



Intelligence Quarterly

Journal of Advanced Analytics

Q4
11

The battleground for the future	3
Public security perspective	5
Modernizing the military supply chain	8
Fighting cyberwars with cyber-analytics	11
Building a better, more effective fusion center	14
Rising to the challenge of London 2012	18
The role of social media in the battle for public security	21
How to use open data to create safer, more secure societies	24
Combatting organized crime and terrorism one bullet at a time	27
Northwest Federal Credit Union fights financial crime with analytics	30
Four ways to address cyberconflict – and how analytics can help	32

Editorial Director

Mikael Hagstrom

mikael.hagstrom@sas.com

Editor-in-Chief

Alison Bolen

alison.bolen@sas.com

Managing Editor

Anne-Lindsay Beall

anne-lindsay.beall@sas.com

Copy Editors

Amy Dyson

Chris Hoerter

Trey Whittenton

Editorial Contributors

Barry Gay

Mark Gibson

Lindsay Beth Gunter

Bryan Harris

Jason Healey

Mark Kagan

Charles Leadbetter

Ian Manocha

Lindsay Marshall

Marcie Montague

Ann Morgan

Joanne Taylor

Catherine Traugot

John Quinn

Art Direction

Brian Lloyd

Photography

John Fernez

Steve Muir

Intelligence Quarterly is published quarterly by SAS Institute Inc. Copyright © 2011 SAS Institute Inc., Cary, NC, USA. All rights reserved. Limited copies may be made for internal staff use only. Credit must be given to the publisher. Otherwise, no part of this publication may be reproduced without prior written permission of the publisher.

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies.

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions delivered within an integrated framework, SAS helps customers at more than 50,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW.®





ANALYTICS

Defend against cyberattacks.

SAS® Analytics can predict and prevent sophisticated cyberattacks, including hard-to-detect “low and slow” attacks, by aggregating and analyzing massive amounts of data. Decide with confidence.



sas.com/cybersecurity
for a free white paper


THE POWER TO KNOW.®

The battleground for the future

by Mikael Hagstrom, Executive Vice President, SAS

A number of intelligence officials – many of whom I have had the privilege to meet as a board member of the Atlantic Council – have raised concerns about the West’s growing vulnerability to cyberwarfare threats and malicious computer activity. In February Leon Panetta, then head of the CIA, testified before the US House Permanent Select Committee on Intelligence that “the potential for the next Pearl Harbor could very well be a cyberattack... If you have a cyberattack that brings down our financial system, brings down our government systems, you could paralyze this country.”

During a hearing with the US Senate Committee on Armed Services in June, Panetta further stated that “the next Pearl Harbor we confront could well be a cyberattack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems.”

The message is clear: Cyberwarfare is no empty threat. Consider the new US Cyber Command, which was created in 2010 to protect the country’s

military networks and is expected to spend \$10.5 billion annually on information security. If you add to that the speed at which cybercriminals are moving, you can only conclude that our new world of hyperconnectivity and free-flowing information is also a vulnerable one.

Likewise in the recent book *McMafia*, author Misha Glenny dissects the prevalence of organized crime, which he claims accounts for 15 to 20 percent of world gross domestic product. Globalization has unfortunately been accompanied by a dramatic increase in organized and transnational crime that affects us all.

As a leading provider of systems spanning public and enterprise fraud, anti-money laundering and real-time transactions, I’ve seen countless statistics that estimate the total effects of crime, like the 2009 study by security firm McAfee that shows costs of cybercrime to be \$1 trillion each year and estimates that the typical organization loses five percent of its annual revenue to fraud. In response, I’ve seen many

organizations that are making attempts to overcome vulnerabilities and thwart potential attacks.

Fact is that most corporate and government organizations primitively erect a “Berlin Wall” to combat cyberwarfare – in some cases combined with rule-based systems – and simply hope they will not be a target. But building a wall and creating rules will not safeguard organizations in today’s world of open, hyperconnected data. Instead, with planned data sharing and analysis, organizations can gain not only the desired protection from criminal activity but also reap great benefits for citizens, consumers and businesses alike – something that is illustrated throughout this issue of *Intelligence Quarterly*.

Many businesses, ministries and agencies are looking to use new methods that enable them to monitor and adapt the strength of their defense in real time through the use of analytics, such as self-learning neural networks or social network analysis.

For example, on Page 27 you’ll learn how members of the European Union are sharing data to understand criminal networks across country boundaries in a project called Odyssey. The prototype platform in place today will eventually become a full-blown system that pulls data from law enforcement agencies in the EU to combat both terrorism and organized crime.

In another example of cross-agency cooperation, many local, state and federal government teams are joining together to share data for crime prevention through the fusion center concept. On Page 14, Joanne Taylor, Director of Public Security for SAS, explores six lessons learned from successful fusion centers and why using the right technology is a critical step in maximizing their impact.

Data sharing and data analysis will also be important to ensure safety and security at the 2012 Olympic Games in London. See Page 18 to learn how data can play a role in preventing or disrupting various facets of organized crime both before and during the event.

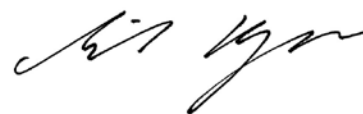
History has proven the public security threat to be real. Take, for instance:

- Russia’s alleged three-week cyber-attack on Estonia that virtually shut down various government, media and banking websites in 2007.
- The Pentagon’s disclosure that in 2008, malicious code on a flash drive from a foreign spy agency spread undetected on classified and unclassified US military computer networks.
- The extended cyberattacks, dubbed Operation Aurora, that originated in China and whose targets included Google and at least 20 other major companies in late 2009. It is believed that the attacks were an attempt to gain information on Chinese human rights activists.
- The Israeli foreign intelligence agency’s successful cyberattack on Iran’s nuclear program using a highly sophisticated computer virus called Stuxnet in 2010.
- China Telecom’s alleged hijacking and rerouting of 15 percent of the world’s Internet traffic through

Chinese servers for about 18 minutes in 2010. This disruption affected US government websites, including the Senate, NASA and the Department of Commerce, as well as major international corporations like Microsoft and IBM.

Cybercrime, cyberwars and cybersecurity are now at the forefront. As Shumeet Baluja comments in a preface to *The Silicon Jungle*, “It is important to remind ourselves that the technology, policies and sheer enormity of the amount of personal detail amassed about all of us is new. ...All of us... are, quite literally, in uncharted territory.”

It is for this and the reasons outlined above that SAS recently made a substantial investment in its Public Security Business Unit. **Locking yourself behind a firewall is not the answer.** To be better prepared, you need to closely monitor the activities going on around you, constantly sweep the growing volumes of structured and unstructured data, and then pool that data rather than keep it locked up. To instantly understand and respond to everything from combinations of extreme events to “low and slow” attacks, you need systems that can adapt and respond in real time. And for that, you need analytics. **Q**




As head of an expanding global team of more than 4,000 professionals in over 50 countries, Mikael Hagstrom is passionate about providing a culture where innovation can flourish, resulting in market leadership for the organization and its customers. He leads SAS’ Europe, Middle East, Africa and Asia Pacific regions, which account for 54 percent of SAS’ 2010 revenue, or \$1.3 billion.

Public security perspective

Helping to solve real issues that touch every aspect of public life

by Mark Gibson, Sales and Marketing Director, EMEA Public Security Business Unit

Everyone involved in public safety is acutely aware that budgets are reduced. But while budgets fall, governments expect agencies to find new ways to protect frontline services. Austerity measures, as seen by the recent student protests in the UK, could act as a catalyst to public unrest. So just as budgets are squeezed, the demands on security forces are increasing. The phrase “doing more for less” could have been coined for public safety, and I’m aware from discussions with customers that it can appear a daunting task.

But now the good news: My experience with police teams shows that effectively using operational data can have a dramatic impact both in generating operational efficiencies and enhancing performance.

Data analytics: Doing more with less

When we start discussions with customers, we often find that many police forces are working with numerous data systems. These “information silos” prevent data from being cross-referenced and take a good deal of time in maintenance. This point was recently highlighted by

Simon Kinsey, Business Intelligence Manager for the South Wales Police. The force used SAS® as its data management tool when migrating from multiple legacy systems to a single database. He said, “Before (the deployment of SAS), staff had the word ‘analyst’ in their title, but actually spent most of their time gathering and processing data, rather than analyzing and reporting.”

The migration project was able to move relevant, clean data over to the new database and move the rest of the legacy data to a searchable archive. This approach had the dual benefit of enabling the retirement of the legacy systems (at considerable cost savings) while retaining access to the historical data through the SAS reporting infrastructure – providing what Kinsey describes as a “wealth of criminal and policing intelligence.”

SAS continues to be used by the force for performance reporting across multiple systems.

“We want to empower people in their divisions, reducing dependency on



spreadsheets, avoiding duplicated effort and removing inefficiencies. Previously, analysts could spend days preparing data. Using SAS means they have far more time for analysis,” Kinsey continued.

Helping to ensure the highest quality of data is a benefit SAS brings to a number of forces, including South Wales, Gloucester and the Metropolitan Police. A high-quality data source has obvious value to a police force by driving efficiency, removing ambiguity and reducing errors. But it also enables the next generation of policing tools - powerful modeling techniques that identify behaviors, patterns, trends and links.

**Predict to prevent:
Building public confidence**

Although statistics reveal that crime levels have generally fallen over the last decade, fear of crime – driven by recent social unrest and concerns about terrorism and cybercrime – remains high. In response to this, we see citizens becoming more open to data being shared across agencies and government departments if doing so helps support crime fighting. Also, despite budget cuts, the public expects the police to have the very best crime-detection systems available to them.

Providing your teams with access to high-quality data systems and analytics satisfies this demand. Patterns that indicate where and when problems might occur in the future can be identified to help tackle the issues that affect every area of people’s lives, including:

- Predicting incidents of car crime.
- Profiling the “career path” for young criminals.
- Understanding triggers for domestic violence.
- Identifying commonalities associated with antisocial behavior and gang crime.
- Identifying links and series, to predict when and where terrorists might strike.

Used in tandem with modeling capabilities, you also can run scenarios such as how changes to policing strategies could reduce the crimes. This proactive approach improves your teams’ ability to make informed decisions about how to optimize resources. The data can be applied to understand what training your officers are likely to need, based on their deployment areas. And it can help you work with communities on crime reduction initiatives and understand the difference that campaigns have on offenses. Such community liaison

My experience with police teams shows that effectively using operational data can have a dramatic impact both in generating operational efficiencies and enhancing performance.

The power of timely and accurate data for the Metropolitan Police

The Metropolitan Police Service that serves London is one of a number of UK police forces using SAS technology. It has implemented a data quality project that helps police officers improve the quality of data entry, flag exceptions, and identify and encourage best practices.

When the project commenced, just one borough was rated as having “excellent data quality” – a figure that rose to 18 boroughs in just eight months. In addition, the number of incidents of “poor data quality” fell from 18 boroughs to zero over the same time frame.

Time efficiencies have also been realized, as less time is needed to re-enter data and field error rates are down to zero in many cases. According to Nick Crouch, head of Met’s Directorate of Information, “We are providing operational staff with practical tools for them to use to improve quality. The direct outcome here is that real operational data is corrected and made fit for purpose.”

The results? Here’s just one story: A prolific offender was arrested for a daytime burglary in the weeks before Christmas. A routine check on the Stops database revealed that this offender had been stopped at 3 a.m. the previous morning, shortly after a woman had been mugged in the area. In a lineup after the arrest, the woman identified her mugger as the offender. The accurate and timely Stops data entry allowed the connection to be made. It also allowed the woman to identify the mugger while his face was fresh in her mind.

makes a big difference in tackling fear of crime, and improves perceptions of police performance.

But perhaps the most important benefit is that quality data analysis demonstrably reduces crime.

Predictive analytics

Another benefit involves looking at serious crime and applying modeling techniques to high-volume crime. Automatic Number Plate Recognition (ANPR) data is used to identify vehicles involved in serious crimes; the same techniques could be applied to burglary, assault, antisocial behavior and a wide range of other crimes. Forces use analytical tools to look for possible links and series in crimes across their region, but the complexity and time needed to perform these tasks limits its use to specific crime types and cases. SAS reduces the completion time and complexity of these tasks, which can then be applied to all offenses and used to target prolific offenders.

High-volume crimes have the greatest impact on people’s perception and fear of crime. Tackling such crimes requires a new approach in light of present-day budget cuts.

Analytics technology is a powerful ally in the drive to improve services for the public while operating with reduced budgets and resources. Data quality and analytics can free the intelligence held in your information and give you

the insight to know when crimes might occur. Armed with this foresight, you can predict and prevent crime, define training needs and create initiatives in partnership with your local communities that greatly improve the quality of life for citizens. You can also use data analytics to model how changes to policing or resources will affect crime levels. As you work to reduce the crime issues that touch every aspect of people’s lives, data analytics offer powerful knowledge about crime in your area and improve responses accordingly. **Q**



ONLINE

More from Mark Gibson on battling organized crime: www.memex.com/resources/articles/information-sharing-and-organised-crime



Mark Gibson is responsible for SAS Public Security sales and marketing efforts across the entire SAS Public Security Group including the UK, Americas and the group’s international business. Mark joined the group’s management team in 2005. He has 20 years diverse vertical sector industry experience with a number of global technology companies including Seagate Software and Doubleclick.

Modernizing the military supply chain

Lockheed Martin and the US Marine Corps join forces to keep combat supply lines open using a powerful weapon — business analytics

Amid the physically grueling and hostile terrain of southeastern Afghanistan, an exhausted platoon of US Marines begins its 10-mile march back to a small outpost camp following a routine patrol. During a bridge crossing, with about half of the unit safely across, the structure explodes under a barrage of mortar and small arms fire raining down from the mountains above. With the platoon split in two, both sides take up their positions and engage the enemy insurgents in fierce combat. As the battle rages, ammunition, water and medical supplies begin to dwindle. Without a resupply of these basic necessities soon, the platoon will record significant casualties before the day is through.

Faced with this outcome, the platoon commander asks for a situation report on efforts to reinforce his unit with the supplies it will need to overcome the enemy forces who are relentlessly slinging fire down from the surrounding mountains.

While fictitious, this scenario is just one of many combat situations US military personnel are trained to face while deployed in an active combat

zone. Thanks to 24/7 cable news reports, delivered to living rooms around the world, the perils of modern day warfare – be they deadly snipers' bullets fired from afar or buried improvised explosive devices awaiting the footfall of battle-weary soldiers or a convoy of fuel tankers – are well documented. But what if soldiers were suddenly left without supplies to accomplish their mission?

Logistics is a crucial aspect of military operations that often goes unnoticed. Without an informed and efficient logistics strategy in place, the lives of combat troops would hang in the balance every day. In the world of military leaders, maintaining supply lines – while disrupting the enemy's – is one of the most critical success factors in mounting and winning wars. After all, what good is a military force without food, water, fuel and ammunition?

War games prove the power of analytics

As one of the most complex and technologically equipped armed forces in the world, the US military takes supply logistics very seriously. As part of the USMC's pre-deployment training



exercises, they contracted with global systems integrator Lockheed Martin to demonstrate how the power of leading-edge technologies can deliver better real-time information to military command centers and the field, to ensure the right supplies are delivered by the most effective means, to the right place, when they are needed – no matter what the situation.

Lockheed Martin partnered with SAS to support their business analytics requirements for a proof-of-concept project to modernize battlefield logistics capabilities for the USMC. Mission goals were to integrate disparate sources of mission-critical data, and develop an information dashboard and reporting system that would provide leaders with critical logistics information in real time.

“SAS played a key role in the Expeditionary Logistics War Game, which resulted in several significant achievements for data analytics and dashboard development to help mili-

tary commanders with their decision making,” says Thad Beckert, Logistics War Game Lead, Lockheed Martin Global Training and Logistics.

“Starting with raw military logistics data and rudimentary dashboard design concepts, the SAS team rapidly built dynamic, self-updating dashboards that mirrored the detailed information commanders typically receive in a static format. Critical information could be easily accessed and immediately actioned through the dashboard interface. In short, the dashboard proved it was possible to deliver a continuous stream of actionable, quality information necessary to accelerate military decision making.”

Life and death decisions in an ever-changing environment

For the exercise, SAS technical specialists were embedded in a command post with military leaders and logistics specialists to simulate the disruption of supply lines in a mock Afghanistan combat zone. From an

impressive control center, equipped with cutting-edge technology and massive floor-to-ceiling screens, the simulated exercise observed how military personnel react and improvise when the line of supply is impeded during combat situations, and how decisions are formulated on the fly to ensure that the front-line supply chain is continuously sustained.

During the exercise, every detail mimicked a real-life scenario to recreate the kind of pressure the military is under to make the right decisions when lives are at stake. The SAS specialists worked in real time, integrating crucial data feeds to generate analysis and reports under tight deadlines, and were even challenged by the limited technical infrastructure and bandwidth one might expect when communicating with remote combat outposts, forcing the SAS team to calculate what type of information and how much could be sent at any given time.

“The combat environment is always changing, but the chain of supplies can never stop,” says Lt. Col. Terry Hagan of the Marine Corps. “As soon as you stop providing supplies, the military stops – people’s lives are at risk. We’re combining logistics data with operational and intelligence data to deliver real-time information that is consumable by the different levels of military personnel, who have to make fast, accurate and confident decisions to ensure the continuous supply of things like ammunition and water during critical situations.”

Real-time information, critical insight

With an array of legacy systems that collect supply information, such as consumption rates and transportation

“The combat environment is always changing, but the chain of supplies can never stop. As soon as you stop providing supplies, the military stops – people’s lives are at risk.”

Lt. Col. Terry Hagan, United States Marine Corps

tracking, the military has no shortage of data to inform its supply chain decisions. What was lacking, explains Hagan, was an efficient and accurate method of combining and sharing data, as well as a flexible tool to perform complex analyses and generate meaningful reports on the fly, instead of waiting hours for reports and presentation slides to be generated for briefings.

“I was impressed that SAS was able to replicate our existing process and automate the delivery of data and information into a real-time dashboard,” says Hagan. “Not only did we get the statistics and performance measures that are important to us in real time, but we also received the ability to perform trending analysis, which we couldn’t easily do before. By compiling data from all of our critical data systems, we’re able to derive additional insights into what is actually happening on the battlefield.”

According to Hagan, efficiency and productivity are crucial benefits that can be derived from applying business analytics to support real-time decisions, at the most critical moments of war.

“Commanders weren’t aware of how much time and effort it took to pull information together, from all the disparate systems to provide reports and analysis,” Hagan explains.

“When I was in Iraq, I worked with a corporal who got up at 3 a.m. to manually compile 30 spreadsheets of data every day to have them ready by 7:30

a.m. – and that’s just one example. The power of business analytics is its ability to bring data sources together and combine tables easily, and then serve it up all in one dashboard – it’s very flexible and customizable. When a general looks at information on a chart, we want to be able to assure him that the data is accurate and current to make the most informed and confident decisions.

“We’ve always completed our missions, but the amount of labor it took to produce the same level of insight before was significantly reduced using SAS,” he continues. “With better productivity and efficiency, we can better support our soldiers in the field. With business analytics, we know exactly what the pulse is automatically, all the time. And that’s the way it should be. We’ve proved that our concept of automating information delivery is valid – I think this is the first time ever in the military that we have been able to do this from a logistics and operational perspective.”

As for the future, Hagan says the proof-of-concept project performed by Lockheed Martin and supported by SAS will support the military’s aim to have inventory, consumption and transportation of supplies monitored using real-time sensors, which will transmit data back to the supply chain system to support ongoing decision making.

“Waging and winning wars is heavily reliant on the bravery and skill of the soldiers that fight for freedom.

And success with as few casualties as possible is our goal,” concludes Hagan. “With intelligent people and systems supporting our troops on the front lines, we have a better opportunity to achieve that goal.” **Q**



ONLINE

Analytics and defense logistics webcast:
www.sas.com/sascom-defense

Keys to modernizing logistics:
www.sas.com/sascom-logistics

Fighting cyberwars with cyber-analytics

Mitigate security risks proactively and strategically

by Mark Kagan, consultant and analyst on defense and foreign affairs, security, and intelligence

If the United States were at cyberwar, it would lose. That's what Mike McConnell, former US Director of National Intelligence, told the US Senate in February.

Many government officials would probably assert that the US is already engaged in cyberwar, although it has not reached the point where attackers are taking down critical infrastructure (85 percent of which is privately owned), disrupting communications, or shutting down agencies. Many government officials from other countries might also say that their countries are engaged in cyberwars, though perhaps on a smaller scale – perhaps.

The trend is clear. For example, the number of incidents reported by US federal government agencies to the United States Computer Emergency Readiness Team (US-CERT) soared from 5,503 in 2006 to 16,843 in 2008 – a 206 percent increase. The number of incidents was almost surely understated because the report covered only detected incidents. In the always-on, always-connected world today, a

new computer, if unprotected, can be scanned within seconds and infected with malware within minutes.

An army of millions

The types of threats and attacks are many and growing in volume, sophistication and agility. They come from foreign nations, criminal groups, hackers, hacktivists, disgruntled insiders and terrorists. The most serious, sophisticated and persistent attacks come from foreign governments and organized crime groups – sometimes working in tandem – that directly or indirectly employ hundreds of thousands of well-trained, highly motivated hackers and engineers.

The United States is by no means alone in bleeding terabytes of sensitive, proprietary, classified information and intellectual property. It just happens to be the biggest target.

The threats and attacks include denial of service, distributed denial of service, exploitation, logic bombs, sniffers, Trojan horses, viruses, worms, spyware, war-dialing, war-driving, spamming, phishing,

spoofing, pharming and botnets – often in various combinations. PandaLabs estimates that 99.6 percent of all email traffic directed to government mailboxes comprises spam or malicious messages – only 0.4 percent is legitimate.

Concern greater than ever

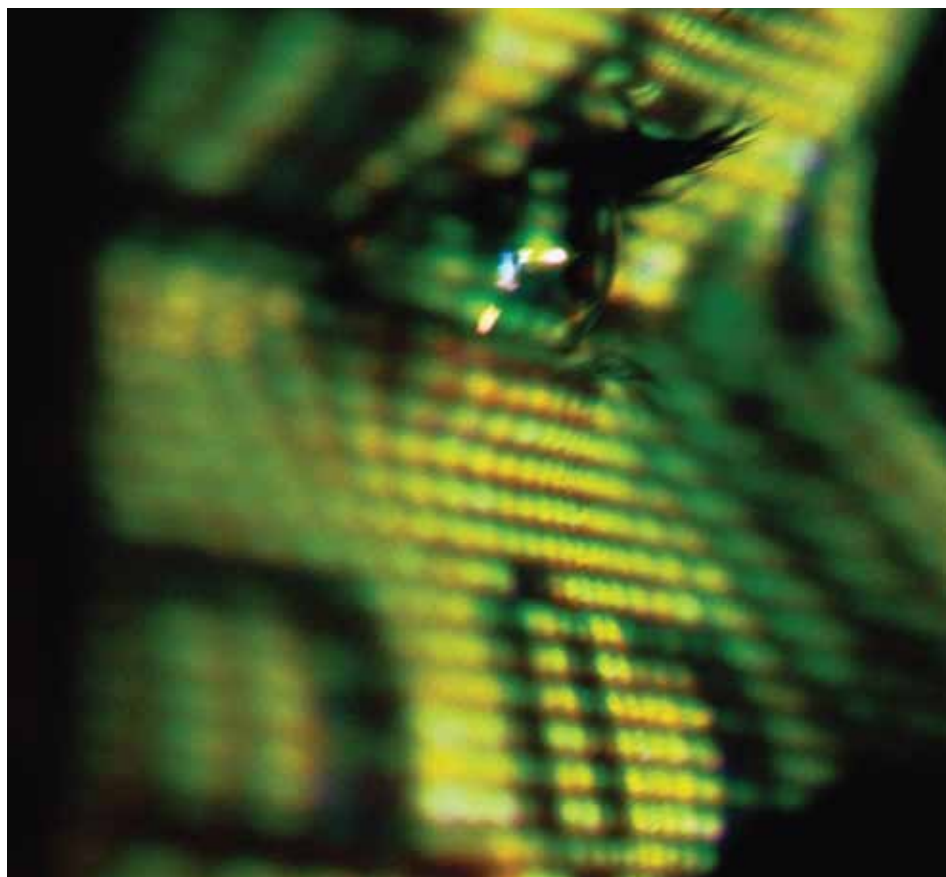
Cyberdefenders are most concerned with attacks, particularly from insiders, aimed at stealing, modifying or destroying data. The relatively recent phenomenon of advanced persistent-threat attacks has raised the level of concern even higher. These attacks penetrate organizations and insert software programs that repeatedly steal or modify data – and typically exist for as long as eight months before being detected.

Government IT managers are losing sleep because the data they must protect is growing by terabytes every month. They are being inundated by masses of disconnected, uncorrelated data from all of their security systems. At the same time, the disparate and diverse systems that typically constitute IT infrastructures make it practically impossible to gain a comprehensive view of cybersituational awareness.

More sophisticated threats

Overworked and overstressed cyberdefenders spend most of their time plugging holes, fighting fires and patching their networks. They operate in perpetual catch-up mode against increasingly sophisticated attackers who rapidly respond to security fixes with newer, more sophisticated threats.

Some government agencies have established cybersecurity operations centers, which are great for network monitoring. But they haven't provided operators and analysts with the tools to understand what drives the attacks, intrusions and



anomalies – what it all means, and what's going on. While dashboards, security information and event management systems are great for reporting what's happening and what happened, they're not much use in detecting and analyzing patterns, predicting future attacks, issuing alerts and warnings, or sketching out what-if scenarios.

According to Zalmi Azmi, the former CIO of the US FBI, in today's cyber environment, all government agencies worldwide must increasingly accept the fact that they are engaged in cyberwarfare. In such an environment, says Azmi, cyberanalysts will need to employ tools and processes that correlate data, improve situational awareness and alleviate shortages of qualified IT security personnel.

Weapon of choice: cyber-analytics

Analytics can provide many of those tools and processes through statistical analysis and modeling – much as analytics can be applied to fraud detection, financial management or human resources.

Cyber-analytics can provide governments with enhanced and complementary capabilities and situational awareness about the security of their systems, networks and enterprises. It does this by analyzing activities; uncovering vulnerabilities, threats and patterns; integrating disparate data to find patterns and trends; and predicting future threats and attacks so agencies can take proactive measures to protect their data and networks.

Cyberwars, by the numbers

206

Percentage increase in detected incidents against US federal agencies (2006-2008)

8

Number of months that malicious software typically runs on government computers without detection

99.6

Percentage of all email hitting government inboxes that is either spam or malicious

0.4

Percentage that is actually legitimate

Cyber-analytics can help government agencies meet two of their biggest challenges: coordinating cybersecurity efforts and producing practical metrics to quantify the effectiveness of those security efforts.

Cyber-analytics can also:

- Provide near-real-time analysis that automatically generates attack alerts while simultaneously dramatically reducing the number of false positives.
- Aggregate, correlate and merge data from all relevant network devices and other sources to provide enhanced network domain and situational awareness.
- Detect and score the severity of possible attacks before they happen to support prevention and timely interventions.
- Provide early recognition of anomalies in network traffic and uncover otherwise hidden relationships and behavior patterns that might indicate low and slow attacks.

Analytics contribute to a holistic view of the entire chessboard – where the pieces are located, both white and black. This holistic view helps government organizations significantly improve the coordination of their cybersecurity efforts and produce metrics that provide a more accurate picture of those efforts. Finally, analytics enable governments and corporations to better understand, use and protect their data, regardless of volume, condition, state or location.

Mitigating security risks

Government cyberdefenders can no longer follow the outdated paradigm of protecting the perimeter and patching, plugging and putting out fires. They can no longer view cyberspace tactically and react to threats and attacks, instead of taking a strategic view and being proactive. The threats and attacks are growing too fast and sophisticated and the enemies are smart, resourceful and agile. Forget script kiddies and hackers in basements – more often than not, the attackers are foreign governments and/or transnational criminal organizations.

Using analytics for cybersecurity enables government agencies to think and act strategically, be proactive in mitigating security risks, and defend their data and IT infrastructure. With analytics, IT security managers can become strategists who always look three or four moves ahead and play offense as well as defense. In other words, they can stop playing checkers and start playing chess. **Q**



Download the white paper:
Cyber-Analytics for Network Situational Awareness
www.sas.com/reg/wp/corp/16942

Mark Kagan is a Washington, DC-based consultant and writer and long-time analyst on defense and foreign affairs, security and intelligence. He began his professional career as a defense intelligence analyst.

Lessons learned

Building a better, more effective fusion center

By Joanne Taylor, Director of Public Security, SAS

Fusion centers began in the US as a grassroots effort by several forward-thinking state and local police organizations that were reluctant to sit back and wait for another intelligence failure like the one leading up to the events of Sept. 11. This “hometown” initiative was quickly embraced by the federal government, especially the US Department of Homeland Security (DHS) and the US Department of Justice, whose missions include enabling the unfettered sharing of information and intelligence to help protect the homeland across all levels of law enforcement.

The basic principles of fusion centers are sound: collect information from all available sources, including federal, state, regional, local and tribal agencies; vet the information; analyze it in order to identify trends, patterns and threats that may indicate planned or ongoing criminal activity or terrorism; and most importantly, share the information among all concerned parties.

Since 2004, the 72 DHS-recognized fusion centers have received \$426 million in federal funding for this purpose. However, fusion centers have largely been left on their own to determine how best to accomplish their mission.

In some ways it makes sense. Individual fusion centers do not focus on the same goals or serve the same purpose. Some cover larger areas and concerns, while others are narrower in their purview. Yet there are commonalities in the way they need to operate – enough that they don’t have to go it completely alone when determining the most efficient and effective way to operate.

Although originating in the US, the concept of the fusion center has long since expanded beyond those shores. Many countries are now embracing the concept and deploying their own versions. In the developed world, the fundamental challenges of multiple intelligence agencies not sharing data has led to numerous intelligence “failures” driving the need to introduce the fusion concept. In the developing world, the opportunity exists to not make the mistakes of the West, which often started out with disparate systems that led to intelligence breakdowns. Instead, countries such as India and South Africa are embracing the use of an integrated, countrywide view of their intelligence data.

Most fusion center wins do not make the nightly news. So it is important to be able to show the value a fusion center is bringing to the state, region and even the nation in the prevention of terrorism, as well as the reduction of organized crime and gangs.



But whether a US state fusion center, a countrywide fusion concept or any variation between, all fusion centers are underpinned by successfully gathering, managing and exploiting their intelligence data. Therefore, a solid technology platform must be used.

Using technology that helps make sense of disparate pieces of information is one of the most important steps a fusion center can take to ensure it is operating at maximum efficiency and performance levels. As more and more states and countries adopt the fusion center concept, it's useful to hear lessons from early adopters. Here, we share six lessons learned from successful fusion center initiatives.

Six lessons from successful fusion centers

1. Start by installing a technology platform rather than a collection of disparate products. One of the keys to peak performance is having a good workflow – making sure every single step of the process is identified, that the software being used incorporates all those steps, and that there is an ability to audit activities to ensure proper procedures are being followed. Accomplishing all of this is easier if there is a single platform, which allows you to monitor the entire workflow. It also

simplifies the technical requirements because there are no compatibility issues when moving the data from one phase to another. Finally, it establishes a flexible foundation on which you can build as new needs arise.

2. Make sure you have the ability to manage and supervise the work.

In a typical fusion center, intelligence is received from multiple sources and multiple agencies supply personnel. Problems can arise when those personnel are accustomed to following different procedures.

The ideal platform provides oversight as to what is taking place among the analysts and the rest of the workforce. This oversight helps ensure that all policies and procedures are being followed and approvals are met and tracked. This is an area where individual applications often fall short and serious issues arise, particularly regarding privacy. A good, single-source platform has these capabilities built into the workflow.

3. Train, train, then train again. The technology is only as good as the people using it, and they are only as good as the training they have received. Analysts and fusion center leadership particularly require it, so they understand the capabilities of the technology and can take full advantage of them. There are

In the developing world, the opportunity exists to not make the mistakes of the West, which often started out with disparate systems that led to intelligence breakdowns. Instead, countries such as India and South Africa are embracing the use of an integrated, countrywide view of their intelligence data.

a plethora of training options, so it's important to determine which courses are the best for training a good intelligence analyst.

Skills required by analysts can be identified based on whether they are performing tactical, strategic or statistical analysis. Many skills cross over all three of these areas, but each is unique and requires different skill sets to be successful. Identifying the responsibilities of each analyst and then training for that specific purpose will result in a well-balanced staff that is able to meet the demands placed on today's modern fusion center. The most difficult function for law enforcement is the transition from tactical to strategic analysis, which requires the ability to view disparate pieces of information and recognize trends within them. It's a different mindset for many in law enforcement, but critical to adopt if the fusion center is to be successful. It is also helpful to know the software platform intimately via training. For example, some analysts may be unaware of advanced search capabilities in a particular platform, such as link charts, nested and proximity searches - which can dramatically speed up analysis and help connect the dots.

4. Place high priority on protecting privacy/civil liberties. The protection of privacy and civil liberties is a strong point of contention among groups opposed to fusion centers. Another point

of contention is information sharing among law enforcement and intelligence agencies. Ensuring privacy is a challenge due to ambiguity in national and federal rules, and privacy law variations between countries and states. Differences in the missions of individual fusion centers exacerbate the problem. These factors underscore the need for each fusion center to establish an inviolate set of policies, procedures, rules and regulations that fall in line with national and state laws. Each center must also ensure close supervision of the work being performed on a daily basis, and have an audit trail that documents adherence to established policies and procedures.

5. Keep tight controls on who can see what data. Having multilevel security protocols within the technology answers two significant concerns.

The first is leaving control of data in the hands of the data owner. When agencies are reluctant to participate actively in a fusion center, the reason is usually a concern over who can access their data, particularly confidential sources. Technology that establishes roles and privileges on multiple levels - while leaving data security under the control of the original contributor - goes a long way toward assuaging those concerns.

The second is the ability to use lower-level staff for data entry, thus relieving analysts of a necessary but time-consuming chore. Other staff can be

The many roles of the fusion center

One of the basic tenets of the fusion center approach is the role the centers play in enabling information sharing among multiple agencies working to deter terrorist acts, but that is just one of a broad range of different roles most centers have to play. Others include:

- Intelligence management, covering the entire intelligence life cycle – including information collection, review, evaluation and analysis. In this area, information sharing is key. In particular, systems have to ensure that the right information gets to the right person at the right time.
- Threat assessment reporting, so that leaders and law enforcement resources can be focused on high-priority threats. Again, information sharing plays a key role in making sure that executives at the center are notified in a timely manner to be able to make informed decisions.

To achieve these objectives, agencies and centers urgently require systems that present their analyst teams with the relevant information all in one place. This is where the public security business unit of SAS can help provide intelligence management and analytics, allowing investigators to analyze the data more effectively and to forecast and predict likely future patterns of behavior.

given access to enter data, yet be restricted from accessing the data once it is in the system. Using this method ensures privacy policies are being upheld while freeing analysts to focus on the mission – spotting trends and threats – rather than performing repetitive and mundane data entry tasks.

6. **Have a performance matrix to measure success.** In order to continue to obtain funding and expand the mission, fusion centers must be able to demonstrate success. Much of what is done is done quietly, out of the public eye. Most fusion center wins do not make the nightly news. So it is important to be able to show the value a fusion center is bringing to the state, region and even the nation in the prevention of terrorism, as well as the reduction of organized crime and gangs. A well-designed performance matrix, with metrics tracked through the technology, can help fusion center leaders make that case.

Technology supports national security

Fusion centers are still in the early stages of their development, and they continue to grow and adapt to changes in their homeland security mission. As such, many continue to feel their

way along, trying to determine the operational standards that will help them prevent and disrupt criminal activity – including terrorism.

The right technology platform can help shortcut that process by providing strategic, tactical and investigative insight while still allowing the flexibility to adjust for varying missions, state requirements and other factors. It is one of the keys to the success of the fusion center concept in the future – and our national security. **Q**



ONLINE

More about fusion centers:
www.memex.com/industry/fusion-center



Joanne Taylor is the Director of Public Security for SAS Europe, Middle East, Africa and Asia Pacific. With a background in technology for law enforcement and national security, forensic psychology and business analytics, Joanne joined SAS in 2004. Joanne has responsibility for the applications of SAS technology to the public security market and intelligence solutions.

Rising to the challenge

Why intelligence-led policing is key to tackling threats to London 2012

By Mark Gibson, Public Security Marketing Manager, SAS

The London 2012 Olympic Games are likely to be one of the largest events ever staged in the UK. There are 205 nations expected to take part in a total of 300 events. According to Lloyds TSB, the Olympics will generate £10 billion in revenues for the UK economy as a whole, while the London Council's 2012 team claims that "revenue from tourists attracted by the 2012 Olympic and Paralympic Games are forecast to add up to an additional £2.1 billion."

The games are likely to see a massive influx of visitors into the UK. Lord Coe, chairman of the London Organizing Committee, has spoken of 1 million extra people coming to the country for the Games. The huge influx of visitors will inevitably result in an upsurge in all sorts of opportunistic offending, from pickpocketing to fraud and cybercrime.

Many of these crimes may not be directly linked to the Games itself, but will instead be a feature of the wider

"Olympic economy" – innocent tourists conned into parting with their money for non-existent tickets to the theatre or major London tourist attractions.

For UK police, these are just a few of the many issues they will need to address in the days leading up to the Games. Organized crimes - such as immigration, intellectual property, e-crime and money laundering - are all likely to be serious concerns in addition to the ever-present threat of terrorist activity that's both homegrown and international.

According to the Serious Organised Crime Agency (SOCA), "fraudulent activity currently linked to the London 2012 Olympic Games includes the use of the 'London 2012' name appearing in mass-marketing frauds, including fake websites and email scams, offering employment, tickets, and lotteries and prize draws which purport to raise funds for the Games."

The truth is that solving the criminal threat presented by the Olympics will require a more strategic approach. There will indeed be a greater need for integration and cooperation across different police forces, but this should not just extend to numbers on the ground but also to sharing information and intelligence.

Resourcing issues

As the police look to tackle these multifaceted threats in advance of the Games, the issue of resourcing will inevitably be a major issue, with police in London drawing manpower from a wide array of provincial forces. If required, they may even consider bringing in extra officers from back-office functions into front-line policing.

On face value, this would appear to make perfect sense. There will be many who point at how effective the surge in police numbers proved in combating the recent London riots.

However, in light of the planned cuts to police numbers, this kind of surge is likely to prove much more difficult to achieve by summer 2012. It is worth noting that policing the Olympics is a completely different challenge that involves a far wider range of potential threats than the recent social unrest. Few of the threats that surround the Olympics are likely to be solved by the simple step of putting more “bobbies on the beat.” After all, the reality is that most of these extra officers will be employed in crowd control.

Shared information

The truth is that solving the criminal threat presented by the Olympics will require a more strategic approach. There will indeed be a greater need for integration and cooperation across different police forces, but this should not just extend to numbers on the ground but also to sharing information and intelligence.

The key is in identifying and dealing with increased risks before and during the Games. The ability to pool intelligence - not just about antisocial behavior but also about organized crime and terrorism - will be key as the Games approach.

In combating the potential threats, information sharing is increasingly a priority. In dealing with these, the Metropolitan Police will need access to more than just its own data. If data about potential threats is not effectively shared, then intelligence will likely have key data points missing.

Even when relevant data is available, it will be of little benefit unless it is utilized effectively. Disparate data sources must be brought together so that it makes sense to all operatives; otherwise, investigations will be delayed and decision making is likely to be slow and inaccurate. It will be difficult for forces to effectively predict and prevent crime.

It is not just about sharing and consolidating the information effectively, however. To overcome these challenges, agencies need to exploit data using analytic techniques that reveal patterns, anomalies, key variables and relationships in the data.

Taking action

Of course, even when information has been pinpointed and analyzed, it will be of little use unless positive action is taken to deter and prevent crimes. As an example, Operation Podium, the Met’s dedicated response to serious and organized crime affecting the economy of the London Olympic and Paralympic Games in 2012, has already swung into action.

Podium’s proactive prevention team is hard at work preventing crime from happening and disrupting crime that is already taking place. This is achieved through a number of routes: specialist industry forums – taking in payment service providers; the hotel and hospitality industries; major events ticket suppliers; and vetting industries. Through these forums, police are partnering with industry specialists to



share intelligence, identify risks and trends, and build preventative measures into their business-as-usual practices.

In addition, Podium's proactive investigation teams are making it difficult for those organized criminal networks operating now to avoid detection before the Games begin. They achieve this by taking action against those networks involved in organized ticket crime now - whether it's website abuse, failing to provide tickets, selling fake tickets or touting - by seizing and restraining the assets of criminal networks and partnering with other key organizations to close down criminal networks.

Intelligence is the key

Regardless of what type of activity Podium is involved in, all of its work is led by solid intelligence data. The most powerful tool that the police can use in the battle against crime before and at the Olympics is the ability to convert data into intelligence that's available to those who need it - without compromising its security. If that is accomplished, then Podium is well on its way to ensuring that the London 2012 Games are safe and secure for all involved. Q



Visit Podium online:
www.podium.ac.uk/

Podium's proactive prevention team is hard at work preventing crime from happening and disrupting crime that is already taking place.



Mark Gibson is responsible for SAS Public Security sales and marketing efforts across the entire SAS Public Security Group including the UK, Americas and the group's international business. Mark joined the group's management team in 2005. He has 20 years, diverse vertical sector industry experience with a number of global technology companies including Seagate Software and Doubleclick.

The role of social media in the battle for public security

by Joanne Taylor, Director of Public Security, SAS

2011 has been witness to a total revolution in the use of social media. It is no longer just reflecting social attitudes but now defining them. Social media sites have evolved from being a form of communication to a social activity in their own right and now into a channel for active group psychology so powerful it can overthrow governments.

In the world of public security this has massive importance. The “Arab spring” witnessed in the first six months of the year proved for the first time that the attitudes expressed through social media are not just the muttering of the young or rantings of the disillusioned, but can stir an entire nation to action. Would the events in Tunisia, Egypt or Bahrain have occurred without the presence of Facebook and Twitter, sites so uncontrollable by governments? If undemocratic governments had in fact realized the power of such sites, they no doubt would have tried to control them, as we see in China.

During the recent riots in London, social media was used not to incite the violence, but rather to coordinate the rioters’ activities. BlackBerry Messenger

became the rioters’ most useful weapon against the police, allowing them to select a target, move and attack en masse, leaving the police trailing behind for three nights in a row. The response of last resort? BlackBerry offered to completely shut down its Messenger site – at least temporarily.

In the attempt to maintain law and order, is the only answer government control of social media channels? No. Public security professionals need to stop seeing social media as the problem and start tapping into it as part of the solution. In the fight against antisocial criminals, organized crime and terrorists alike, social media can be law enforcement’s most powerful weapon.

Seeing social media as part of the solution

Police and intelligence services across the world have been using the Internet extensively for a while now in the fight against crime and terror. “Open-source intelligence” – the use of publicly available information sources – is fundamental to most agencies’ daily activities and has proved hugely useful in unlocking a

There simply aren't enough resources to focus on all negative conversations – no matter how hateful – or all people known to associate with antisocial groups. But by using predictive analytics, sentiment analysis and advanced risk modeling techniques, those that pose the greatest potential threat can be identified.

multitude of investigations. For social media the focus has mainly been on what is termed the “black Web” – monitoring known sites that criminals use to communicate and educate one another, sites used to propagate hate and feed propaganda, or chat rooms used by predators to target the young and naïve.

In extreme cases, law enforcement can use the Web to track a person's activity, social network use and movements. As we learned after the terrible events of the July massacre in Norway, Anders Behring Breivik was an avid social media user. He used the Web to propagate his abhorrent beliefs and gave very clear indications as to his intended actions. Breivik was known to authorities as a potential threat and was active in extremist circles. So why wasn't he being monitored?

The painful truth is that he is only one of thousands, perhaps millions, of individuals across the globe who pose a potential threat to the world's law-abiding citizens. So how are public security professionals expected to monitor them all, deal with the massive volume of open-source social media data, and extract the crucial information that will prevent another tragedy? How do you find the needle in the social media haystack?

The argument public security professionals most often raise is that they simply do not have the resources to

turn the contents of social media communications into useful intelligence. If we are to rely on people as the interpreters of the open source, that is most certainly true. People are not the answer here – technology is.

Three technologies fill the need

Since analyzing public conversations across social media requires text analytics tools, modern public security professionals must understand the technical aspects of text analytics. Unfortunately, the concept of text analytics is often understood as little more than the collation of open-source data, and many companies take advantage of this. They want public security professionals to believe that simply collating data from open sources (including social media) and reporting on it is the answer. But that's just not good enough.

Moving lots of text-based data from the Web into data stores does not in any way exploit its full potential or turn it into useful intelligence. What public security professionals need is a way to interpret text-based data on an industrial scale.

Three advanced analytics technologies that will help with this process are:

Text analytics technologies can now pore over huge amounts of social media information – in all major languages – to uncover patterns and analyze content. Social media analytics can continuously monitor online and social conversa-

tions to identify important topics and content categories, which enables public security professionals to focus on the most important content areas. To meet the crucial challenge of understanding interrelationships and context, text analytics technologies automatically extract “entities” – such as people, places and locations – and build linkages among them.

Social network analysis technologies also can be used as part of this process to understand the human networks behind groups of people, both online and off. Uncovering patterns of relationships and connections between individuals, the technology recognizes how people are connected, the closeness of those connections and the likely ringleaders. This enables public security professionals to identify and focus on key individuals and so utilize resources most effectively.

Sentiment analytics assess and monitor the sentiment of text to flag changing attitudes that may signal a shift from words to action. Allowing the technology to do the monitoring frees resources to intervene when an increased threat is identified.

These types of capabilities filter out the noise within social media and focus on the data that could provide valuable intelligence. There simply aren't enough resources to focus on all negative conversations – no mat-



Banks, insurance companies and governments have been using these technologies for years to decide whether to give you a loan, whether your credit card transaction is fraudulent and whether you are likely to evade taxes. It's time we also trusted it to monitor online activity, identify potential threats and predict potential wrongdoing.

ter how hateful – or all people known to associate with anti-social groups. But by using predictive analytics, sentiment analysis and advanced risk modeling techniques, those that pose the greatest potential threat can be identified. This means valuable human resources can focus on where the greatest threat lies and let the technology monitor the wider community.

Of course, with all three of these technologies, special care should be taken to analyze data in aggregate form, to respect individual privacy rights and to follow the legal framework in your jurisdiction related to the monitoring of online information for law enforcement purposes.

Do we trust technology enough to put our security in its hands?

Hindsight is easy, I know, but it does prove the point. Here is just one example from this year.

Having reviewed the available news feeds from the Middle East from the first few months of this year, text analytics clearly identified the escalating unrest that led to revolution in Tunisia – and the same patterns in content categorization and sentiment analysis could have predicted events in Egypt.

Running text analytics on millions of tweets during the London riots flagged specific locations as targets and groups

as ringleaders in real time, which would have been enough to at least keep up with the rioters, if not get ahead of them.

Fundamentally, this is about interpreting the text and modeling the risk. Banks, insurance companies and governments have been using these technologies for years to decide whether to give you a loan, whether your credit card transaction is fraudulent and whether you are likely to evade taxes. It's time we also trusted it to monitor online activity, identify potential threats and predict potential wrongdoing.

In times of financial austerity, public security agencies cannot just increase their resources to ensure social media is being appropriately monitored for threats. They need to use those resources smarter and free them to act on intelligence – not be bogged down by sifting through data. They need to use technology to extract useful intelligence from mass social media data. **Q**



SAS Social Media Analytics:
www.sas.com/software/customer-intelligence/social-media-analytics

SAS Social Network Analysis:
www.sas.com/solutions/fraud/social-network

SAS Text Analytics:
www.sas.com/text-analytics



Joanne Talyor is the Director of Public Security for SAS Europe, Middle East, Africa and Asia Pacific. With a background in technology for law enforcement and national security, forensic psychology and business analytics, Joanne joined SAS in 2004. Joanne has responsibility for the application of SAS technology to the public security market and intelligence solutions.

How to use open data to create safer, more secure societies

Big data to the wisdom of the crowd

By Charles Leadbeater, Demos associate and author of *We-think*

As more interactions between citizens and government move online, this activity should yield rich new flows of information about citizens' views and preferences. The data trails left by our use of the social Web are creating unfathomably large sets of data that could provide new sources of economic and social innovation, together with new anxieties about privacy and ownership of information.

The increasing volume and detail of information captured by enterprises, the rise of multimedia, social media, the spread of the internet to mobile devices, and the potential embedding of networked sensors in everything from ovens to pacemakers will fuel an exponential growth in data. The emergence of these "big data" sources, drawing on a mass of miniscule transactions, comments and connections, creates a potentially rich mine of information for governments.

At the same time, social media is creating the conditions for the emergence of a "civic long tail" – a mass of loosely connected, small-scale conversations, campaigns and interest groups, which

might occasionally coalesce to create a mass movement. From now on, governments everywhere will have to contend and work with this civic long tail.

The future of government will be shaped by the interaction between these two trends:

1. Big data and the ways that governments can mine and analyze the data on these trends to become more efficient, effective and perhaps, more connected.
2. The civic long tail and the trend toward a more active citizenry.

The hopeful Web

To their credit, political leaders in the developed world have not been slow to spot the potential of social media and the Web to revive political systems, which seem detached and exhausted, and service delivery systems, which seem cumbersome and clumsy.

The US federal government has launched a string of hopeful initiatives, including Data.gov, which opens up government data. The UK government has not been far behind. It has set up

The promise of big data to make government more intelligent will only be realized if government learns how to open up data so citizens, entrepreneurs and campaigners can start using it for themselves.



the Public Data Corporation to make government data public and available in reliable and easy-to-use ways. Likewise, flagship projects such as national crime mapping have been designed to help local communities hold the police to account.

Across the world, others have been plowing similar furrows. In Italy, for example, government is endorsing the open, participative, collaborative potential of the Web to make public services and administrations more effective and accountable.

Far from being threatened by the rise of social media, governments may find that through the masses of data it generates, social media offers a way to understand the shifting sentiments, interests and demands of citizens. If government can analyze and understand these data cleverly and quickly, it should be in a better position to respond to emerging needs and even to forestall them. Government could become more intelligent, use its resources more efficiently, and create personalized services and localized solutions more easily.

Sounds promising. Yet creating that kind of capacity, especially in entrenched and often inward-looking bureaucracies, will be far from easy. It will require new skills, outlooks, ways to commission innovation and relationships with outsiders – private companies, civic Web entrepreneurs – who can bridge the gap between the fleeting world of social media and the bureaucratic world of government.

If government can make good use of the tools and data that the social Web is making available, then it could become more accountable, collaborative, innovative and effective. Just as importantly, communities and citizens should become more capable, adaptive and resilient. Better government and stronger communities could grow together.

Working together with open data

Yet the promise of “big data” – large and growing data sets about what citizens do and want – will only be realized with more open data to allow more people to analyze and find value in it. Left to its own devices, government is unlikely to spot all the potential value in the data available.

Opening it up to others to sift through should engage more eyes and ideas to spot potential value. Open government data are data sets released by government in the public interest, in which all data are anonymous. Citizens have the right to repurpose, reuse and share the data without asking anyone's permission.

The promise of big data to make government more intelligent will only be realized if government learns how to open up data so citizens, entrepreneurs and campaigners can start using it for themselves. Again, big data and the civic long tail need to work together.

The challenge is to find a way to these two very different visions of the civic future: more effective and intelligent public systems, based in part on the analysis of big data combined with more adaptive and capable communities, able to use the data to solve problems they face. How might that be possible?

The key in the long run is that government needs to make stronger, more creative connections with communities of locality and interest to sustain and improve how it does its job.

Government 2.0 is about improving people's relationships with government, either as citizens through the political process, as taxpayers or as service users. Community 2.0 is about enlarging and empowering citizens' relationships within one another. The first is about

delivering better services to people, mainly by solving problems in government supply chains and decision making. The second is about communities looking after themselves more effectively and providing a Web platform for unfolding communitarian creativity.

The social Web seems to offer a way to combine these two stories, perhaps for the first time. Smarter government could be combined with stronger communities: more intelligent, integrated, skilled public services, combined with the long tail of civic activism; systems that scale but are also intelligent enough to attend to the local, the human and the personal. These will be the systems of the future, capable of operating at scale but with a sophistication that allows them to be intimate and adaptable. Q



ONLINE

SAS executive Ian Manocha on open data:
blogs.sas.com/content/sascom/author/ianmanocha/

UK think tank Demos on open data:
www.demos.co.uk/publications/thecivictongtail



Charles Leadbeater is a leading authority on innovation and creativity. He has advised companies, cities and governments around the world on innovation strategy and drew on that experience in writing his latest book *We-think: the power of mass creativity*, which charts the rise of mass, participative approaches to innovation from science and open source software, to computer games and political campaigning.

Combatting organized crime and terrorism one bullet at a time

Pan-European ballistics intelligence platform fights crime with analytics

What if a single gun used in multiple crimes could be tracked throughout Europe? Could that type of information – on a large scale – help reduce murder rates, genocide, honor killings, trafficking in drugs and weapons, smuggling of human beings, and laundering of the proceeds of crime?

A project called Odyssey hopes to make these achievements possible through the use of data sharing technologies and good data management practices. The project is a partnership between many agencies across Europe to help reduce terrorist activities, organized crime and transnational crime.

Cooperation across the European Union is vital to reducing these types of international criminal activities. While there has long been both political and operational commitment to share data and no shortage of ballistics and crime information data, Project Odyssey pro-

vided the technical means to do so. The EU project recently completed its first goal to develop a ballistic crime data sharing system.

The Odyssey platform links crimes and weapons using advanced analytics technology, promoting mutual co-operation and knowledge sharing among police, security and intelligence professionals across Europe. The system makes it easier to identify guns and, potentially, criminals as they move between jurisdictions. By constantly monitoring new data and current items of concern, the system will “red flag” potential matches to alert policing professionals in the relevant EU member states.

Odyssey: the beginning

The Odyssey prototype was developed by a team of experts ranging from police, computer scientists and researchers and uses SAS analytics

software to drive key components of the system. The aim of the project is to analyze and process crime information and ballistics data to help understand criminal networks without country boundaries.

The prototype platform was coordinated by Sheffield Hallam University and was supported by a number of other security agencies including EUROPOL. Once fully implemented, the system will gather data from a very large number of law enforcement agencies in the EU. This would allow the network to record and share a significant amount of information about gun crime in one single secure system, ensuring benefits across Europe.

Anschutz or Beretta?

Ballistics information relating to the types of weapons, bullets and cartridges recovered from crime scenes is critical to the project's success. Projectiles have unique characteristics like size, shape and texture that can be used to differentiate between one weapon and another. This means that the characteristics of a crime scene can be profiled and compared to others that are similar with respect to the nature of the crime, suspects, weapons and other evidence.

Traditionally, finding links between crimes has been an incredibly complex, time consuming and difficult process

that often involved physical transport of evidence and manual searching of data. A lack of standards for data acquisition, match declarations and different input methods between organizations and geographies makes the matching process tricky and often unreliable. Odyssey Project has addressed this issue by bringing information from police, security and intelligence organizations across Europe together into the same system in the same format.

A key feature of the fight against gun crime is to identify large-scale patterns and undertake data mining to identify key issues – for instance, the sudden arrival of new arms or ammunition in crime across Europe. Identifying such patterns can lead to identifying the source of the arms and cutting off the supply through police action, border security action or international political and economic action.

The analysis of the collected ballistic crime data uses a prediction, detection and modeling system from SAS to gain an understanding of criminal networks around Europe. The data is analyzed using algorithms and semantics to understand its meaning by reporting back on patterns. This extracts meaningful data that the team can use to determine the distribution of gun crime. Ballistics data that appears to map to similar incidents is then flagged up instantly to show connections between crimes,

What Is Odyssey?

Partially funded by the 7th European Framework Programme for Research and Technological Development, the Odyssey project uses non-personal ballistics data and crime information. Intelligence will be extracted using semantic knowledge extraction and data mining to facilitate appropriate, fast and responsible decision making and alerts. The work will include the use of cutting-edge science and technological methods and develop new research agendas for future work.

Setting the ballistics standard

Currently, different parts of the European Union have ballistics standards in place, but there are few widely recognized and applied standards in place for the whole of the EU. Such standards could ensure that best practices and approaches are taken – without stifling existing processes or hampering future innovations in the field of ballistics.

What aspects of forensic ballistics could be standardized?

1. Output from ballistics analysis technologies.
2. Forensic processes (such as test firings).
3. Data recorded about a ballistics object.
4. Data recorded about a crime.
5. Security standards for sharing data.
6. Functionality of technology.
7. Compatibility and interoperability of technologies.

The Odyssey Project is acting as a facilitator in the standardization process to harmonize technology, procedures, practice and policy across the European Union – and at the same time encouraging new innovation for the next cycle of development and growth.



allowing agencies to share and cross-reference information based on more accurate evidence. Similarly, agents in other geographies are automatically alerted to matches on gun and bullet signatures so they can build a profile of crime networks that may affect their area.

To the future and beyond

Odyssey Project has just reached the end of its first stage of development. Over this period, the team has worked to come to grips with the data collection problems faced by agencies tracking and managing criminal investigations involving firearms and has used this insight to develop best practices for data collection to ensure smooth coordination across Europe. Using this information, it built a prototype computer architecture to help integrate the variety of systems to ensure that information held is secure, securely exchanged but useable for complex cross-jurisdiction matching. Q



Learn more about the Odyssey program:
odyssey-project.eu/

Northwest Federal Credit Union fights financial crime with analytics

Banks of all sizes can prevent criminal financing using anti-money laundering software

Fraud is a constant concern for the banking industry, and while the issue continues to plague both small and large institutions alike, anti-money laundering software is helping the financial services industry keep pace with the ever-changing and sophisticated fraudulent activity of criminals the world over.

Comparatively smaller than most banking institutions operating in the US today, Northwest Federal Credit Union (NWFCU) – a not-for-profit financial cooperative of 105,000 members, with assets in excess of \$2 billion and five branch offices in northern Virginia and Washington, DC – makes fraud prevention a priority and uses analytical tools to combat financial crime on behalf of its membership.

Pinpointing crime

In the past, NWFCU had to generate a number of transactional reports that contained a large volume of detail each day and then manually comb through each transaction to identify

possible fraudulent activity. Today, life's a whole lot easier for the credit union now that it's using SAS Anti-Money Laundering – part of the SAS Enterprise Financial Crimes Framework for Banking – to pinpoint suspicious activity and stop criminals in their tracks.

“We'd been looking for suspicious, fraud-related activity using manual reports and it was very labor intensive; we were very interested in an alternative to enhance and streamline the process,” says Nancy Huntoon, Security and Fraud Manager and Bank Secrecy Act (BSA) Compliance Officer at NWFCU. “Our internal system did not generate alerts and we had daily, weekly and monthly raw data reports – basically, 50 to 100 pages of transactions to look over. It was very difficult to get through them each day.

“SAS Anti-Money Laundering has definitely been a huge asset for us from a process and efficiency standpoint; it's really made a world of difference. It crunches all the data and readily



Why AML matters

by David Park, VP of Financial Solutions, SAS

Many banks across the globe already have an anti-money laundering (AML) solution in place, but there are very good reasons why we continue to stress the importance of AML and financial fraud in general. One of the most effective means of finding and preventing criminal activities continues to be through the financial system. The fact is: organized crime and acts of terrorism require funding, and thanks to the controls put in place through global legislation, we can detect an incredible number of illegal activities just by watching how the money flows through the financial system.

Even in countries that are known for being supportive of terrorist organizations, the controls originated in other countries can help dry up the funds available to criminals. The various blacklists and sanctions applied to “terrorist-friendly” countries and financial institutions provide real incentive for the legitimate members of the financial community to cease doing business with such entities, thereby cutting off their ability to move money and support terrorist activities. Never have I been so proud to be associated with SAS and our AML solution - named the number one worldwide AML product by the Aite Group in 2011.

Read more about the Aite Group award:
www.sas.com/news/preleases/aite-aml-report.html

provides the fraud and money laundering scenarios and risk factors up front. It’s helped us with our time management by identifying possible fraudulent activity or transactions, which allows us to focus more accurately on suspicious alerts. Now, our BSA Specialist can effectively review the new alerts and move on to monitoring case activities on a daily basis. In the past, it might have taken the specialist more than a day to just work through the large volume of transactional data.”

Removing the guesswork

According to Huntoon, her team monitors a wide variety of fraud scenarios and risk factors – such as large cash withdrawals and deposits, wire transfers, the velocity of debit card activity and money structuring – and says the predefined scenarios and factors in the SAS solution helped the credit union adapt to the new system very quickly.

We didn’t exactly know where to start in analyzing our transactions, so we took the scenarios out of the box to start,” she explains. “We’ve done a few tweaks to a couple of the scenarios, such as changing some dollar amount thresholds or time frames, and now that we are more comfortable with the application we review each scenario every six months just to make sure we’re seeing what we need to review. From the standpoint of pinpointing certain activities, it has enabled us to further define what we actually need to look at, and how to categorize each activity. SAS has made it easier to pinpoint more indicators that we may not have seen before. It takes a lot of the guesswork out of the process and helps us catch things earlier to prevent potential fraud losses.”

Establishing connections

To build upon the credit union’s financial crimes capacity, Huntoon and her team are also building a householding process to analyze the relationships between member accounts, and the money that moves between them, to identify suspicious activity.

“The flexibility of SAS allows you to synthesize your analysis of transactions and prevent potential fraud,” concludes Huntoon. “I like SAS’ customer support structure and their availability. SAS was the best fit overall – from service to install to the actual application. The solution had most of what we needed; if it wasn’t available, it was certainly programmable. There’s a lot of flexibility.”



ONLINE

More about anti-money laundering:
www.sas.com/reg/gen/corp/1591963

Financial crimes prevention conference:
blogs.sas.com/content/sascom/tag/turning-point

Four ways to address cyberconflict – and how analytics can help

Using analytics for critical infrastructure protection, cyberwarfare prevention and more

By Jason Healey, Director of the Cyber Statecraft Initiative, the Atlantic Council of the United States

Cyberspies “have penetrated the US electrical grid and left behind software programs that could be used to disrupt the system” during a future war or to coerce the US.

That is not the beginning of a dystopian cyberpunk novel but news reported by *The Wall Street Journal* (“Electricity Grid in US Penetrated by Spies,” April 8, 2009). And as the Stuxnet worm showed the following year – disrupting Iranian nuclear fuel production – cyberattacks can have real-world national security consequences for any government.

How can analytics help combat cyberconflict? Analytics will be of ever-increasing importance, playing at least four different roles to help prevent or minimize the damage from future cyberconflict: critical infrastructure protection, secure operations, law enforcement and warfare. Each of these approaches to cyberconflict has different customers who require different types of analytics to support different decisions.

Critical infrastructure protection is a catchall term for actions taken to protect or improve the resilience of the basic foundations of modern life, such as the finance, electrical, oil and gas, government services, transportation, water and communications sectors. These sectors are interdependent in deep – but often mysterious – ways.

Because a cyberattack on the electrical system may cascade in an extremely unpredictable manner, analytics is moving front and center to drive decision making in the field of critical infrastructure interdependency modeling tools. These models tend to be extremely data heavy – and there are a great many of them, often competing or overlapping – ensuring analytics plays an important role in determining whether an attack will be trivial or catastrophic, with failures cascading quickly into other sectors.

Secure operations require a different set of analytics tools to handle more



routine, but equally critical, decisions, such as risk management and resource optimization that are fed by the masses of technical data generated by devices, users and attackers.

Important analytics tools here include forecasting to understand demand, operations research for resource management, and visualization to make sense of the complex results. Advanced security heuristics will help identify and defend against a cyberattack on the electrical grid.

Tools used in the past required an understanding of the exact signature of attacks in order to detect them. For example, Stuxnet spread through Iranian systems undetected because it used three “zero-day” attacks completely unknown to the defenders and was therefore undetectable by their older systems.

Newer tools like those from SAS, Bivio or NetWitness are increasingly adept at spotting abnormal behavior that is likely to be an attack. This is incredibly data-heavy work, and the newer tools can inspect traffic as it passes in real time at “line speeds” of 10Gbs or

more (that is, hundreds of times faster than a typical local Wi-Fi network).

For the **law enforcement** approach, analytics must help to predict and stop crime but also identify perpetrators and their conspirators. Many of the same tools used for secure operations, fortunately, are of use here. Crunching through device logs and network traffic can spot patterns of fraud and crime, while analysis of abnormal behavior and modus operandi can uncover networks of wrongdoers. Social network analysis is essential here, but modeling and risk management tend to be less important since law enforcers want to arrest perpetrators and conspirators causing disruption – not, for example, optimize network resources.

On the other hand, text analytics and data mining can be extremely important for law enforcement since data is often less structured than for critical infrastructure or secure operations. When intelligence or law enforcement analysts are investigating cyber tools left behind in the electrical grid, for example, they will need to piece together bits of leads from many sources: technical and intelligence databases, public articles in several

languages, lists of known associates with nicknames, alternate spellings, and links to possible collaborators and government officials. This is extremely difficult for analysts even when there is sufficient time – but can be very easy for an analytics engine trained to spot patterns in messy data.

Finally, because **warfare** is a newer approach in cybersecurity (and one not as data-driven as the others), the use of analytics here is more experimental, yet still important. For example, if Stuxnet was, as some analysts have claimed, created by the United States, it would have to go through similar approval as any other weapon used by Western militaries. Under commitments such as the Geneva and Hague Conventions, weapons must undergo rigorous testing and legal approval to ensure they have the intended effect and only that intended effect, which requires extensive modeling under a wide variety of extremely complex circumstances. Commanders (and their judge advocates general) will reject using a weapon that might cause unintended civilian casualties or not work as intended.

Because a cyberattack on the electrical system may cascade in an extremely unpredictable manner, analytics is moving front and center to drive decision making in the field of critical infrastructure interdependency modeling tools.

Analytics also is likely to help to understand cyberdeterrence, a topic of extremely high interest in the US. During the Cold War, decision modeling and game theory were integral parts of Western nations' planning in their efforts to dissuade the Soviet bloc from attacking. Yet even simple versions, such as the Prisoner Dilemma games or Monte Carlo simulations, are rarely seen in discussions on cyberconflict. These tools could still be extremely helpful. For example, because it is difficult to attribute the source of cyberattacks and because they do not cause casualties, an enemy might be tempted to use an attack against the electrical grid to coerce a government during diplomatic negotiations but before a traditional "kinetic" military fight. Decision modeling and game theory are likely to be very useful to unravel such hidden and otherwise unknowable dynamics of conflict in cyberspace.

What we know

In *The New Know*, Thornton May writes that analytics should focus on what can be known, what should be known, and what actions need to be accordingly taken. In the area of cybersecurity and conflict, analytics is already playing a deep role in the technical approach and is starting to get a grip in the criminal and warfare approaches. However, because these are such new fields,

often the decision makers are unfamiliar with what decisions need to be taken – or are even unaware that there is a decision to make.

Practitioners of analytics (whether in the government sector, or elsewhere) have already helped to stop cyberattacks, arrest those behind them, and foresee the impact of attacks on critical infrastructure. Analytics will continue to be at the center of the defense, driving understanding and decision making for government and business alike. Q



ONLINE

Download the white paper:
Cyber-Analytics for Network Situational Awareness
www.sas.com/reg/wp/corp/16942



Jason Healey is the Director of the Cyber Statecraft Initiative at the Atlantic Council of the United States and was a former intelligence officer who pioneered methods for predictive warning for cyber-incidents. He also served in the White House as a policy director on cybersecurity issues. You can follow his comments on cooperation, conflict and competition in cybersecurity on Twitter, @Jason_Healey.



SAS Institute Inc. World Headquarters +1 919 677 8000

To contact your local SAS office, please visit: **www.sas.com/offices**

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies.
Copyright © 2011, SAS Institute Inc. All rights reserved. S79885.1011

