Fight crime.
Unravel incidents... one byte at a time.

ARTIFICIAL INTELLIGENCE AND LAW ENFORCEMENT

GIAC (GCFA) Gold Certification

Author: John Wulff, john@jwcyberforensics.com
Advisor: Chris Walker
Accepted: August 21, 2017

Abstract

After the 9/11 terrorist attacks against the United States, law enforcement, and intelligence communities began efforts to combine their talents and information gathering assets to create an efficient method for sharing data. The central focus of these cooperative efforts for information dissemination was State Fusion Centers, tasked with collecting data from several database sources and distributing that information to various agencies. This vast amount of intelligence data eventually overwhelmed the investigative organizations. The use of Artificial Intelligence (AI) is the preferred technology for analyzing data to recognize behavioral patterns and create a method for the sharing of data in the fight against crime and terrorism. AI can analyze threat data and historical information and then create attack hypotheses for predicting when and where crimes will be committed. The use of AI can directly affect the cost of operations. Criminal activity locations can be predicted by AI so equipment and personnel can be directed to those areas to prevent those events from occurring. Financial resources must be allocated to allow for the development and testing of these applications so that the options available to law enforcement and the intelligence communities can be increased.

Introduction

On the morning of September 11, 2001, at 8:46 an airliner carrying 10,000 gallons of fuel crashed into the north tower of the World Trade Center in lower Manhattan. A few minutes later, at 9:03 a second plane hit the south tower. Both structures collapsed in less than 90 minutes. On the same morning, at 9:37 a third airliner slammed into the Pentagon and at 10:03 a fourth plane crashed in a field in Pennsylvania, its target never reached due to the heroic actions of passengers with knowledge of the previous attacks. The human death toll from these events amounted to nearly 2700 (9/11 Commission, 2004).

Nineteen young Arab men, implementing the plans of Islamic extremists in Afghanistan, committed these acts of terrorism. Some had been in the United States for over a year and blended into the population. While four had training as pilots, the rest were not well educated and spoke English poorly. In small groups, they were able to carry knives, box cutters, Mace, or pepper spray onto the hijacked jetliners and convert them into deadly weapons (9/11 Commission, 2004). How did this happen? How were they organized and financed? How did the authorities fail to anticipate and prevent this tragedy?

1.0. Fusion Centers & Information Sharing

These events highlight the inability of law enforcement and the intelligence community to effectively share information. The 9/11 Commission Report found that the United States, while having access to vast amounts of data and information, is ill equipped to process the data that it has. The report suggested that the Intelligence community's culture of "need to know" be replaced with "need to share". Moreover, the report recommends that the President lead an effort to turn an outdated mainframe structure into a distributed network. In response to these recommendations, the law enforcement and intelligence groups began efforts to combine assets, knowledge, and skills in the pursuit of terrorists and to gather intelligence to prevent further attacks (9/11 Commission, 2004). The central focus of these cooperative efforts for sharing information was State Fusion Centers.

A State Fusion Center is defined as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their

ability to detect, prevent, investigate, and respond to criminal and terrorist activity" (Fusion Center Guidelines, n.d., p. 12). While the exact makeup of the centers varies from state to state, they are mostly comprised of state and local law enforcement agencies, public health and safety organizations, and federal agencies, most notably, the Federal Bureau of Investigation, U.S. Department of Homeland Security, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives. The mission of fusion centers is to bridge the gap between these agencies, facilitating real-time information sharing. In addition to providing this intelligence, fusion centers provide agencies all-encompassing views of the threat environment (Grant & Terry, 2005). The end product of this mission is a tremendous amount of data that is generated and must be disseminated to the various law enforcement agencies that can best utilize these data.

However, fusions centers have come under great scrutiny from Congress and the law enforcement community because of their perceived inability to digest the amount of data that they are collecting and distribute it in a meaningful way (Sypherlink, 2008). For example, terrorism often involves multiple suspects who are connected through various relationships. It is necessary to use research techniques such as link analysis to digest the information regarding these individuals and treat them like a network in which they interact and participate in differing roles. The adaptability and learning protocols inherent in Artificial Intelligence (AI) make it a solution that can constantly monitor the changing landscape of these criminal and terrorist networks.

A study of this landscape often involves criminal network analysis by studying drug trafficking, fraud, gang related crimes, armed robbery, etc. An analysis of criminal network activity with AI can highlight previously unknown relationships between the actors in the criminal network and can identify and classify the individuals or groups into their appropriate network roles. This combination of network and behavior analysis can also be used to predict the commission of terrorist and criminal events, using the same AI techniques that retailers use in predicting the purchasing habits of consumers.

The purpose of this research was to examine how law enforcement actors can better evaluate data distributed by fusion centers. What would Artificial Intelligence's role be in the aggregation of critical threat data into actionable intelligence? How could Artificial Intelligence be used as an aid to intelligent policing? How could resource management leverage Artificial Intelligence for more effective deployment of resources?

John Wulff, john@jwcyberforensics.com

By looking beyond state and national borders, the fusion centers are intended to enhance the ability to predict crime and terrorism, rather than just react to events. Fusion centers analyze information from local criminal activity and can therefore determine whether a connection exists between that activity and terrorist threats. It is possible that the application of Artificial Intelligence to the processing of these data can help with these connections.

1.1. Advancing Law Enforcement

The existence of fusion centers and their mandate to coordinate and disseminate these data has moved the technology of crime fighting into new territories of advanced law enforcement. The use of information technology gives these local agencies access to a vast amount of information and data, for better or worse that would previously be unavailable to them without this technology, and has coined the term, Intelligence-Led Policing (Grant & Terry, 2005).

This information access is increasing exponentially and law enforcement must keep up with the amount of data collected. In order to create actionable intelligence necessary for successful Intelligence-Led Policing, crime analysis is completely dependent upon the quality of the data or information collected and the ability to collate and interpret its meaning. According to Canter (2000), the criteria for designing the data collection processes that will create the greatest possible relevance to the crime analysis are:

1. Timeliness: Does the pattern of the data or information relate to the current problem or are they indicative of a previous issue?
2. Relevancy: Is this information an accurate representation of that needed to carry out the intended task?
3. Reliability: Would different people come to the same conclusions after examining these data?

In order to foster the technological and organizational capacities for information sharing, the National Institute of Justice made information sharing its top priority among state and local jurisdictions as well as internationally (Tomek, 2001). However, as the universe of collaborative participants expands, the difficulty in sharing information is

related to different agency formats, protocols, standards, and even how extensively the data is collected (Tomek).

Other overarching issues for the sharing of these intelligence data is the sheer amount of it as well as the expertise necessary for its proper distribution. “Sharing isn’t bad, it’s broken” ("Cyber intelligence tradecraft," 2013, p. 5). This was a point from the Carnegie Mellon Software Engineering Institute’s *SEI Innovation Center Report: Cyber Intelligence Tradecraft Project Summary of Key Findings.* The report, known as the CITP, examined the cyber intelligence, methodologies, best practices, technologies, processes, and training from six government agencies and 20 organizations from industry and academia. It concluded that while some organizations excel at gathering and analyzing data from various sources, the sharing and dissemination of those data, lack the finesse and efficiency that are necessary for confronting the cyber conflicts that are prevalent in the world ("Cyber intelligence tradecraft, 2013").

According to the Carnegie Mellon report, government agencies that were profiled in the CITP were quite capable at sharing data internally. The agencies stated however, that access to data from external organizations was difficult and challenging. The arguments of classification and need-to-know restrictions on information sharing were no longer true, due to technology solutions available. Most cited that the organizational culture that was in place was the biggest hindrance. Organizations in industry and academia shared this cultural bias prevalent in government; they are reluctant to share “sensitive” indicators and intelligence data with competitors. Those who are able to overcome this bias, by sharing indicators of malicious activity, analytical reports and various data surrounding malware and suspect IP addresses, have enjoyed success in being able to stay ahead of the cyber threats ("Cyber intelligence tradecraft," 2013).

Unfortunately, no framework is fully in place that provides a common format for the importing of these data into the analytical structure of the organizations and agencies. It does not matter how these entities process their information internally, a common output format must be designed for importing into the analytical processes. Protocols are in place as an attempt at this standardized output; the National Information Exchange Model and its components, is one example (Fusion Center Guidelines, n.d.). There are a number of other

options available to be explored, which would allow agencies to leverage existing resources.

Among these options would be the development of an effective Artificial Intelligence (AI) system to deal with the problems of extracting information from the massive amount of background data on both criminal and terrorist activities. Through a blend of learned pattern matching and relationship development on these indistinct and scant indicators of potential or actual threat activity (Steinberg, 2009), an AI solution can be crafted to adaptively generate attack hypotheses, analyze and process these hypotheses, as the program begins to understand the situation. The software's integration of the data from diverse database sources and "context-conditioned" reasoning will help agencies manage threat activity (Steinberg).

1.2. Different means of terror

This threat activity information being delivered by the fusion centers reflects the fact that terrorist groups and modern day criminal entities are beginning to cultivate alternative ways to interrupt or demolish critical infrastructures (Johnson, 2012). Sometimes these plans generate patterns, but usually not. AI applications can be developed to address the common issues of searching through massive collections of unstructured data from unrelated or confidential data sources. These hypothesis development and examination techniques can create a solid foundation for new data mining approaches by law enforcement (Johnson).

The San Diego County Automated Regional Information System (ARJIS) is an example of a carefully crafted attempt at bridging the inter-jurisdictional data-sharing barriers. Information from 71 state, local, and federal agencies in the two California counties that border Mexico, San Diego and Imperial counties, is compiled into one website that registered law enforcement agencies can access (ARJIS, 2007). ARJIS is updated every 24 hours with crime-incident data, most-wanted listings, and interactive maps. This secure network, known as ARJISNet, brings together data from approximately 11,000 police, court, and corrections officials who are registered on the system. This virtual private network protects its databases via firewalls and assigned passwords (ARJIS).

The secure network feeds over 6,000 workstations with 4,265 square miles of San Diego County. The number of daily transactions coming into the system number over 35,000. ARJIS provides all manner of tactical analysis, statistics, and crime analysis. The participating agencies share the collated information among all levels of operation, from chief to officers to technical staff (ARJIS, 2007).

ARJIS provides a number of elements directed at major public safety resources such as wireless access to photos, warrants, and other data helpful to the field officer. Mapping of crime and sex offender data, analysis of crime analysis tools, and other applications useful in solving crimes and identifying offenders, is provided as an enterprise-wide system. Due to its unique positioning in the community, the system is an information clearing house and distribution center for officer warning, information sharing, and the interchange, corroboration, and real-time uploading of public safety data (ARJIS, 2007).

The Pennsylvania Integrated Justice Network (JNET) is a network connecting all of the state's criminal justice organizations. Users of the system can submit a name to the JNET Web site, and it will query all of the connected databases and return the results viewable on a web browser. Offender photos and images of any distinguishing marks are part of the database. In one case, a perpetrator was caught because a victim was able to describe a tattoo on the offender to police (Walsh, 2003).

Unlike, ARJIS, JNET does not have a public interface. While it is solely dedicated to law enforcement use, JNET runs on the public Internet using a digital encryption scheme of assigned digital certificates that are allotted to users of the system that encrypts their logon credentials and gives them access to appropriate sections of the network. This secure web portal arrangement allows access to over 38,000 criminal justice members throughout 67 counties in Pennsylvania as well as federal, state agencies, and municipal police departments (Pennsylvania, n.d.).

While the interconnection of disparate databases from various law enforcement entities is made possible by the new technologies, a phenomenon known as "linkage blindness" occurs, due to differences in data storage and collection techniques between the various agencies. At its core is the fact that there is a lack of critical communication links between various jurisdictions and the criminal justice system and the broad community (Grant & Terry, 2005). The variety of the various criminal justice disciplines and

foundational responsibilities make this data-sharing problem even more complex (Tomek, 2001).

Two years after the establishment of San Diego County's ARJISNet network, a number of gas station robberies occurred in Los Angeles County. A group of men in Torrance, California, perpetrated them and while appearing to be a typical local crime, they actually financed a larger scheme to attack military and Jewish facilities. This case sustains the fact that no longer are the lines between criminal and terrorist activities so clearly defined, and that fusion centers are vital in helping those agencies obtain a broad overview of the threats that they face (Torrance, n.d.). A major question is how could AI and the interconnectivity of the various databases, such as those developed by San Diego's ARJIS and Pennsylvania's JNET, be used to develop inferences from patterns of criminal activity and relationships, and aid in the pre-crime detection of the events in Torrance, California and those of 9/11. Patterns of money-flow to the 9/11 hijackers, aviation training, types of crimes in Torrance and their locations, could have allowed AI to create relationships between these activities and alerted authorities to investigate further.

2. Discussion of Findings

What would Artificial Intelligence's role be in the aggregation of critical threat data into actionable intelligence? How could Artificial Intelligence be used as an aid to intelligent policing? How could resource management leverage Artificial Intelligence for more effective deployment of resources?

The battle strategy for dealing with criminals and terrorists depends upon information. However, there is an inability for the various participants in the law enforcement and intelligence communities to share these data. The U.S. can't begin to analyze all of the data that it is collecting. There is now so much of it that AI is the only effective way to monitor, analyze and manage it.

In researching the means for sharing of information used to combat criminal and terrorist acts, if was found that government organizations did not have any trouble with information being shared internally between their various departments. Where they do have problems is receiving data from external organizations. While organizational cultural

differences are most likely to blame, it is also shown that data collected does not exist in a common format that all participants can use.

The fusion centers were created to share data among the various agencies and organizations but they have generated so much data that the problem of sharing and analysis of the data collected has been exacerbated. This has led to organizations that could benefit from the sharing of intelligence data, adopting an organizational culture that prohibits the sharing of intelligence information. It is too difficult to accurately share the intelligence, given the amount and incompatibilities of format. As a recent study conducted by Carnegie Mellon discovered, “Sharing isn’t bad, it’s broken” ("Cyber intelligence tradecraft," 2013, p. 5). The best performing organizations do not just consume data they have informal sharing arrangements with other organizations.

Simplifying the process of sharing data, while attempting to predict crime and terrorism, evaluation of the fusion center information by these organizations would benefit from an Artificial Intelligence application. Its ability to analyze the data returned and to use pattern matching, coupled with behavioral analysis, along with the identification of the connections of all events, allows AI to determine the likelihood of criminal activity in the communities from which the data was returned. In susceptible areas, burglaries will occur at the same houses because burglars there will know the vulnerabilities of that area. Gang violence is also clustered because a gang shooting will often produce revenge shootings intended to enhance the status of the gangs.

AI’s ability to gather and parse information is totally dependent upon agencies and organizations that have an interest in responding to these criminal acts. These organizations can also provide valuable data for AI to collate and disseminate to the appropriate agencies. Hospitals in the area and emergency services, city public works agencies, federal law enforcement agencies, probation and parole agencies, bar and nightclub owners and managers, social service providers, and members of neighborhood groups, are all stakeholders that can provide and benefit from actionable intelligence related to crime and crime prediction that has been processed by Artificial Intelligence.

The timely sharing of information between various jurisdictional entities in disparate geographic areas is generally agreed to be the primary weapon against terrorist and criminal acts. At all government levels, the fusion centers are thought to be the most

efficient way to share this information in not only a timely, but cost effective way. Therefore, fusion centers are located in most states and generate an enormous amount of data used to coordinate counter-narcotics activities as well as the policing of illegal immigrants. The Department of Homeland Security deems fusion centers “all-crimes” centers ("Fusion centers: Turning," 2008).

However, the complications of working with data in incompatible formats can be eased by applying AI in the form of software entities known as intelligent agents. While compiling data on a target or individual, if data formats differ, the agents can reformat the data according to rules set forth for compatibility. Then, as the data is arranged into a dossier, the agent will interpret its findings and, as determined by its rules, act on those interpretations and alert to any conditions that might trigger the notifications.

AI will aggregate critical threat data into actionable intelligence by creating a common framework and format for these data to be effectively analyzed by both human investigators and learning machines. AI will overcome format inconsistencies and relieve the investigators of the burdensome tasks of decoding and reformatting the data before any effective analysis can begin.

Artificial Intelligence and its associated agents can act as information detectives for law enforcement. It is important to be aware that in order for information to become usable, it must be timely and meaningful. The agents must be able to constantly monitor information and determine if there is a better source or means of analysis for interpreting the intelligence received.

Pattern matching is key to creating actionable intelligence; otherwise, it is just a large amalgamation of data with no connections between elements. AI’s ability to discern patterns of behavior and therefore predict future outcomes creates a real tool for finding a use for the data collected. Since finding a use for these data is the intent of data fusion, AI’s ability to learn and pattern match allows it to fit right into this plan of creating actionable intelligence from the vast amounts of data collected.

The vast amount of data produced and available to government and law enforcement has led to the creation of the discipline of Intelligence-Led Policing. An AI program can be crafted to adaptively generate attack hypotheses, analyze, and process these hypotheses as the program begins to understand the situation. The software’s

integration of the data from diverse database sources and "context-conditioned" reasoning will help agencies manage this threat activity through machine learning.

Machine-learning algorithms are sets of adaptive instructions telling the computers that are parsing the intelligence how to carry out their work. The adaptation and adjustments by the associated data instructions provide the best processes for allowing Intelligence-Led Policing to profile criminals and terrorists. The process of data mining involves the use of various statistical and pattern-recognition technologies to take raw data and determine relationships and dependencies between the various elements of that data.

An AI tool known as the Peer-to-Peer Inference System (P2PIS) can organize data for law enforcement from these elements. This solution would require the use of autonomous software agents, placed within the related network and data base systems, called peers. Each of the peers would use a knowledge base related to the database application to which it is monitoring. Any peers having similar interests could establish links, known as mappings, between their individual knowledge bases.

These mappings set up inferences and relationships between the various databases that would allow them to create a dialogue that would be helpful in developing a "semantic" communication between peers ("Artificial intelligence and," 2008). When new data appears in the database, the "semantically-mapped" peers would be tasked to check their knowledge bases. After a number of queries over time, they would be able to find related consequences, conduct diagnoses of these inferences, and warehouse the related data. These data could be stored for knowledge examination and "learning" in order to alert authorities of possible anomalies in behavior, a critical component in Intelligence-Led Policing.

Had the patterns of four young Arabic men taking flying lessons for flying large aircraft without learning how to land them been examined more closely for statistical and pattern matching, the attacks of September 11 might never have happened. Sometimes, these relationships and patterns are previously unknown and are identified solely using data mining. Intelligent data mining with AI and intelligent agents can do a better job of predicting criminal or terrorist acts by assessing risk. AI, while enabling intelligent policing techniques to analyze observed behavior and model it, can assist the analyst in determining

whether that behavior will happen again. This is performed in exactly the same way retailers are identifying consumer-purchasing habits with behavioral profiling.

Behavioral profiling can involve criminal network analysis, which often requires the ability to integrate information from various sources, and discover patterns emerging about organization, processes, and how information flows within a criminal or terrorist organization (Xu & Chen, 2005). This analysis can become very expensive and would require funds to be dedicated solely for the purchase of AI software as well as manpower to interpret the output.

In order to disrupt or predict operation patterns of these networks, data retrieved via the use of sophisticated AI pattern matching techniques need to be reliable and are essential to the success of any investigation. However, as is usually the case, the intelligence and law enforcement agencies are faced with a huge amount of data. Manual interpretation of these data is difficult, but AI could be used to assist in the criminal network analysis. The manual data mining techniques used in other data acquisitions are more prone to difficulties when dealing with criminal networks due to:

- Incompleteness - criminal and terrorist networks by their very nature operate covertly (Krebs, 2001). Criminals rarely interact with each other in order to minimize attention from police. Any interactions that exist are kept hidden behind their illicit activities. Any data about the criminals and their networks are missing nodes and links, and present incomplete patterns and associations that are troublesome, if parsed manually (Sparrow, 1991).
- Incorrectness - data regarding the suspects' identities, physical characteristics, and addresses are usually incorrect due to faulty data entry or deception by criminals who usually lie about their identities when apprehended.
- Inconsistency - when a criminal has multiple contacts with police his information will be entered into the criminal databases multiple times. These records are neither compatible nor consistent and would make the single criminal appear to have multiple identities and appear to be different individuals.

Another reason for the use of AI to help with proper analysis of these data for the law enforcement community is that an investigator must deal with the inherent problems in using multiple databases. AI can help with:

- Data transformation - AI would present the data in a specific format that would be conducive to network analysis, showing network members as nodes, and their associations or interactions as links. When given the appropriate rules for the associations and pattern recognition, AI would be able to parse the raw data and visualize these relationships for the investigator.
- Fuzzy boundaries - the various terrorist and criminal networks are likely to be ambiguous. An analyst would have a difficult time trying to place subjects in one network or another (Sparrow, 1991). AI would be able to ingest a larger number of datasets and categorize accordingly, greatly easing the burden of the analyst.
- Network dynamics - criminal networks are subject to change all of the time and are not static (Sparrow). AI will be a critical tool for the analyst to capture the dynamics of criminal networks.

Social Network Analysis (SNA) utilizing AI will be the ideal combination of critical analysis tools. SNA is specifically designed to recognize any patterns of behavior and interaction between social actors in social networks (Wasserman & Faust, 1994). Modernize these techniques with the self-correcting and machine-learning techniques presented by AI and intelligent agents to reveal the various structures and interactions in these terrorist and criminal networks, and the dismantling of these terrorist and criminal networks will be made easier.

The leveraging of Behavioral Recognition Technology by intelligence-led police organizations will be made easier by coupling this technology with machine-learning techniques that can provide actionable intelligence in real-time by alerting authorities to camera-observed anomalous behavior. It is relatively simple to program a computer to detect movement in a video image. It is just as simple to apply a “rule” and have the computer alert when that movement violates the conditions of that rule. The slightest variation in the environment in which the video is monitoring can cause miscalculations and false alerts which can provide frustrations to those monitoring the alerts (BRS Labs,

2012). Since surveillance video plays an important part in the prediction of crime, AI will be needed for interpretation and analysis in order to lessen the chances of miscalculations and false positive or false negative alerts.

The data mining evolution will also be enhanced through AI by the creation of algorithms that allow software to learn, grow, and improve independently. Neural networks have also advanced to where they are accepted tools for classifying, predicting, and profiling. The successful development of intelligent agents that can move out into networks and the Internet and look for whatever information they were programmed to retrieve, are the norm. All of these elements, when combined, allow AI to develop theories that can point to everything from fraudulent credit card transactions, to identifying tanks on the move from satellite imagery. These applications can learn, grow, and adapt to creating actionable intelligence that can even be used to thwart potential criminal activity (Mena, 2003).

From identifying which of the millions of people who cross United States borders each day is a smuggler, to predicting that a merchant on eBay is about to abandon successful bidders and skip out with hundreds of thousands of dollars, AI can bring a new dimension to law enforcement's ability to predict and prevent crime. Statistical Criminal Analysis, utilizing AI can take prior criminal and terrorist activities and cross-reference the variables and baseline data characteristics into relational connections for change and relevant dependencies ("Artificial intelligence and inference," 2008). This is the intent of AI being applied to the data and interpolating any relationships between those data. Once that relationship is defined and codified, it will be in a better format for disseminating to law enforcement and intelligence agencies.

AI's potential for pattern matching and inference of data relationships would make it ideal for integrating the identification and analysis of continuing problems such as auto theft or drug crimes, and would assist in studying and evaluating relevant responses and procedures for dealing with these crimes.

Before the era of Intelligence-Led Policing, the entire policing strategy was based on random patrolling of areas, responding to an incident as rapidly as possible, and investigating why the crime was committed after the fact. While this was an effective means of thwarting crime, due to its unpredictability, managers tasked with making the

efficient use of police resources were hard-pressed to keep up with the ever-changing face of crime in their communities (Ratcliffe, 2008). A reactionary means of determining how patrols were to be set up and maintained was not the best way to allocate manpower and equipment.

Crime analysis has been defined as comprising “the collection and analysis of data pertaining to a criminal incident, offender, and target” (Canter, 2000, p. 3). This analysis should ideally help police managers in making decisions for resource deployment and allocation, provided these decisions are linked to a true understanding of the nature of the problem. The Center for Problem-Oriented Policing states that police organizations need to see the relationship of data collected to the components of the crime triangle, defined as victim, offender, and location, to develop creative solutions for suppressing, intervening, and preventing crime ("The problem analysis,"). Canter (2000) provides the best source for understanding what must be done with these data to transform them into actionable intelligence. This crime analysis is best organized into strategic and tactical forms.

Analysis of data collected over a long period of time is considered strategic crime analysis. The use of statistics to make conclusions puts this analysis into a research focused container (Charlotte-Mecklenburg, 2013). This aggregated data can be assembled into monthly, quarterly, and/or yearly sets of criminal and non-criminal data aggregations. The categories of date, time, location, and type of incident are analyzed at a statistical level instead of analyzing narratives of the incidents. Variables in the data are analyzed as well. These variables consist of race, class, sex, income, population, location, and location type (Boba, 2001).

With a heavy dependence on research, law enforcement agencies and departments can find this analysis useful for crime-trend prediction based on past trends in criminal activity (Canter, 2000). While utilizing this crime-trend prediction, resources such as patrol schedules, can be adjusted as a reflection volume of activity. Strategic crime analysis can point to changing community dynamics and risks for specific criminal patterns in specific areas. The partnerships between police and other public and community agencies would help to reduce criminal activity on a more long-term and sustainable basis (Charlotte-Mecklenburg).

John Wulff, john@jwcyberforensics.com

With strategic crime analysis using data representing a period of a year or more, tactical analysis depends on real-time data from several days or less. This analysis can be used on data from an area as large as an entire departmental jurisdiction or the few block radius of a crime hot spot. The pattern identification of multiple offensives over a short period of time can be determined via the type of crime and type of weapon used in the commission of that crime (IACA, 2011).

Another potential product of tactical crime analysis is linkage analysis which can connect a suspect to a series of incidents based on modus operandi, suspect description, as well as the identification of known offenders, living in close proximity to a given area (IACA, 2011). As an example, many police departments regularly search their databases for sex offenders in the area whenever a sexual offense is identified. This use of target profiling can determine the risks that are endemic to an area based on known crime patterns. Using the data from the previous example of sex offender proximity, some police departments have experimented with profiles that reflect community risk (i.e. day care centers, parks, etc.) as a catalyst for notifying the community of the presence of registered sex offenders (Canter, 2000).

AI, with its ability to predict patterns and identify likely areas of criminal activity, provides a more economical alternative for resource management, crime prevention. Police departments are always facing budget cuts and while outsourcing is not the solution, predictive policing can bring resource management to a new level of efficiency and optimization. It is the proper use of AI and predictive modeling that will be beneficial to the departments and to the community.

Companies like Wal-Mart have long embraced the ability to predict or anticipate future demand. For example, when a large weather event is expected, Wal-Mart may redirect its supply chain to distribute duct tape, bottled water, and Pop-Tarts to the affected area before the storm hits. While it is understandable that duct tape and bottled water will be needed in the time of disaster, Pop-Tarts may seem like an odd choice. Wal-Mart has years of experience in dealing with large weather events and has found that there is an increase in sales of Pop-Tarts, strawberry Pop-Tarts to be exact (Borne 2006). Pop-Tarts have the benefits of not needing to be cooked; they're flavorful; kids to not have to be

coerced into eating them, etc. This is the discovery part of predictive analysis, which can be a powerful ally in policing and resource management.

The disciplines of computer science, law enforcement, intelligence, and health have long had technical issues with searching through large amounts of data in the form of unstructured text and databases ("Artificial intelligence and," 2008). All of these techniques rely on crime pattern identification techniques for their planning. Research has shown that crimes usually occur in populous areas. A completely random pattern of crimes rarely occurs. The application of AI techniques would allow the usage of predictive analysis to be integrated with point randomization processes, in order to better understand the influences of these processes on crime. An AI algorithm could be developed to analyze a seemingly random pattern of data and possibly reveal the underlying processes for crimes, while pulling these point patterns to the top for additional study, therefore allowing resources to be allocated accordingly, thus making fusion centers viable.

From a Cyber Crime perspective, AI can be applied to data relating to cyber threats. In this case, there is a framework that has been created to identify the behavioral characteristics of cyber threat bad actors (ODNI, n.d.). The Cyber Threat Framework provides a consistent format for the information regarding cyber threats. AI's benefit to this Framework would consist of developing the most efficient use of this information to the policy and decision makes in the law enforcement community so that they can determine the most beneficial use of the economic and personnel resources.

AI is the perfect tool to aggregate information from the specifications for cyber security, STIX – Structured Threat Information Expression, TAXII – Trusted Automated Exchange of Indicator Information, and CybOX - Cyber Observable Expression (Oasis, 2015), and focus the appropriate behavioral characteristics for cyber threat actors into the disciplines of prevention, detection and remediation. This use of AI will lift the burden of classification of these data for the cyber analyst and provide a faster and more effective result for determining who is to blame and how to respond.

John Wulff, john@jwcyberforensics.com

3. Future Research and Recommendations

Fusion centers have been criticized for excess spending and not performing as intended ("Federal support for," 2012). Despite criticism in Congress, it doesn't look like fusion centers are going to be dismantled. A Department of Homeland Security white paper on budget recommendations for 2013 placed a strong emphasis on maintaining and growing fusion centers ("FY 2013 budget," 2012).

It is recommended that a budget item for this maintenance and growth be included for the development of Artificial Intelligence software and procedures for the analysis of data collected by these centers in the Federal Budget. Money that is granted to active fusion centers is often spent on training, improved communications systems and various items associated with any incidents that might result in mass casualties (Hodai, 2013). The ability to determine patterns of behavior in order to predict these events would be enhanced with the implementation of AI and monies intended for mass casualty reaction could eventually be redirected to other pursuits.

Not only will budgets need to account for the development or purchase of AI software but training as well. Training for fusion center personnel is usually conducted to instruct in the rules concerning classified information as well as the type of information these personnel will expect to receive during fusion center briefings ("Considerations for fusion," 2010). A new level of expertise will be required due to the fact that while the AI software will do a majority of the "heavy lifting" to extract the appropriate information, it will take a knowledgeable team of operators to examine the output from these programs to determine if the projected assumptions are reasonable. It would be foolhardy to blindly trust the output from the AI programs without a formal program of checks and balances.

The personnel at the closest layer of the intelligent agents being used for data collection and classification will need to be conversant in the techniques being used by AI and the agents. Knowing what is being done "under the hood" will help to monitor the output of the data that the agents are producing. Then the data can be passed on to the subscribing agencies or other investigators, once the formatting of the data is arranged in a compatible format for analysis.

John Wulff, john@jwcyberforensics.com

The fusion centers operate under a mandate that is broad and ambiguous. The task before them is to fuse data to produce "intelligence" that can be used to prevent terrorist acts. The fact that they are also expected to respond to all crimes or hazards amounts to an invitation for personnel at the fusion centers to engage in almost any surveillance that they think is necessary to accomplish the task. This amount of flexibility has a perceived benefit to local police departments to use the Department of Homeland Security and other assets for whatever needs the departments deem as being necessary to address the tasks at hand, for their particular jurisdiction. However, it is suggested that people at some fusion centers are exploiting this leeway granted to them to engage in racial profiling, political profiling, illegal data mining, and illegal data collection (Monahan and Palmer, 2009).

Given the myriad amount of data sources and options available to the fusion centers, it is possible that "mission creep" or "function creep" develops, whereby analysts exceed the policies and laws that govern their activities (Monahan & Palmer, 2009). The implementation of AI will allow this collection to proceed at a much faster and broader pace. It is recommended that a more detailed study of the effects and possible incursions into the privacy of individuals due to the increased efficiency of AI in the collection and analysis of data, be conducted.

Assuming that the intelligence gathered was better and presented a more reliable means of predicting crime or terrorist events, what should be done with this information? The prospects of incarceration or invasion under the predictive assumptions that AI can create, seem excessively harsh, considering the alternatives available, such as surveillance or containment. The laws must be modified for the new concerns that AI will generate.

The strategies that police departments use over the years are constantly evolving. The potential use of Artificial Intelligence to enhance the current tactic of Intelligence-Led Policing (ILP), while still in its infancy, can become an effective tool for police investigations. In order for AI techniques to be crafted into the everyday operations for crime fighting, an examination of the attitudes and opinions of police managers be conducted to identify any hurdles or resistance to the fusion of AI with ILP.

Based on the findings of that research, police administrators would be able to anticipate any problems and understand the mind-set of supervisors. Historically, police resources and responses have always come from goal shifts. In London, for example, Sir

Robert Peel first organized the London Metropolitan Police to focus on crime prevention, instead of response (Johnson, 1988). Technological advances, such as telephones and cars, reduced response time and expanded the areas an officer could cover during patrol (Philips, 2012). As with these advances, AI can help to shift the goals of Intelligence-Led Policing into a pre-crime detection phase.

The ability to have AI identify covert intent of individuals who may be contemplating hostile activities would improve the counter-insurgency and peacekeeping operations. These persons are usually deeply embedded in the "clutter" of neutral, friendly individuals. Whether this identification is accomplished through facial recognition technologies or pre-crime analysis of acquired data, studies should be conducted to reduce false-negative and false-positive rates. By determining covert adversarial or hostile intent in advance, the resources needed for operations, planning, training, and simulations can be redirected from broad based approaches to more defined, targeted operations based on AI's predictions of activity.

Obviously, additional funding for testing the use of AI for pre-crime detection, if implemented, will be needed. The most obvious source of this funding will be the Federal government. Advancing Intelligence-Led Policing will require research and development programs for AI and should be promoted by programs from U.S. Department of Defense, Department of Homeland Security, Intelligence Advanced Research Projects Activity and other Federal research and development (R&D) programs. Specifically:

- The Federal government should fund R&D of an AI prototype system for the parsing of data from regional fusion centers and a working model for the remote detection of covert adversarial intent.
- The Federal government should continue to provide extensive support for academic and industrial development of AI's ability to connect disparate systems of information necessary for the detection of remote adversarial intent. Recognizing this intent is a crucial central requirement for the success of AI in predictive crime analysis.

John Wulff, john@jwcyberforensics.com

4. Conclusion

The utilization of facial recognition technology along with the non-physical measurement of a suspect's vital signs, the attitude of the public regarding the potential for the technologies' encroachment on the suspect's 4th Amendment Rights must be studied. If an individual goes out in public and their image is captured by AI facial recognition technology, has that person, by default, given up all 4th Amendment privacy protection? This activity must be studied and conclusions drawn regarding the legal ramifications of this type of surveillance.

If the police community and the government were to move into a preemptive criminal investigation or military action posture, the data returned by AI would need to be tested to achieve a high level of accuracy. The potential for AI's ability to streamline the jobs of law enforcement and intelligence communities is immense, but the cost will be a factor. Homeland Security estimates that the money that will be spent on AI systems used for determining observable hostile intent in individuals will quadruple in the next three years (Pierson, 2012).

The amount of money involved makes this a multi-billion-dollar industry. It is only reasonable that a system of checks and balances be instituted to prevent the questioning or search of a person because a computer system thinks that the individual looks suspicious. The system can work if properly designed and vetted. The investment, while high, is worth the price.

John Wulff, john@jwcyberforensics.com

References

9/11 Commission, (2004). *The 9/11 commission report executive summary*. Retrieved from website: http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf

Artificial intelligence and link analysis: Papers from the AAAI fall symposium. (2001). Retrieved from http://www.aaai.org/Press/Reports/Symposia/Fall/fs-98-01.php

Boba, R. U.S. Department of Justice, (2001). *Introductory guide to crime analysis and mapping*. Retrieved from website: https://www.ncjrs.gov/App/publications/Abstract.aspx?id=194685

Borne, K. (2006). "Scientific Data Mining: Digging for Nuggets," seminar, Space Science Data Operations Office, July 5, 2006. Retrieved from http://74.125.93.132/search?q=cache:Anh6srZxtyEJ:classweb.gmu.edu/kborne/kborne-SSDOO-BBU5july2006.ppt+Scientific+Data+Mining+for+Nuggets&cd=4&hl=en&ct=clnk&gl=us

BRS Labs, (2012). *What is behavioral recognition*? Retrieved from http://www.brslabs.com/what-is-behavioral-analytics

Canter, P. (2000). *Using a geographic information system for tactical crime analysis*. In Analyzing Crime Patterns: Frontiers of Practice, edited by V. Goldsmith, P. McGuire, J. Mollenkopf, and T. Ross, 3–10. Thousand Oaks, CA: Sage

Carnegie Mellon, Software Engineering Institute. (2013). *Cyber intelligence tradecraft project: Summary of key findings*. Retrieved from http://www.sei.cmu.edu/library/abstracts/whitepapers/CITP-Summary.cfm?wt.mc_id=goto50

John W

Charlotte-mecklenburg police department: crime analysis division. (2013). Retrieved from http://www.charmeck.org/city/charlotte/CMPD/organization/Administrative/Pages/CrimeAnalysis.aspx

Department of Homeland Security, (2012). *Fy 2013 budget in brief*. Retrieved from US Government Printing Office website: http://www.dhs.gov/xlibrary/assets/mgmt/dhs-budget-in-brief-fy2013.pdf

Department of Homeland Security, Federal Emergency Management Agency. (2010). *Considerations for fusion center and emergency operations center coordination*. Retrieved from website: http://www.fema.gov/pdf/about/divisions/npd/cpg_502_eoc-fusion_final_7_20_2010.pdf

Fusion center guidelines: Law enforcement intelligence, public safety, and the private sector (n.d.). Retrieved from http://www.iir.com/global/guidelines.htm

Grant, H. J., & Terry, K. J. G. (2005). *Law enforcement in the 21st century*. Retrieved from http://www.pearsonhighered.com/samplechapter/0205336337.pdf

Hodai, B. (2013). *The homeland security apparatus: Fusion centers, data mining and private sector partners*. Retrieved from http://www.prwatch.org/node/12122

International Association of Crime Analysts. (2011). *Crime pattern definitions for tactical analysis* (White Paper 2011-01). Overland Park, KS: Author

In Chantal Reynaud (Chair). *Artificial intelligence and inference systems*. (2008). Laboratoire de recherche en informatique

Johnson, H. (1988), *History of Criminal Justice.* Cincinnati, OH: Anderson Publishing Co.

John Wulff, john@jwcyberforensics.com

Johnson, J. R. (2012, August). *Detecting emergent terrorism events: Finding needles in information haystacks*. Intelligence and security informatics conference (eisic), 2012 european, Odense, Denmark. doi: 10.1109/EISIC.2012.72

Krebs, V. E., (2001). Mapping networks of terrorist cells. *Connections 24, 3,* 43-52.

Mena, J. (2003). *Investigative data mining for security and criminal detection*. Butterworth-Heinemann

Monahan, T. & Palmer, N. (2009). "The Emerging Politics of DHS Fusion Centers." *Security Dialogue* 40, 6: 617-636.

Oasis (2015). *OASIS Advances Automated Cyber Threat Intelligence Sharing with STIX, TAXII, CybOX.* Retrieved from https://www.oasis-open.org/news/pr/oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox

ODNI: Office of the Director of National Intelligence (n.d.). *Cyber Threat Framework* Retrieved from https://www.dni.gov/index.php/cyber-threat-framework

Pennsylvania justice network: *Who we serve?* (n.d.). Retrieved from http://www.portal.state.pa.us/portal/server.pt/community/who_we_serve/21386

Philips, S. (2012). *The attitudes of police managers toward intelligence-led policing*. Retrieved from http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/september-2012/research-forum

Pierson, R. [Web log message]. Retrieved from http://www.lockergnome.com/news/2012/08/25/can-artificial-intelligence-detect-crime-before-it-happens/

Ratcliffe, J. (2008). *Intelligence-led policing*. Devon, U.K.: Willan Publishing.

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks 13* (1991), 251-274.

Steinberg, A. (2009). *An approach to threat assessment*. In E. Shahbazian, G. Rogova & M. J. DeWeert (Eds.), Harbour Protection through Data Fusion Technologies (pp. 95-108) Retrieved from http://link.springer.com/chapter/10.1007/978-1-4020-8883-4_16

Sypherlink Inc., (2008). *Fusion centers: Turning data into actionable intelligence*. Retrieved from website: http://www.sypherlink.com/support-downloads/white-papers.asp

The problem analysis triangle. (n.d.). Retrieved from http://www.popcenter.org/about/?p=triangle

Tomek, W. (2001). "Information Sharing: A Strategic Necessity." *Police Chief*. February, 2001. Retrieved from http://www.iacptechnology.org/library/techtalk/techtalk0201.pdf

Torrance, California: A genesis fable for fusion. (n.d.). Retrieved from http://www.publiceye.org/magazine/v24n4/a-genesis-fable-for-fusion.html

US Senate, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS. (2012). *Federal support for and involvement in state and local fusion centers*. Retrieved from website: http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04

Walsh, T. (2003). "Data Sharing Tightens Net for the Law—Agencies Put Criminal Justice Data On-line for Sharing." *Government Computer News*, July 10. Retrieved from http://www.gcn.com

Wasserman, S. & Faust, K. *Social network analysis: Methods and applications*. Cambridge

John Wulff, john@jwcyberforensics.com

University Press, Cambridge, MA, 1994.

What is ARJIS? (2007). Retrieved from http://www.arjis.org/WhatisARJIS/tabid/54/Default.aspx

Xu, J., & Chen, H. (2005). *Criminal network analysis and visualization*. Communications of the ACM, 48(6), 102-107. Retrieved from http://ai.arizona.edu/intranet/papers/communications_acm.pdf

John Wulff, john@jwcyberforensics.com

Last Updated: August 14th, 2018

Upcoming SANS Forensics Training

SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NY	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
Community SANS Columbia FOR610	Columbia, MD	Aug 20, 2018 - Aug 25, 2018	Community SANS
SANS San Francisco Summer 2018	San Francisco, CA	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, Denmark	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FL	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS vLive - FOR585: Advanced Smartphone Forensics	FOR585 - 201809,	Sep 04, 2018 - Oct 11, 2018	vLive
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LA	Sep 06, 2018 - Sep 13, 2018	Live Event
Threat Hunting & IR Summit - FOR526: Memory Forensics In-Depth	New Orleans, LA	Sep 08, 2018 - Sep 13, 2018	vLive
SANS Baltimore Fall 2018	Baltimore, MD	Sep 08, 2018 - Sep 15, 2018	Live Event
Threat Hunting & IR Summit - FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting	New Orleans, LA	Sep 08, 2018 - Sep 13, 2018	vLive
Threat Hunting & IR Summit - FOR572: Advanced Network Forensics and Analysis	New Orleans, LA	Sep 08, 2018 - Sep 13, 2018	vLive
SANS Munich September 2018	Munich, Germany	Sep 16, 2018 - Sep 22, 2018	Live Event
Community SANS Columbia FOR508	Columbia, MD	Sep 17, 2018 - Sep 22, 2018	Community SANS
Community SANS Toronto FOR508	Toronto, ON	Sep 17, 2018 - Sep 22, 2018	Community SANS
Community SANS Madrid FOR508 (in Spanish)	Madrid, Spain	Sep 17, 2018 - Sep 22, 2018	Community SANS
SANS London September 2018	London, United Kingdom	Sep 17, 2018 - Sep 22, 2018	Live Event
Network Security 2018 - FOR585: Advanced Smartphone Forensics	Las Vegas, NV	Sep 23, 2018 - Sep 28, 2018	vLive
SANS Network Security 2018	Las Vegas, NV	Sep 23, 2018 - Sep 30, 2018	Live Event
Network Security 2018 - FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques	Las Vegas, NV	Sep 23, 2018 - Sep 28, 2018	vLive
Network Security 2018 - FOR500: Windows Forensic Analysis	Las Vegas, NV	Sep 23, 2018 - Sep 28, 2018	vLive
Mentor Session - FOR500	Phoenix, AZ	Sep 28, 2018 - Nov 02, 2018	Mentor
Mentor Session - FOR500	Atlanta, GA	Sep 29, 2018 - Oct 27, 2018	Mentor
SANS DFIR Prague Summit & Training 2018	Prague, Czech Republic	Oct 01, 2018 - Oct 07, 2018	Live Event
Mentor Session - FOR500	Tampa, FL	Oct 06, 2018 - Nov 17, 2018	Mentor
SANS vLive - FOR526: Memory Forensics In-Depth	FOR526 - 201810,	Oct 09, 2018 - Nov 15, 2018	vLive
SANS Northern VA Fall- Tysons 2018	Tysons, VA	Oct 13, 2018 - Oct 20, 2018	Live Event
SANS London October 2018	London, United Kingdom	Oct 15, 2018 - Oct 20, 2018	Live Event