The Business of Connecting Dots:

The $1 Billion Intelligence and Security Informatics/Analytics Market

A CEUT-CIC Security Insights Report

C.E. UNTERBERG, TOWBIN

CHESAPEAKE Innovation Center

C.E. Unterberg, Towbin / Chesapeake Innovation Center

November 17, 2005

Table of Contents

Executive Summary

From special forces units hidden in the mountains of Afghanistan to huge federal agencies ringing the "Washington Beltway," from the research labs of pharmaceutical giants to the call centers of Fortune 1,000 businesses, America's most important organizations are drowning in a tidal wave of data. Companies with solutions that can transform that data into knowledge will help prevent terrorist attacks, cure diseases, and increase corporate revenues – and build substantial value for themselves and their shareholders.

Intelligence and Security Informatics/Analytics (ISI)

The events of 9/11 highlighted the urgency of "connecting the dots" to prevent and combat terrorism. The need for vastly improved capabilities to collect, analyze and share information was reinforced by the national analytical failure regarding the presence of WMD in Iraq. These and other factors have generated vast budgets for informatics solutions – technologies that can derive knowledge from immense data sets and help humans cope with "information overload." This report describes and sizes the Intelligence and Security Informatics/Analytics (ISI) market, profiles key public and private solution providers, outlines market drivers and describes potential growth constraints. Our focus is on analytical technologies used to detect terrorist and criminal activities. Such technologies may be stand-alone or embedded in larger solutions - such as intelligent video surveillance, access control, or specialized data storage - that depend upon informatics technology to produce value. In these cases, it is the informatics technology, rather than the often commoditized underlying hardware, that differentiates the solution and boosts sales and valuations.

Convergent Informatics Markets

While their need is especially pressing and their budgets expanding, ISI customers represent just one market for informatics. Other large informatics markets include health sciences, where medical and pharmaceutical organizations use bio-informatics technologies to optimize treatments, develop drugs, and detect health hazards such as avian flu, and business intelligence, which harnesses informatics to increase operating efficiencies and ensure compliance with regulations. While the objectives of these user groups vary widely, the tools used for these activities are often the same. This creates an opportunity for companies to create "dual benefit" technologies that focus on multiple markets. We call these combined sectors — which represent billions of dollars in spending — the "Convergent Informatics Market."

Unstructured Data Mining and Other Breakthroughs

The sub-sectors of the convergent informatics market share the need for common solutions to pressing requirements. One is the challenge posed by mining "unstructured data," or information that cannot be stored in the rows and columns of traditional databases. Unstructured data includes text, audio, video, email and graphics. It is estimated that 80% to 85% of the information that flows through organizations is unstructured; this is especially true for many security organizations, which frequently capture data through surveillance and wiretapping technology in the form of video, audio and electronic signals. Powerful new solutions are emerging to mine unstructured data, including advances that allow the emotional content of written and spoken

data to be mined. In other words, software can detect, analyze and support decisions based upon the emotional state of the person writing the email or making the phone call. We call this "affect mining" and it is just one of the breakthroughs now emerging in the informatics arena.

Market Drivers, Size and Performance

Key factors driving the ISI and convergent markets include:

- More powerful and/or cheaper computing and storage technologies
- Huge increases in information production from email and Web chat to video and mass media
- Growing regulatory, compliance and liability pressures
- Growth of "intelligent" sensor systems, from video cameras to biometric readers, that employ analytical software to identify patterns and matches
- Urgent requirements and increased funding for "actionable intelligence" and information sharing for homeland security and the Global War On Terrorism (GWOT)

These factors have generated what we estimate is a $1 billion market expanding at a compound annual growth rate (CAGR) of 20%. ISI transactions have accounted for some $2 billion in M&A activity over the past 18 months. The stock market has taken note. We have created the CEUT ISI Stock Index, which compared to our over-all CEUT Global Security Index and the four traditional stock indices has substantially outperformed the market. The ISI Index returned 90% in 2003, 54% in 2004, and 10.8% in 2005 (as of Nov. 11) - the only index of the six to show a positive return so far in 2005 (see more detail and a chart later in this report).

The ISI market is not just important to corporations, government agencies, financial institutions and investors. It is also critical to every American citizen who is concerned about his or her safety and civil liberties. In addition, as the tidal wave of data continues to cascade from organizations into the lives of individual citizens, "convergent" informatics solutions will increasingly be used in the private sector, including by individual consumers as they attempt to manage the flood of data in their personal lives, from finances to health care and communications.

The Tidal Wave of Data

Enterprises at all levels of government and the private sector are creating, collecting and storing more data than ever before. The trend extends across the globe. According to a U.C. Berkeley estimate, more than five exabytes of new information (10^{18} bytes) are created every year worldwide – enough to fill 37,000 new Libraries of Congress and more than all the words ever spoken or printed. This is the annual equivalent of a 30 foot stack of books for every man, woman, and child on the planet.

Perhaps nowhere is unstructured data piling up faster than at American security organizations tasked with winning the war on terrorism. They are inundated with an unprecedented "volume, velocity and variety," or "3Vs," of data, causing massive "information overload." According to congressional testimony and other public sources, U.S. security agencies are collecting far more information than they are able to process.

A good example is the National Security Agency (NSA). Reported to be America's largest intelligence organization, the NSA is responsible for intercepting enemy communications and breaking their codes. This entails a global, multi-media, multi-lingual intelligence collection and analysis effort of enormous scope and complexity. The amount of information processed by the Agency is classified, but Dr. Eric Haseltine, then head of research at NSA, stated in a 2004 speech that NSA's data challenges are far beyond those seen by leading IT companies. Even the legendary "big iron" of NSA's massive computer systems has trouble keeping up.

"We in the NSA are encountering problems with the flood of information that people (in the outside world) won't see for a generation or two," said Haseltine, now a senior official in the Office of the Director of National Intelligence. "We've been into the future and we've seen the problems" of a "tidal wave" of data, Haseltine commented, adding: "We can either be drowned by it or we can get on our surfboard and surf it and let it propel us. And, of course, that's what we're trying to do."

Similar if less dramatic challenges exist at other federal, state and local agencies and commercial organizations. Factors driving increased data production and collection include:

Wiretapping activity – the capturing of communications made by suspected terrorists or criminals - will grow 20-25% per year as new high-speed data and packet-based networks generate incremental demand for wiretapping software. This market is at historically high levels. It will accelerate if, as we believe, the 1994 Communications Assistance for Law Enforcement Act (CALEA), which facilitated telephonic wiretapping, is extended to IP/packet networks (including VOIP) communications channels next year.

The deployment of **intelligent video surveillance** monitoring systems in governmental and commercial facilities might be the most prolific of all security measures post-9/11. Video security systems accounted for three out of every four corporate security purchases in 2004. The number of public surveillance systems around the world is expected to grow by 20% annually over the next six years, generating about $7.5 billion in revenues for system providers by 2008. The transition from analog to digital video systems is lowering system costs, significantly improving data archival and retrieval, and enabling video networking across multiple sites using the Internet. It also provides real-time alert capability by enabling intelligent data analysis at the camera level, such as motion and behavior detection. Examples include Motion Detection (the camera identifies a passenger walking the wrong way through a security checkpoint and sends out a streaming video of the passenger's face to a security guard), Behavior Detection (a camera identifies a man dropping off a briefcase in front of an elevator bank – the camera recognizes this as an "unattended baggage alert" and sends a video frame of the bag and man in

question to a security guard) and Loss Prevention (a camera recognizes a shopper stuffing clothing into a briefcase and attempting to leave the store).

Defense Transformation and "Network-centric Warfare" (NCW): The goal of NCW is to network sensors, decision makers and "shooters" to achieve greater "situational awareness" of the battlefield. A key in moving to "netcentricity" is networking operators and intelligence, which includes transforming shooters into sensors. This will require ISI software and be facilitated by the Global Information Grid (GIG), a massive Pentagon project that will in turn drive more data.

Legal, regulatory and compliance requirements such as the USA Patriot Act place demands on corporations to understand their customers and data in order to prevent money laundering and other terrorist activities. Combined with Sarbanes Oxley, these regulations create major data collection and analysis requirements.

Increasingly government and corporate customers are realizing that without innovative informatics solutions, all these data sets will simply create "information overload," at best wasting storage space and at worst clogging the decision making process or losing key clues that could enhance efficiency, prevent financial loss or – in the most significant case – forestall attack or win battles.

The ISI Market: Size and Drivers

Our report is the first to define and size the ISI market. We approached this challenge by analyzing numerous public and private companies, public filings, government contracts, media reports, and other data to identify ISI products and services. In addition, we visited and/or interviewed executives from some of these companies and others knowledgeable about the market.

Defining ISI

Our definition of ISI covers technologies that help derive knowledge from vast amounts of data. Specific solutions include certain artificial intelligence & expert systems; collaboration technology; analytics and mining for structured, semi-structured and unstructured data; intelligent video surveillance software; wiretapping; intelligence and defense signal interception software; biometric access control software; decision support/optimization; multi-media, multi-language processing; search and fusion; predictive analysis; search; visualization; and selected enabling technology (sensors and remote sensing, massive storage, data transfer optimization, machine translation, etc).

We focused on products and services that incorporate analytical software as a central differentiating component and eliminated hardware revenues that are frequently part of an overall systems sale. Revenues from service and maintenance contracts are included in our evaluation.

$1 Billion Market

We estimate that in 2005, the market for data analytics software solutions – addressable spending by government and corporate customers - will reach or exceed $1 billion in size. Going forward, we forecast that the market will grow at a 20% CAGR over the next five years, resulting in a market larger than $2 billion by 2009.

Examples of Government Spending

The size of the market is demonstrated by recent federal contracting activities involving informatics. For example, our survey of recent government contracting actions shows numerous data mining efforts related to intelligence and security. The Air Force announced in 2004 a five year, $36 million project focused on "Rapid Processing of Intelligence Data." The program includes efforts to develop "revolutionary techniques" for processing huge databases. The Pentagon plans another project with a budget of up to $49.9 million to develop a software toolkit providing a data visualization and analysis infrastructure. The Navy has been identifying providers to provide data fusion services connected to Maritime Domain Awareness (MDA), or the tracking of ships and boats around the world.

In May 2004, a government survey identified 199 federal "data mining" efforts planned or underway. 29 focused on analyzing terrorist and/or criminal activities; the rest were being used to analyze data such as genetic information, government oil and gas leases, and human resource records. However, this list did not include data mining programs at the CIA and NSA and also excluded classified projects.

America's annual intelligence budget, while classified, is believed to be $44 billion, up from $26.7 billion in FY 1998. Classified Pentagon spending has also increased rapidly over recent years and reportedly approaches $27 billion. We assume numerous major ISI projects are funded by these budgets, although because of sensitivities involving classified spending this report does not attempt to break down such expenditures more specifically.

Perhaps the largest publicly known ISI-related spending program is the NSA's Trailblazer Contract, which is said to be valued in the billions of dollars. Launched in 2000, the program was reportedly designed to help the Agency deal with the huge volume, velocity and variety of data it was collecting from sources ranging from mobile phone intercepts to satellite intelligence gathering. "(T)he more success you have with regard to collection, the more you're swimming in an ocean of data," testified Gen. Michael Hayden, Principal Deputy Director of National Intelligence and former director of the NSA, during a 2005 congressional hearing. "So what Trailblazer was essentially designed to do was to help us deal with masses of information and to turn it into usable things for American decision- makers."

According to congressional testimony, an SEC filing, and media reports, the NSA has almost certainly committed some $700 million to Trailblazer contractors over recent years. SAIC, Inc.'s recent S-1 filing reports the "total contract value" of its share of Trailblazer at $348 million

through April 2006. Prior to this filing, the company was publicly known to have won a $280 million Trailblazer contract with a team including Northrop Grumman, Boeing and Booz Allen Hamilton. Conquest Inc. has reportedly received $197 million in Trailblazer contracts. Gen. Hayden testified that additional, unforeseen Trailblazer costs could exceed $200 million, although it is unknown whether some of these over-runs are included in SAIC's increased reported contract value.

Such ISI spending, and convergent market expenditures from organizations such as the National Institutes of Health and FDA, are spurring rapid economic development, employment growth and corporate value creation in the region dubbed the "Informatics Corridor," centered at NSA headquarters in Anne Arundel County, Maryland, and spreading across the "Washington Beltway" to encompass DHS; IC members such as the CIA, DIA, NRO and NGA; various federal labs; and researchers at institutions such as Johns Hopkins University and the University of Maryland.

Major Opportunities on the Horizon

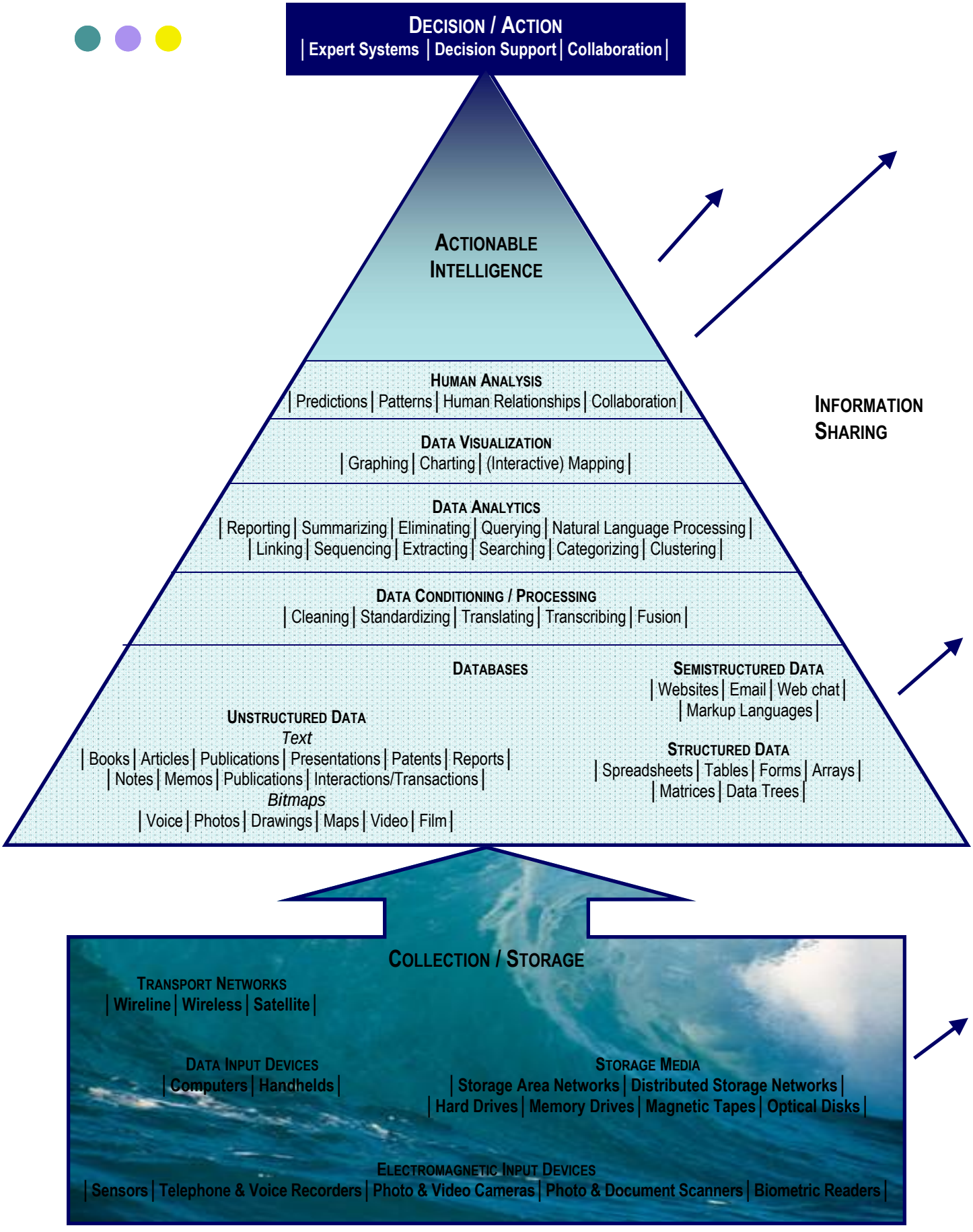
We expect continuing and new federal programs, and to a lesser extent ISI procurements at the state and local level, to drive substantial opportunities in 2006 and beyond.

The new Office of the Director of National Intelligence is gaining traction as a driver of innovative technology solutions. The Department of Homeland Security has consolidated its own intelligence operations; its $40.6 billion FY-06 budget contains hundreds of millions of dollars for activities involving intelligence and warning. The Department's new Secretary, Michael Chertoff, is also known as an early proponent of ISI in his days pursuing terrorism for the Department of Justice after 9/11. ISI technology will be required by other major homeland security-related activities such as the on-going U.S.-Visit program to screen international visitors; the forthcoming Border Security Initiative (BSI); maritime security programs; money laundering prevention; information sharing projects; watch list screening operations; the multi-billion dollar effort to prevent an avian flu pandemic; and many others.

In response to these and other factors, major corporations continue to enter the market. In August, data storage giant EMC announced the Surveillance Analysis and Management Solution (SAMS) system to provide organizations with an integrated way to deal with vast amounts of surveillance data. That same month, IBM – which offers numerous informatics products - announced the open source release of its Unstructured Information Management Architecture (UIMA), developed with the Defense Advanced Research Projects Agency (DARPA), a significant funder of ISI research. The technology supports new applications for text search and unstructured data analytics. Microsoft and Motorola in October announced an alliance to offer the law enforcement sector "a unified architectural approach to integration and information-sharing that meets the security and interoperability requirements of comprehensive government information systems of all sizes, types and standards." Even Google has begun to explore the ISI market.

This movement appears certain to accelerate if SAIC - a major ISI provider to the federal government - succeeds in its plans to raise almost $2 billion in an IPO next year.

THE ISI PROCESS



Technology Solutions

Informatics responds to the reality that human analysis is not "scalable" – there is just too much raw data for an analyst, or an army of analysts, to process manually. One solution is to surround human analysts with "machine reasoning" tools that augment human capacity. Such technology can process data before it is even seen by a human being and support the analytical process at all stages.

The ISI Process

The basic imperative for ISI is to transform electronic bits into actionable intelligence that drives decisions and actions. The process is depicted in the preceding chart.

The ISI process is commonly divided into steps that include data collection, storage, processing, analysis, retrieval, and dissemination. Some elements of the process are:

Collection/Storage: The foundation of the process involves the hardware and software that captures, inputs, stores, sends and receives data. This may range from a Top Secret satellite soaring above North Korea to a call center operator inputting a tip from a concerned citizen. Where possible, human analysis starts at this stage and continues throughout the ISI process. Computers and other handheld devices process data – often via human computer interfaces such as keyboards - and convert them to digital bit streams. Sensors, such as cameras, readers or satellites, convert electromagnetic signals to digital bits. The analytical process can be accelerated even at this stage; the sensor may be programmed to collect only the most important data and to share this information immediately in specific ways. For example, video surveillance systems may begin recording - and send an alert and picture to a security guard via his PDA - only when an anomaly is detected. The system can then track an anomaly, such as a suspicious person, as it moves through a coverage area. Processing of data collected by sensors can also be conducted at the "lowest" possible level so the "dots can be connected" without any human intervention. The video surveillance program might attempt to match the suspicious person with images in its database, a traffic camera system could identify the license plates and driving records of speeders, or a biometric system would match fingerprints of suspects in real time.

Once the data is captured, it is stored on hard drives, memory devices, magnetic tapes and optical discs. Storage devices may be connected to form storage area networks or distributed storage networks. Wireline, wireless and satellite networks transport data between dispersed locations for storage and retrieval. ISI "enabling" technologies such as advanced storage and data transfer solutions may be applied at this stage.

Databases: Information is aggregated into files that can be accessed, searched and managed by computer technology.

Data Conditioning/Processing: Raw data is prepared for data mining by such processes as cleaning, standardizing, translating, transforming, formatting and merging. Where possible, the data is fused to allow the analysis of different types of information.

Data Analytics: Data mining and related tools are used to find previously unknown patterns. For example, investigators use "link analysis" to identify and connect suspects by patterns in their email, phone calls, purchases, travel and other actions. Such analysis, focused in large part on the names of extended family members and tribal links, helped lead the U.S. military to Saddam Hussein's hiding place. Increasingly, existing data is also used to predict future activity ("predictive analysis").

The tools used depend in part on the form of the data:

"Structured data" refers to data already categorized into spreadsheets or standard databases.

"Semi-structured" data involves audiovisual material or text that includes some descriptive information, such as emails with headers that include names and dates. Information placed on Web sites using markup languages such as HTML or XML may be considered semi-structured.

"Unstructured data" includes audiovisual recordings and "free text," or words that have not been placed into categories such as fields with headers.

Unstructured Data Mining

Unstructured data sets present substantial challenges but often yield significant knowledge. Bitmap mining involves extracting useful information from audio, video and images. Spoken words are transcribed into text, where they can be analyzed using text mining tools. They may also be analyzed for other characteristics, from voice recognition to "affect mining" in which the tone and other features of speech are evaluated to determine the emotional state of the speaker. Image mining is the extraction of useful information from still or moving images. Analytical tools may be used to match patterns, such as facial characteristics, or detect changes or abnormalities.

Text Mining

Techniques used for mining unstructured data include: text summarization, which highlights key sentences in long documents; text categorization, which groups documents into pre-defined categories; text clustering, which links documents containing similar concepts; foreign language text mining, which clusters related documents even when the analyst cannot speak the language; and information or entity extraction, which identifies people, places, and organizations in data and the links among them. These "entities" can be employed to create "metadata," or labels linking data to specific categories – turning the unstructured data into semi-structured data.

Natural Language Processing

Many of these techniques depend on Natural Language Processing (NLP), which is related to Artificial Intelligence (AI). NLP processors try to emulate the human capability to "understand" spoken or written words. This can be extraordinarily complicated, as NLP programs must take into account issues such as grammar, colloquialisms, cultural factors and context. For example, an efficient NLP algorithm would need to understand that "Bob" may be the same person as

"Robert." Harbinger (a CIC member company) offers a related technology that matches foreign-language names on watch lists to prevent suspected terrorists from traveling or transferring money. It not only connects a single Arabic name to its various English language spellings, but also captures links from the genealogical information contained in many Arabic names. Advanced NLP programs also grasp context, such as determining whether the phrase "Julia is the bomb" is innocuous or a threat indicator, or discerning the critical phrase from the following comments: "Gas up the car for our trip to the Embassy. We'll be discussing natural gas at the Embassy reception. The Embassy reception will be a gas. We will gas the Embassy reception."

Predictive Analysis

Identifying patterns that can support reliable predictions about future actions or trends can produce the most valuable analytical products. This system employs a "predictive model" that identifies "predictors," or variable factors linked to future behavior. Often using advanced principles such as neural networks (based on how the human brain functions), fuzzy logic, or Bayesian networks, the model is continuously refined as additional data becomes available.

Predictive analytics can be used in real time by businesses to upsell or retain customers or detect fraud. For example, as a call center employee enters data from an upset customer, the system can recommend the offer most likely to retain the customer's business. In the case of suspected criminals or terrorists, this technique might be used to predict their future actions, such as phone calls or travel. Of greatest potential value, predictive analytics could be used to provide "Indications and Warning" of terrorist attack or other critical threats.

Visualization: Though not always required, visualization tools help human beings grasp complex relationships by displaying relationships in multi-dimensional forms. "Connecting the dots" is usually not a linear process. Visualization tools produce charts, graphs and interactive maps that indicate the relationship of data points, including how they are connected geographically or over time. They may allow users to "fly" though masses of data to grasp underlying concepts.

Human Analysis: The final stage of analysis depends on the capabilities of human analysts. A skilled analyst can detect subtle trends or relationships far beyond the capabilities of modern technology to uncover in a practical manner. The federal government is undertaking a major effort to increase the size and capabilities of the analyst corps at agencies from the FBI to the CIA. The work of analysts is supported by technology that allows them to collaborate with other experts. In addition, technology can be used to improve human performance by identifying individual analytical styles and adapting the presentation of data to best support the analyst's style. It can also detect shortcomings or biases in the analyst's processing of the data.

In many cases, analysts, working through a structured review process, complete their analysis by issuing alerts or reports that must be shared and evaluated in a systematic manner.

Decision-Action: Informatics technologies continue to offer support to the process during the decision or action stage. Expert systems, decision support technologies, simulation/modeling, and/or adaptive learning technologies may help leaders and operators improve the quality of their decisions and the execution of their actions.

Information Sharing: The lack of information sharing prior to 9/11, continued stove piping among federal agencies, and stubborn challenges in providing useful intelligence to local law enforcement officials and private critical infrastructure owners are driving renewed emphasis on information access. Under the emerging paradigm, information is shared not just at the end of the ISI process, but at all stages from the first collection. Government agencies are moving from "the need to know" to "information sharing" and even beyond, to "information access." Information sharing systems distribute information as widely and quickly as possible while still safeguarding sensitive data. Numerous private sector companies provide software that optimizes information sharing

Solution Providers

Public Company Profiles

The ISI Index of public companies is comprised of: Acxiom, Applied Signal, ChoicePoint, Cogent, Essex, NICE Systems, SPSS, SYS Technology and Verint Systems. Together they represent the key technology solutions and customer base of the ISI market.

Acxiom: provides database, analytic, risk management and consumer information services.
http://www.acxiom.com/

Applied Signal Technologies: designs and manufactures advanced signal collection and processing equipment.
http://www.appsig.com/

ChoicePoint: offers "decision-making information" based on its analytical tools and vast databases of consumer information.
http://www.choicepoint.com/

Cogent: a leader in Automated Fingerprint Identification Systems, or AFIS, that can capture fingerprints electronically and compare them to millions of records in seconds, providing real-time identification.
http://www.cogentsystems.com/

Essex Corporation: serves U.S. government intelligence and defense agencies with optical signal processing, informatics, communications and other complex solutions.
http://www.essexcorp.com/

NICE Systems: provides commercial and government clients with advanced solutions and consulting services that generate insight from multimedia interactions, from call center interactions to wiretapped conversations.
http://www.nice.com/

SPSS: specializes in predictive analytics technology, data mining and statistical tools.
http://www.spss.com/

SYS Technologies: real-time information technology, data visualization, decision support, wireless communications and other systems for the Department of Defense, DHS, and corporations.
http://www.systechnologies.com/

Verint Systems: is a leader in analytic software for video surveillance and wiretapping. Its software can analyze unstructured data such as voice, video, fax, email, and Internet information.
http://www.verint.com/

Private Company Providers*

Many innovative companies are bringing emerging ISI technologies to the market. As customers seek "plug and play" solutions, and major contractors continue their movement into IT services, superior private companies will be poised for success. This is especially true for those that also serve the business intelligence and bio-informatics convergent markets. The following are some private companies we have encountered in our research that offer interesting technologies and/or growth potential:

21st Century Systems: decision support tools for defense and other customers; on Inc. 500 list of fastest-growing private companies.
http://www.21csi.com

Attensity: extraction engines pull entities and facts from intelligence documents; received In-Q-Tel funding.
http://www.attensity.com

Autonomy: public company trading on LSE; included in our list to reflect this month's purchase of In-Q-Tel-backed Verity.
http://www.autonomy.com

AXS Technologies: middleware that extracts super computer-like performance from commodity computers used to view digital imagery (enabling technology; CIC member company).
http://www.axstech.com

Basis Technology: multi-language entity extraction; has national security business.
http://www.basistech.com

BBN Technologies: various informatics solutions; some based on DARPA research.
http://www.bbn.com

Bridgeborn: Advanced Visualization Solutions (AVS) allow users to view and interact with large amounts of complex data through intuitive, 3D visualizations; counts DHS, NASA, DOD and large corporations as users. (CIC member company).
http://www.bridgeborn.com

Cernium: intelligent video surveillance; just raised $7.5 million D Round.
http://www.cernium.com/index.asp

Content Analyst: text analytics tools; CEO is former senior DHS official; SAIC provided technology and holds minority stake.
http://www.contentanalyst.com

Convera: knowledge discovery platform; significant government customer base.
http://www.convera.com

Corpora Software: "automatic sentiment analysis," among other solutions.
http://www.corporasoftware.com

Data Mining International: analytical tools used to detect money laundering and other crimes.
http://www.datamininginternational.com

Endeca: guided navigation and search; received In-Q-Tel funding.
http://endeca.com/

Engenium: conceptual search tools used by numerous government agencies and contractors.
http://www.engenium.com

Equbits: predictive analysis tools for drug discovery and other applications. http://www.equbits.com

Exegy: high speed data mining software for commercial and government clients. www.exegy.com

Fair Isaac: risk management and fraud analytics for industry and government.
http://www.fairisaac.com

FMS Advanced Systems Group: 2D and 3D network link chart visualizations; on Inc. 500 list of fastest-growing private companies).
http://fmsasg.com

Harbinger Technologies Group: proven technology to match Arabic and other non-English language names and terms on terrorist watch lists and in databases; system also provides genealogical links and other data mining. (CIC member company).
http://www.harbingertechnologiesgroup.com

Holocom Networks: complete end-to-end "PDS" hardware solution designed to safeguard cables carrying classified information; company experiencing explosive demand as information sharing requirements drive installation of classified networks around the world (enabling technology; CIC member company).
http://www.holocomnetworks.com/

Infoglide: technology finds patterns, exact matches, similarities and relationships using current data; selected as Texas Deloitte "Fast 50" high-growth company.
http://www.infoglide.com

Intelligent Software Solutions: analysis and situation awareness software; on Inc. 500 list of fastest-growing private companies.
http://www.issinc.com

Intelliseek: open source information discovery; received In-Q-Tel investment; on 2004 Inc. 500 list of fastest-growing private companies.
http://www.intelliseek.com/

Intellisophic: software to identify subject area taxonomies; government applications.
http://www.intellisophic.com

Inxight Software: integrated solution for text understanding, search, entity extraction, event and relationship extraction; recently won $1.7 million contract with U.S. Defense Intelligence Agency (DIA).
http://www.inxight.com

iXmatch: data clustering finds non-obvious occurrences for output to visualization tool; research supported by Department of Defense; includes health science and commercial customers.
http://www.ixmatch.com

McDonald Bradley: recently won $8.15 million contract from Defense Intelligence Agency for ISI; acquired Infodata in August.
http://www.mcdonaldbradley.com

MetaCarta: geographic intelligence solutions; DHS is customer; recently announced $10 million C Round.
http://www.metacarta.com

Nexidia: audio mining and speech analytics; received Paladin investment.
http://www.nexidia.com/

NovoDynamics: foreign language text mining and other applications; received In-Q-Tel investment.
http://www.novodynamics.com

Object Video: leading intelligent video surveillance company.
http://www.objectvideo.com/

piXlogic: visual search engine; received In-Q-tel investment.
http://www.pixlogic.com/

Realinterface: expert systems that allow first responders to identify WMD and collect and disseminate information, including reports on emerging health threats; "dual benefit" of technology enables separate product that dramatically increases efficiency of clinical trial recruitment (CIC member company).
http://www.realinterface.com

RiverGlass: software supports intelligence fusion and other functions; used by Illinois State Police.
http://www.riverglassinc.com

SAS: an industry standard bearer for business intelligence, data and text mining, and statistics.
http://www.sas.com/

Secure Cognition: software uses thermodynamic principles to collect, analyze and visualize vast data sets, including IT network traffic; system designed at NSA (CIC member company).
http://www.securecognition.com

Secured Processing: EAL4 validated pc/laptop solution for multi-domain security and multi-domain access system for legacy databases (enabling technology; CIC member company).
http://www.securedprocessing.com/

Semagix: anti-money laundering and other analytics tools.
http://www.semagix.com

Vidient: security surveillance software; recently announced $12 million B Round.

Visiphor: law enforcement information sharing and automated book software.
http://www.visiphor.com

Visual Analytics: pattern discovery for homeland security, intelligence and law enforcement.
http://www.visualanalytics.com

Visual Purple: highly immersive, decision-based simulation and training tools for U.S. security organizations (enabling technology).
http://www.visualpurple.com/

Vistascape: advanced security surveillance; received funding from Paladin.
http://www.vistascape.com/

*This list focuses on technology providers and does not include: pure integrators; ISI-related human capital companies (such as CIC member CINTT, which provides general and ISI technology training and education for intelligence analysts); providers of specialized ISI analysts, such as SpecTal; or small public companies such as Insightful, which recently announced a sale to the DIA.

Market Constraints

Despite its significant potential, the ISI market faces potential constraints and poses challenges to companies that would serve it.

Privacy, civil liberties and public policy concerns: The most important limitation to this market comes not from budget or technology limits, but from public fears that ISI technologies will be misused. This can be called the "Big Brother" factor.

Modern American society has a growing interest in privacy and control of personal information and many Americans distrust the ability of government agencies and corporations to protect civil liberties and safeguard personal data. Such concerns disrupted ISI projects such as the Total Information Awareness (TIA) and Computer-Assisted Passenger Prescreening System (CAPPS-II) programs. There is also substantial debate about the integration of privately owned databases into government ISI projects, as well as the use of private contractors and data owners to perform ISI services. Finally, publicized security failures have demonstrated that personal information, including that held by private contractors involved with government ISI projects, is vulnerable.

There are potential solutions to these challenges. Improved security can better protect critical data. Government agencies can develop strict authorization standards for access to information and implement auditing logs and other measures to ensure compliance. "Anonymization technologies" allow data to be mined without revealing the identity of specific individuals until final, authorized stages of the process; this protects the privacy of "innocent" individuals whose data is searched. A recent government report found agencies are making progress in addressing these issues, but that substantial work remains to be completed. Such concerns are common and carry considerable force among segments of the American public and their political representatives.

Other potential constraints include the potential slowing of federal spending; fragmentation of the market among federal agencies and contractors; the often onerous procurement process and bureaucracy involved in serving government clients and the competitive advantage enjoyed by incumbents; strict security requirements in certain ISI projects, which increase operating expense and require the recruitment of scarce "cleared" personnel; and the need to comply with government technology security standards mandated for certain software. However, some of these constraints, such as security and government contracting considerations, will provide successful companies with strong competitive insulation, especially from foreign companies which may be excluded from large segments of the ISI market.

M&A and Funding Activities

"Chasing the Money" is a key story line in the security market, as public and private firms compete for an increasing amount of federal and commercial spending on security products and services. This trend has been accelerated by the desire of major government contractors to increase their IT contracts, which are seen as less susceptible to future budget cuts than large weapons programs.

The stock market for these companies has responded – the CEUT Global Security Index of 190 public security companies has risen over 250% since 9/11, vs. low double-digit or single-digit returns for the Dow Jones, S&P and NASDAQ indices. These returns have naturally attracted private equity investors – The Carlyle Group, Giuliani Partners/Bear Stearns, and others have raised multi-hundred million dollar funds targeted for investment in security companies. In-Q-Tel, in effect the CIA's VC arm, has focused much of its investment dollars on ISI companies. The Paladin Capital Group, whose leadership includes a former NSA director, controls a $235 million homeland security fund.

The M&A market in the security vertical has been just as active, with the number of deals increasing in both 2005 and 2004. Defense companies, systems integrators, diversified industrial companies and others continue to chase the growth in the security industry and the premium multiples awarded in the public marketplace. The market for ISI-related firms has been red hot, as they offer industry penetration and the attractive margins of a software model. By our estimates, about $2 billion has been spent during the last 18 months to acquire these types of businesses. Some examples:

11/4/2005: Autonomy purchasing Verity for approximately $500 million

> Verity provides business search and process management to major companies and has moved into homeland security intelligence sharing.

9/19/05: Compudyne buys Xanalys Corporation (terms not disclosed)

> Xanalys offered investigative management and analysis solutions to security and commercial organizations.

8/26/05: McDonald Bradley acquires Infodata Systems for $7 million

> Infodata provided data fusion and content management to the intelligence community and other customers.

7/14/2005: Verisign buys iDefense for $40 million

> iDefense provided intelligence regarding network-based security threats and vulnerabilities.

6/1/2005: ManTech acquires Gray Hawk Systems for $100 million

Gray Hawk provided information services, counter-intelligence mission support and services to intelligence and homeland security organizations.

5/12/05: SAIC purchases Object Sciences Corporation (OSC) (terms not disclosed)

OSC supported government agencies with intelligence and reconnaissance information processing and analysis.

4/11/2005: NICE buys Dictaphone's Communications Recording Division for $38.5 million

Dictaphone provided recording systems for 9-1-1 centers and other mission-critical operations.

4/1/2005: General Dynamics acquires MAYA Viz (terms not disclosed)

MAYA Viz provided situational awareness and collaboration tools for military customers.

3/1/2005 Essex acquires Windermere for $64.9 million

Windermere provided a range of information solutions to the intelligence community.

2/18/2005: Lockheed Martin purchases the SYTEX Group for $462 million

SYTEX provided information technology solutions and technical support services to the U.S. Department of Defense and other federal agencies.

12/22/2004: ChoicePoint acquires i2 for $100 million

i2 is a global provider of visual investigative and link analysis software for intelligence, law enforcement, military and large commercial applications.

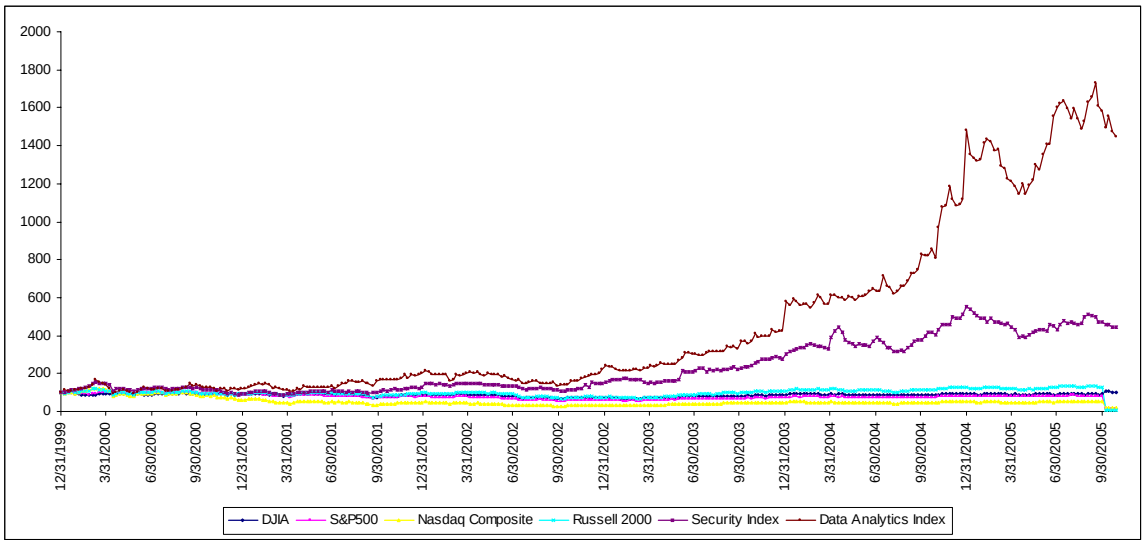
9/1/2004: Lexis-Nexis buys Seisent for $775 million

Seisint provided information products that allow business, financial services, legal and government customers to quickly and easily extract valuable knowledge from a vast array of data.

Stock Performance of ISI Companies

As discussed earlier, public security stocks have significantly outperformed the overall market since 9/11. For this white paper, we created the CEUT ISI Index, comprised of the nine leading public companies profiled earlier. The relative performance of these companies - Acxiom, Applied Signal, ChoicePoint, Cogent, Essex, NICE Systems, SSPS, SYS Technology and Verint Systems – is demonstrated below.

ISI Index Compared to 4 Major Indices and CEUT Global Security Index



Source: FirstCall, and C.E. Unterberg, Towbin data.

	2003	2004	2005 YTD[1]
DJIA	25.3%	3.2%	(3.2%)
NASDAQ Composite	50.0%	8.6%	(2.5%)
S&P 500	26.4%	9.0%	(0.4%)
Russell 2000	47.3%	18.3%	(0.85%)
CEUT Security Index	55.7%	43.6%	(8.1%)
ISI Index	90.3%	53.5%	10.8%

As can be seen from the data, the ISI index vastly outperformed the overall security index and the other four traditional stock indices, returning 90% in 2003 and 54% in 2004, and was the only index to show a positive return so far in 2005. A combination of business growth, product need and industry consolidation have driven these returns and should support further gains over the next several years.

Conclusion

Informatics technologies already surround every American. From validating credit card transactions to enhancing customer service, analytical software has increasingly become embedded in modern life. Traditional BI vendors implemented many of these systems. But the challenges legacy BI technologies face in coping with the tidal wave of unstructured data, along with the unique characteristics of the ISI market, are creating major growth opportunities for new vendors.

These opportunities, along with the strong underpinnings of the ISI market, provide the foundation for strong and sustained growth. This growth offers not only the promise of excellent financial returns, but also the prospect of building companies and technologies that can help protect our nation.

Key Acronyms/Glossary

AFIS	Automated Fingerprint Identification Systems
AI	Artificial Intelligence
Algorithm	Mathematical set of instructions, or "recipe," used to analyze data
BI	Business Intelligence
BPM	Business Performance Management
CRM	Customer Relationship Management
CS	Computer Science
DM	Data Mining
DNI	Director of National Intelligence
DSS	Decision Support System
ECM	Enterprise Content Management
ERP	Enterprise Resource Panning
GWOT	Global War On Terrorism
HCI	Human Computer Interaction
HLS	Homeland Security
IC	Intelligence Community
KDD	Knowledge Discovery in Databases
KDT	Knowledge Discovery in Text
NLP	Natural Language Processing
NSA	National Security Agency
OLAP	Online Analytical Processing
RDF	Resource Description Framework
SCM	Supply Chain Management
UDM	Unstructured Data Mining
3Vs	Volume, Velocity, Variety
WMD	Weapons of Mass Destruction
XBRL	Extensible Business Reporting Language
XML	Extensible Markup Language

About the Authors

Scott Greiper is a Principal at C.E. Unterberg, Towbin. He most recently served as CEUT's Senior Analyst covering the homeland security, anti-terrorism and crime prevention sectors. He has researched companies in digital video surveillance, access control, biometrics, anti-counterfeiting, home security and secure communications. Prior to joining Unterberg, Mr. Greiper was Director of Technology Research at Crystal Research Associates, an independent research firm. He began his career at Drexel Burnham before moving on to become a Senior Technology Analyst at S.G. Warburg. Mr. Greiper attended the Executive MBA program at Columbia University and holds a BA in Economics from the University of Chicago.

With more than 70 years of history, C.E. Unterberg, Towbin supplies capital and financial advice to growth companies in the technology, life sciences and global security sectors. CEUT services and operations include public offerings, mergers and acquisitions, private placements, research, asset management and private client work. Principal offices are in New York, San Francisco, Menlo Park, Herzlia (Israel) and Hong Kong. www.ceut.com

Mark Sauter is Chief Operating Officer and Senior Analyst at the Chesapeake Innovation Center (CIC), America's first business accelerator for national and homeland security high technology. Mr. Sauter has served as a senior executive at several venture capital-backed companies. He is co-author of the leading McGraw-Hill college textbook, "Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism." He graduated from Harvard University, magna cum laude, and the Columbia Graduate School of Journalism. Mr. Sauter served as an Army officer in infantry and Special Forces units.

America's first business accelerator for the homeland and national security sectors, the CIC harnesses the power of entrepreneurship to enhance our nation's technological edge. A public-private partnership initiated by the Anne Arundel Economic Development Corporation, the CIC is a driving component of Maryland's emerging "Informatics Corridor." CIC partners include Northrop Grumman, ARINC, Next Century Corp., Innerwall and the National Security Agency. Among the Center's sponsors are C.E. Unterberg, Towbin; DLA Piper Rudnick Gray Cary US LLP; RSM McGladrey; M&T Bank; Kelly FedSecure; and Whiteford Taylor and Preston. The Center's 19 resident member companies offer a range of security and informatics technologies and services. The CIC also offers the *TechBridge*[sm] program, which creates a bridge between major users of security technology and small companies at the forefront of innovation. www.cic-tech.org

Acknowledgements: The authors would like to thank the research team at CEUT; the CIC's Roger London, Director of Technology Scouting, Dana Liedholm, Director of Marketing, and Chad Burns, intern; and Dr. Tomas Brenner for their assistance on this project.