Intelligence Management & Analysis

Increasing effectiveness and reducing costs for protecting against public safety and national security threats

CLYDE W. FORD, CEO
ENTEGRA ANALYTICS

National security threats have dramatically changed… A modern-day intelligence agency must be equipped with the latest information technology to meet the challenges of today's threat environment.

EXECUTIVE SUMMARY

National security threats have dramatically changed over the past several decades. Where once the threat was a militarily equipped large nation, increasingly the threat is a technologically sophisticated small group. Where once the threat was measured in terms of fire-power, increasingly the threat is measured in terms of cyber-power. And, where once the threat was met with boots on the ground and stares down the barrels of weapons, increasingly the threat is met with bodies in seats and stares at the glass of computer screens. Information technology has dramatically changed the nature of threats and the manner and means of their detection and prevention. A modern-day intelligence agency must be equipped with the latest information technology to meet the challenges of today's threat environment.

Still, even the most sophisticated information technology is no substitute for human decision-making. An intelligence management solution should support human decision-making not attempt to replace it. Intelligence analysts should be trained to identify the most likely outcomes from a range of possible outcomes based on the information available to them, then report their findings. Those with decision-making authority then should be able to draw conclusions from those reports and order appropriate actions based on their conclusions. Information technology, like the intelligence management solution described in this paper, should support this process.

Information alone will not counter a threat like terrorism… However, information transformed into intelligence can be the basis for sound decisions and definitive actions to counter terrorism.

DATA TRANSFORMED INTO ACTIONABLE INTELLIGENCE

Intelligence analysis seeks to provide decision-makers the information required for reasoned decisions and appropriate actions to prevent or to investigate threats to public safety and national security. A classic method of describing this transformation of data into intelligence is known as the "intelligence cycle," shown in figure 1, which proceeds through four phases: intake, analysis, dissemination and archiving.

AIM 20/20, Advanced Intelligence Manager, from Entegra Analytics operates as command and control software that assists data collectors, intelligence analysts, and decision-makers through this intelligence life-cycle.

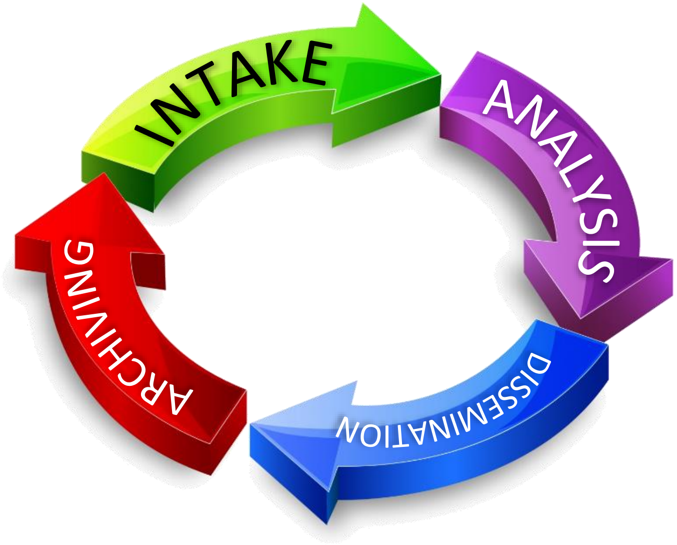


Figure 1. Classic Intelligence Cycle

INTAKE

Figure 2 depicts the intelligence cycle in operation. In the intake phase of this cycle, information about an incident is available from all sources inside and outside an agency. One example of this would be the use of "tip and lead" forms for reporting suspicious activity.

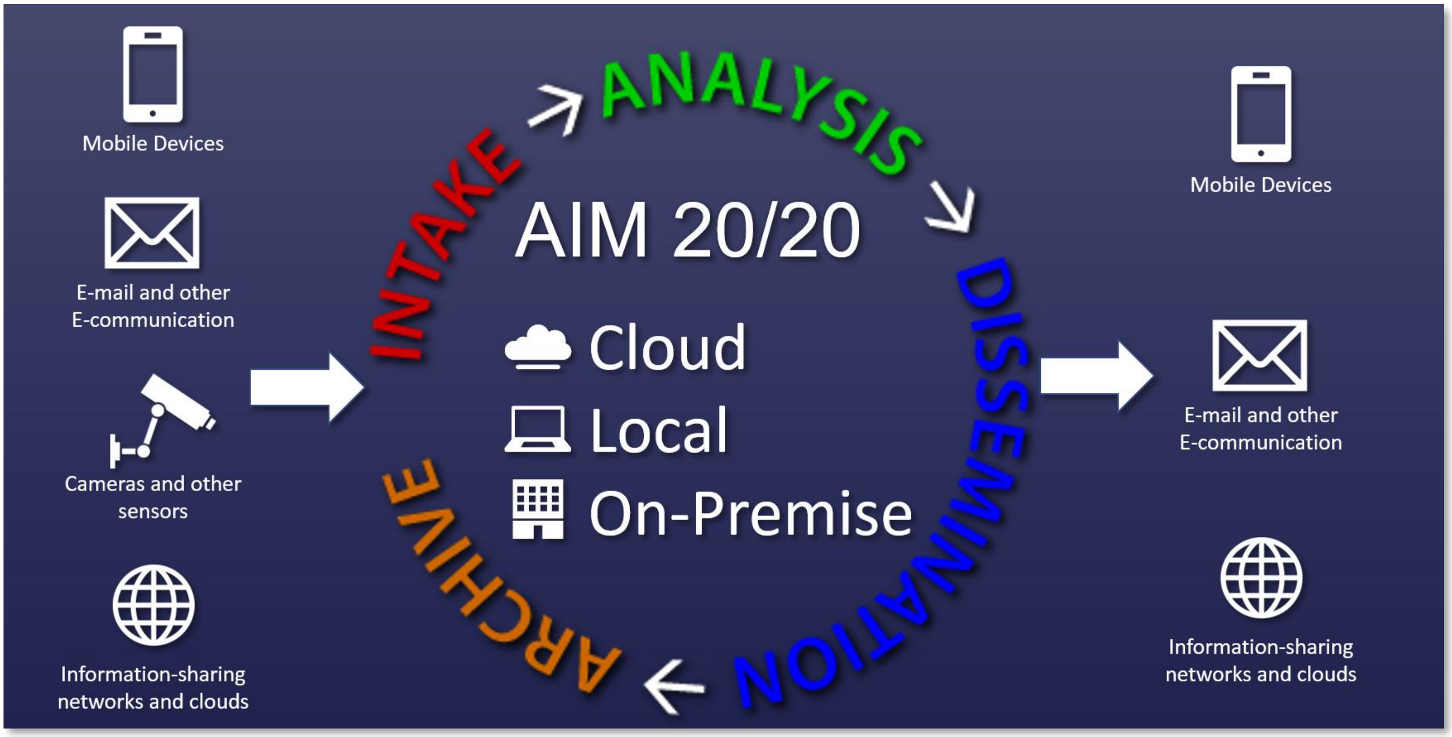

Mobile Devices
E-mail and other E-communication
Cameras and other sensors
Information-sharing networks and clouds
INTAKE
ANALYSIS
DISSEMINATION
ARCHIVE
AIM 20/20
Cloud
Local
On-Premise
Mobile Devices
E-mail and other E-communication
Information-sharing networks and clouds

Figure 2. Intelligence Life-Cycle

Entegra Analytics' AIM 20/20 software offers incident management through the use of "tip and lead" reporting forms. Filled out manually or automatically, these forms become work units that move through each phase of the intelligence life-cycle.

Tip and Lead forms have information about the person or agency reporting the suspicious activity; information about the suspicious activity itself; and supporting information such as attached documents, audio, video, or images.

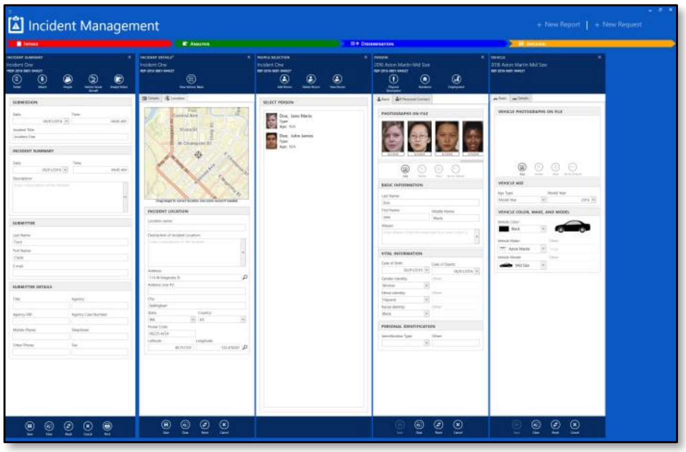


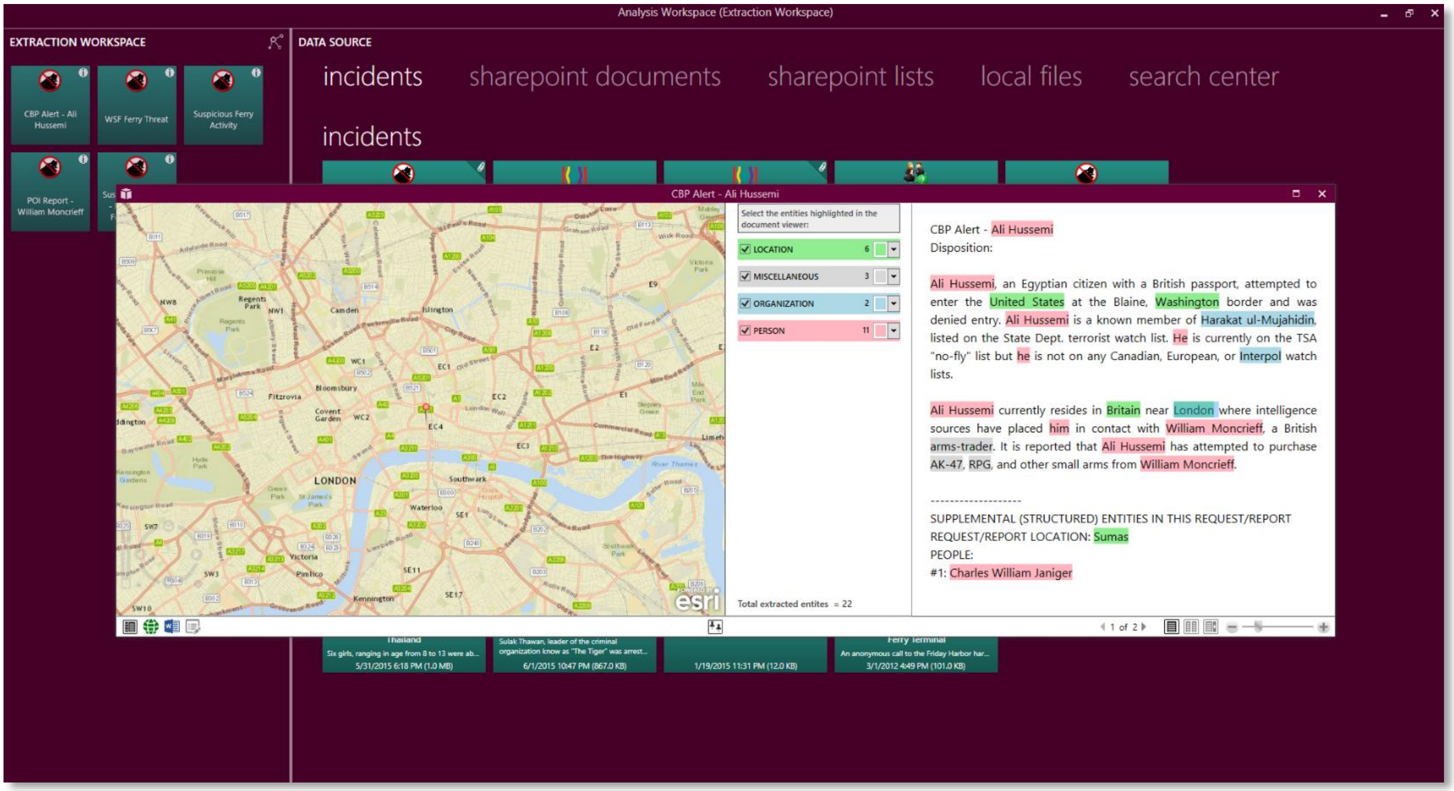
Figure 3. Incident report form from the Entegra Analytics suite.

Figure 3 shows a typical "Tip and Lead" form for reporting suspicious activity from the AIM 20/20 suite. Each panel of the report opens to receive information on a difference aspect of the incident. There's a panel for basic incident information such as a summary of the incident. But there are also panels for the incident location and the people and vehicles involved. Not shown are additional panels for vessels, aircraft, and weapons involved it the incident, as well a panel that allows for the attachment of document, image, audio and video files related to the incident.

ANALYSIS

Open incidents are assigned to intelligence analysts for further investigation and discovery (data management). Analysts can then apply a number of tools to this information (data analysis) and produce a variety of useful views (data visualization).

Intelligence analysis—extracting probable and sometimes multiple hypotheses from available information—is an analyst's task. But the large volume of information an analyst faces frequently requires excessive time spent searching for and sorting through the right information to analyze. Anecdotal reports from within the intelligence community place analysts



Total extracted entites = 22

CBP Alert - Ali Hussemi
Disposition:

Ali Hussemi, an Egyptian citizen with a British passport, attempted to enter the United States at the Blaine, Washington border and was denied entry. Ali Hussemi is a known member of Harakat ul-Mujahidin, listed on the State Dept. terrorist watch list. He is currently on the TSA "no-fly" list but he is not on any Canadian, European, or Interpol watch lists.

Ali Hussemi currently resides in Britain near London where intelligence sources have placed him in contact with William Moncrieff, a British arms-trader. It is reported that Ali Hussemi has attempted to purchase AK-47, RPG, and other small arms from William Moncrieff.

SUPPLEMENTAL (STRUCTURED) ENTITIES IN THIS REQUEST/REPORT
REQUEST/REPORT LOCATION: Sumas
PEOPLE:
#1: Charles William Janiger

Thailand
Six girls, ranging in age from 8 to 13 were ab...
5/31/2015 6:18 PM (1.0 MB)

Sulak Thawan, leader of the criminal organization know as "The Tiger" was arrest...
6/1/2015 10:47 PM (867.0 KB)

1/19/2015 11:31 PM (12.0 KB)

Ferry Terminal
An anonymous call to the Friday Harbor har...
3/1/2012 4:49 PM (101.0 KB)

Figure 4. Entity extraction document reader with attached geospatial viewer.

spending as much as 80% of their time looking for the right information, leaving precious little time to analyze that information. Entegra Analytics' software tools can shift this balance in favor of analysts.

Finding Needles in Haystacks

The volume of information crossing an analyst's computer screen can be daunting and extracting meaningful intelligence from it even more so. One of the first tools Entegra Analytics can place in the hands of intelligence analysts is natural language processing where documents of any kind (text, word processing, spread sheets, images with metadata) are automatically read by software and items of interest (entities) extracted.

Figure 4 shows an incident report after it has been transformed through this entity extraction process into a color-coded document with important items highlighted and an attached geospatial viewer available so locations within the document can be visualized.

A "word frequency cloud" is a logical, and easy data visualization that emerges from entity extraction. Shown in figure 5, a cloud of words (entities) is displayed where the size and intensity of each word varies with its frequency in the underlying document.

Connecting the Dots

More useful even than a word frequency cloud is a link analysis graph, which is both an analytical and visualization tool. Link analysis graphs take multiple entity extracted documents and "link" them together through common entities.

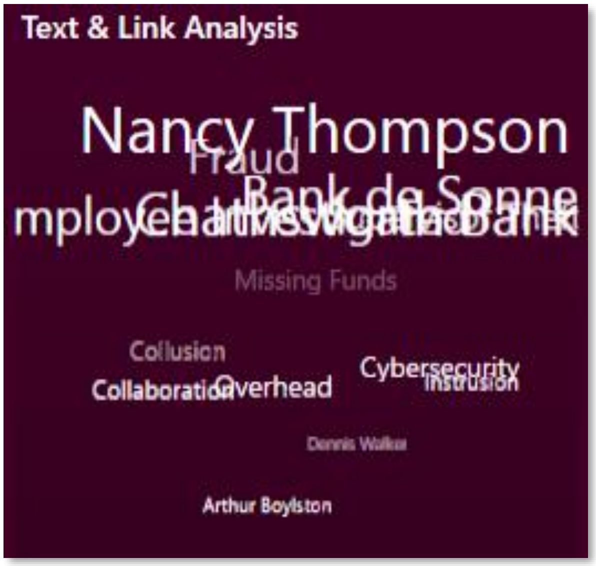


Figure 5. Word frequency cloud.

Before the advent of modern-day, high-speed computers, this time-honored investigative technique was accomplished with index cards and yarn

Link analysis graphs, see figure 6, surface relationships often hidden in disparate documents. They are important tools in aiding intelligence analysts in developing meaningful hypotheses and provide an easily understood way of presenting information to decision-makers.

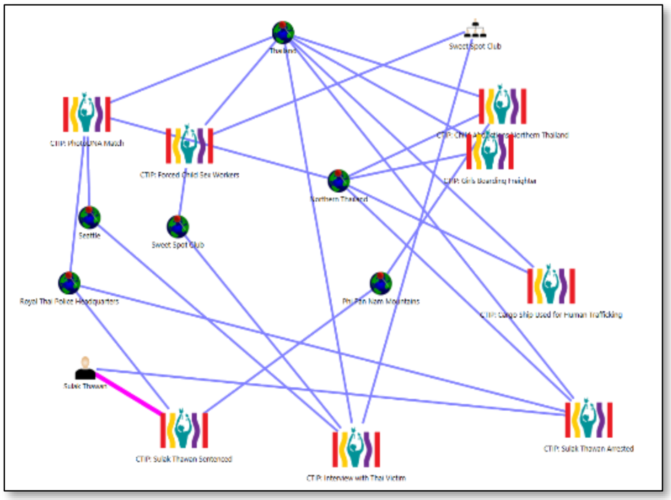

Thailand
Sweet Spot Club
CTIP: Photo/DNA Match
CTIP: Forced Child Sex Workers
CTIP: Child Abductions Northern Thailand
CTIP: Girls Boarding Freighter
Northern Thailand
Seattle
Sweet Spot Club
Royal Thai Police Headquarters
Phi Pan Nam Mountains
CTIP: Cargo ship used for Human Trafficking
Sulak Thawan
CTIP: Sulak Thawan Sentenced
CTIP: Interview with Thai Victim
CTIP: Sulak Thawan Arrested

Figure 6. Link graph helps to discover hidden connections.

A Common Operating Picture

Threats and attacks happens somewhere. Tips may center on a single location but multiple locations are frequently involved. Perpetrators may be located in a given area, or a given country. Location data or geospatial intelligence, often buried in documents or reports, is extremely useful in creating a common operating picture of an agency's attempt to prevent or investigate threats and attacks.

Geospatial intelligence is not simply for data visualization; it is a useful analytical tool as well. A worldwide map can show which areas are connected based on threat reports and assessments, then geographically weighted regression (GWR) analysis then used to estimate risk and predict the likelihood of future threats and attacks emanating in a given area. Tip and Lead reports can identify suspected "hot spots" of suspicious activity when those reports are displayed on a map. And, if the location of potential perpetrators is known, social media can be used to "listen" to real-time Tweets regarding the preparation for and planning of attacks within a given geographical radius.

DISSEMINATION

No matter how accurate, information alone will not prevent or discover threats. However, information transformed into intelligence by tools like those described above, can be the basis for sound decisions and definitive actions to counter threats.

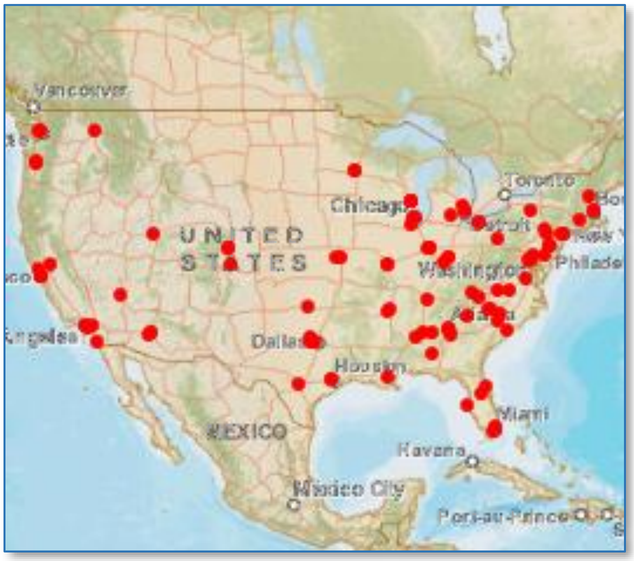


Figure 7. Map of threat reports.

Reports, position papers, briefings—the "work products" of intelligence analysts—should flow directly from the data analysis and visualization tools they use. Using the AIM 20/20 tool suite, for example, color-coded entity extracted documents can be converted into Microsoft Word files and then edited to produce a report. Frequency clouds, link graphs, and maps can be exported as image files and incorporated into briefings, reports or presentations. This process of proceeding from analysis to work products for dissemination can even be automated depending upon the technology available within in institution. AIM 20/20, for example, supports the automated creation of reports and presentations found in Office 365 or Microsoft SharePoint.

Once created, intelligence work products will be disseminated via several routes: immediate-action intelligence may be directly reported in-person; other intelligence may be sent via e-mail, pushed to mobile devices, or incorporated into electronic data sent via networks to other departments or agencies.

Regardless of the dissemination method, the command and control software for threat prevention, detection and investigation should keep an audit trail of what information was disseminated to whom, and my what means.

ARCHIVING

In the final phase of the intelligence cycle, information should be stored in such a way that it can be searched and retrieved as input for subsequent analyses and investigations. Traditional archiving methods were based on in-house storage in databases, but new, cost-effective technology offers other storage options, principally cloud-based storage which AIM 20/20 supports.

A full discussion of cloud-based storage and intelligence management and analysis is beyond the scope of this paper. Suffice it to say that concern is frequently expressed that cloud-based storage is *prima facie* less-secure and more vulnerable than other on-site storage methods.

While this may seem obvious, just the opposite is true. Large, cloud-storage providers like Microsoft Azure are subject to hundreds of thousands of malicious network attacks each week. Because of this, their networks are hardened and better-protected than the majority of institutional networks.

When data stored in the cloud is encrypted through sophisticated double-key methods such as public key encryption (PKE), even legal access to that data only results in the retrieval of unintelligible information without the presence of the second key held by the originating institution.

Perhaps the best testament to the security and integrity of cloud-based storage is found with Mexico's *Servicio de Administración Tributaria* (SAT), the Mexican equivalent of the U.S. IRS, which processes millions of dollars a day and stores all of its sensitive financial information in encrypted form in the Microsoft Azure cloud. SAT is a lynchpin of the Mexican government's efforts to fight fraud and corruption.

CONCLUSIONS

Modern public safety and national security agencies face asymmetric threats such as terrorism, where detection, prevention and investigation can benefit from the tools, techniques, and mindset of classic intelligence analysis.

State-of-the-art software, such as AIM 20/20, offers data management, data-sharing, data analysis, and data visualization tools. Software that supports intelligence analysis increases the efficiency of threat detection, prevention and investigation, and helps reduce costs. The goal of intelligence analysis is providing public safety and national security agencies a solid basis for making decisions and taking actions to combat the modern-day threats they face.

For more information about AIM 20/20, please contact our representative:

JTi JohnsTek®
Strategic Technology Engineering

JohnsTek, Inc.
45 Almeria Avenue
Coral Gables, FL 33134
+1.786.375.9020
info@johnstek.com
www.johnstek.com