** (NYSE: BA), a manufacturer of commercial jetliners, military aircraft, satellites, missile defense, human space flight, and launch systems and services worldwide, acquired **Argon ST, Inc.**, a provider of systems engineering, development, and services, for US\$799.2 million. The transaction implies a valuation multiple of 2.3x LTM April 2010 revenue and 18.1x LTM April 2010 EBITDA. (Source: *Capital IQ*)
- August 3, 2010 – **Goodrich Corp.** (NYSE: GR), a supplier of aerospace components, systems, and services, acquired the cabin management assets of **DeCrane Aerospace, Inc.**, provider of seating, furniture, veneers, and cabin management systems for the business jet market, for US\$280 million. The transaction implies a valuation multiple of less than 8.0x 2010 estimated adjusted EBITDA. (Source: *Capital IQ*)
- August 9, 2010 – **Wyle**, a provider of aerospace engineering, information technology consulting, and life sciences services and portfolio company of **Court Square Capital Partners**, a private equity firm, acquired **CAS, Inc.**, department of defense weapon system analysis contractor, for US\$235 million. (Source: *Capital IQ*)
- August 10, 2010 – **Chemring Group plc** (LSE: CHG), a manufacturer of energetic material products and decoy counter-measures, acquired **Roke Manor Research Limited**, a provider of technology consulting services, product development, and life solutions in sensors, information systems, and communications, for US\$86.6 million. The transaction implies a valuation multiple of 1.2x LTM September 2009 revenue. (Source: *Capital IQ*)
- August 11, 2010 – **Kratos Defense & Security Solutions, Inc.** (NASDAQ: KTOS), a provider of engineering, information technology services, and war-fighter solutions, acquired **DEI Services Corporation**, a provider of simulation and training devices to the military sector, for US\$6 million. The transaction implies a valuation multiple of 4.0x EBITDA. (Source: *Capital IQ*)
- August 16, 2010 – **FLIR Systems, Inc.** (NASDAQ: FLIR), a manufacturer of thermal imaging and stabilized camera systems, acquired **ICx Technologies, Inc.**, a developer and integrator of advanced sensor technologies for homeland security, force protection, and commercial applications, for US\$264 million. The transaction implies a valuation multiple of 1.3x LTM June 2010 revenue. (Source: *Capital IQ*)

KPMG Corporate Finance LLC

KPMG Corporate Finance LLC provides a broad range of investment banking and advisory services to its domestic and international clients. Our professionals have the experience and depth of knowledge in global M&A and project finance to advise clients on mergers and acquisitions, sales and divestitures, buyouts, financings, debt restructurings, equity recapitalizations, infrastructure project finance, and other advisory initiatives. In addition, we remain

independent of financing sources, helping to ensure that our efforts are objective and aligned with the goals of clients.

Operating in 62 countries, KPMG International's member firms' corporate finance practices (KPMG) comprise more than 2,200 professionals who are able to meet the needs of clients across the globe. In 2009, as a leading financial adviser, KPMG completed 260 deals totaling US\$119.7 billion, according to Thomson Reuters SDC's global M&A league tables.



Semco Instruments, Inc.

KPMG Corporate Finance LLC
acted as financial adviser to
Semco Instruments, Inc. on its
sale to TransDigm Group
Incorporated

US\$74 million
September 2010

Contact

Los Angeles

Terence Yeh

Managing Director
1-213-817-3128
tyeh@kpmg.com

We welcome the opportunity to meet with you, learn more about your company's objectives, and discuss our people and capabilities.

KPMG Corporate Finance LLC — We Can Do a Great Deal Together.

KPMG Corporate Finance LLC is a leading middle market adviser serving domestic and international clients. We offer a broad range of investment banking and strategic advisory services. Visit us online at www.kpmgcorporatefinance.com.

Corporate finance services, including Financing, Debt Advisory, and Valuation Services, are not performed by all KPMG member firms and are not offered by member firms in certain jurisdictions due to legal or regulatory constraints. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2010 KPMG Corporate Finance LLC, a Delaware limited liability company, is a member of FINRA and SIPC and is registered as a broker dealer with the SEC. KPMG Corporate Finance LLC is a subsidiary of KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A.

KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative ("KPMG International"), a Swiss entity.