LAW ENFORCEMENT TECHNOLOGY IN COUNTERINSURGENCY OPERATIONS: IS CLEAR THE RIGHT TOOL?

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Security Studies

By

Ian A. Douglas

Washington, DC
April 16, 2010
LAW ENFORCEMENT TECHNOLOGY IN COUNTERINSURGENCY OPERATIONS: IS CLEAR THE RIGHT TOOL?

Ian A. Douglas

Thesis Advisor: Carol Christine Fair, PhD

ABSTRACT

The initial phase of the war in Iraq required traditional, high-intensity war fighting, in which the US was able to utilize its superiority in technology and firepower. After the high-intensity fighting was concluded, though, the role of US and coalition troops moved to stability operations and counterinsurgency. In an ongoing effort to improve US counterinsurgency efforts, the DoD has developed strategies, tactics, and technologies to help American troops better combat enemies that employ asymmetric warfare. This paper evaluates the effectiveness of one such innovation, the Citizen and Law Enforcement Analysis and Reporting System, and similar military versions, as a counterinsurgency tool. Its use in the civilian and military fields is studied to determine if further development of the program is worth investing in.
I would like to thank Dania Douglas and Rebekah Bina for their moral and editorial support during the duration of my research and writing process. I would also like to recognize Dr. Jennifer Sims and Dr. Bernard Finel, who aided me in the early stages of my topic selection. A special thank you goes to Dr. Carol Christine Fair, my thesis advisor, for her expert guidance throughout this process.
# Table of Contents

Chapter 1. Introduction ........................................................................................................... 1

Chapter 2. Methodology and Data Caveats .............................................................................. 4

Chapter 3. Policing Operations for Counterinsurgency .......................................................... 7
    Intelligence in Counterinsurgency ...................................................................................... 7
    Insurgencies and the Third Generation Gang Model ......................................................... 11
    The Soldier as a Beat Cop ................................................................................................. 15
    Requirements of a Law Enforcement Data System for COIN Intelligence ...................... 17
    Summary .......................................................................................................................... 18

Chapter 4. The Citizen and Law Enforcement Analysis and Reporting System 20
    Community Policing, Police Innovation, and the Development of CLEAR .................. 20
    Key Applications ............................................................................................................. 22
        Database Warehouse ................................................................................................. 22
        Automated Incident Reporting Application ................................................................ 23
        Automated Arrest ...................................................................................................... 26
        e Track ....................................................................................................................... 28
        COPLINK .................................................................................................................. 29
        Personnel Suite ......................................................................................................... 30
    Evaluation of Effectiveness ............................................................................................ 31

Chapter 5. Law Enforcement Data Systems in Counterinsurgency .................................... 34
    Legacy Systems: BAT and ABIS ..................................................................................... 34
    Case 1: Operation Snake Eater ....................................................................................... 35
    Case 2: The Camp Roberts Test ....................................................................................... 38
    Case 3: Al Qaim and Project METRO ............................................................................. 40

Chapter 6. Conclusions and Policy Implications .................................................................. 47
    References ......................................................................................................................... 50
Chapter 1. Introduction

The information revolution has influenced the way the US military operates. As the wars in Afghanistan and Iraq have progressed, we have seen the role of combat troops evolve. The initial phase in both conflicts required traditional, high-intensity war fighting, in which the US was able to utilize its superiority in technology and firepower. After the high-intensity fighting was concluded, though, the role of US and coalition troops moved to stability operations and counterinsurgency. The overwhelming superiority in firepower the US enjoyed early in the war is no longer sufficient to entirely degrade the guerrilla tactics of the enemy. Our military, instead, began to rely more heavily on intelligence and understanding of the battle space to enhance the effectiveness of combat troops in stability operations. To fight this type of battle, troops will need to be armed with proper training and tools to operate in this role. Traditional operating procedures, while effective for certain aspects of a counterinsurgency, will need to be bolstered by new techniques, technology, and tactics.

This paper is an evaluation of the efficacy of one such tool, a layered, relational database system, previously used in a domestic law enforcement setting, for use in counterinsurgency operations in Iraq. Qualitative analysis of both the domestic program, known as Citizen and Law Enforcement Analysis and Reporting (CLEAR),
and limited uses of related systems in counterinsurgency operations is balanced against the requirements of intelligence systems in US counterinsurgency doctrine and practice.

The second section of this thesis is dedicated to the methodology used to research these systems, and data caveats. The third section of the paper will establish the environment counterinsurgents will use the CLEAR-like system in by briefly describing the framework of the insurgency in Iraq and counterinsurgency intelligence needs and policing tactics of coalition troops. The fourth section will provide an in depth look at the development of key components of the CLEAR system as used by the Chicago Police Department (CPD) it every day law enforcement activities. The fifth section will then explore the use of similar relational database systems in the Iraqi theater, and in domestic testing for deployment to Iraq. Evaluation of these programs will be based on counterinsurgency intelligence requirements and law enforcement best-practice standards. The paper will conclude with a summary evaluation of the usefulness of the tools being employed and the policy implications associated with such a system.

Though the CLEAR system is not designed for military use, it is my contention that, if modified for the specific needs of troops undertaking a counterinsurgency
strategy, police innovation/incident reporting systems like CLEAR will benefit the military in Iraq.
Chapter 2. Methodology and Data Caveats

A case study methodology will be used for this paper using cases in domestic law enforcement and military applications of CLEAR-like database systems. The implementation of CLEAR in Chicago beginning in 2001 and continuing to 2007\(^1\) will serve as the baseline of what a fully engaged, robust version of CLEAR contains and is capable of achieving in combating criminal activity.

The majority of the descriptive information on CLEAR was obtained from a series of reports written by The Chicago Community Policing Evaluation Consortium, which is a joint program formed by researchers at Northwestern University and the University of Illinois at Chicago. Survey data collected by the Consortium outlining the volume of use and perceived effectiveness was used for a limited quantitative analysis of certain measures of effectiveness. To qualitatively evaluate the effectiveness of the system I compared the functionality of the system to measurements of effectiveness laid out by the CPD and the US Department of Justice (DOJ) Office of Community Oriented Policing Services (COPS).

While these data do give a robust view of the capabilities of CLEAR in the Chicago metropolitan area, a comparative study of its use in other locales is not

\(^1\) This time frame was chosen for two reasons. First, the best data available on the use of the system comes from a series of reports, the last of which was written in 2007. Second, development of the military systems occurred within this timeframe.
available. Though other agencies within the state of Illinois have utilized aspects of CLEAR, there are little data of use to compare to the case in Chicago.

Three scenarios in which CLEAR-like systems were used by the military in counterinsurgency operations were also examined: 1) A full implementation across a Marine battalion in Western Anbar Province, Iraq was tested from March to October of 2006; 2) An independent implementation by a military transition team in Khaladiya, Iraq beginning in January of 2007; 3) A test carried out by Special Operations forces at Camp Roberts, CA from February 21 to March 6, 2007.

Though the users of the system vary from military to civilian law enforcement, the performance of the system should remain consistent. Therefore, the qualitative assessment of all the cases is based on the intelligence requirements set forth by the DoD in the Counterinsurgency Field Manual, as well as the US law enforcement best practice standards mentioned above.

Unfortunately, there are no data available of multiple case studies carried out in identical geographic locations over similar periods of time, and with a similar number of users. Soldiers and marines with knowledge of the US Army/Marine Counterinsurgency Filed Manual carried out all three military case studies, though. It can therefore be assumed that the scope of information they were gathering on the battle space was similar. Also, the two cases in Iraq both occurred in Anbar Province.
within six months of each other, meaning the local population and operating environment have similar characteristics.

While official military or proprietary commercial studies were not available for assessment, the secondary literature used in this thesis involves firsthand accounts by military officers that implemented the programs, as well as in-depth evaluations by military scholars such as James Russell. This data is sufficient for a thorough understanding of the systems in question.

In addition the case studies I present, I establish a framework for which the military versions of CLEAR will be used in by surveying secondary sources on insurgency and counterinsurgency theory. Using US military field manuals, and the works of scholars and practitioners such as David Kilcullen, John Nagl, and David Galula, standards for what information is necessary to carry out a counterinsurgency strategy, and how that information should be collected and utilized, are developed. It is from these sources that the intelligence requirements used to measure the effectiveness of the case studies is derived.
Chapter 3. Policing Operations for Counterinsurgency

This section will explore aspects of insurgencies and US counterinsurgency doctrine and practice that make law enforcement tactics, and therefore law enforcement technology, applicable to the counterinsurgency effort in Iraq. The first subsection will give an overview of counterinsurgency intelligence requirements as specified in US military doctrine and practice. I will then briefly discuss the applicability of the third generation gang (3G2) model to the Sunni-led insurgency in Iraq. (The 3G2 is characterized as a gang that has evolved politically and geographically, as well as in its sophistication of operations.) The final two subsections will then explain how US counterinsurgency efforts have evolved into police-like tactics and why law enforcement technology is essential to carrying out such a mission.

Intelligence in Counterinsurgency

In a population centric counterinsurgency strategy as the US is using in Iraq, intelligence plays a critical role in providing commanders with accurate and thorough knowledge of the battle space. While intelligence is critical in conventional maneuver warfare as well, the information that is necessary, how that information is collected, and the decision makers influenced by the information changes in counterinsurgency warfare. As a more horizontal command structure is employed in counterinsurgency,
direct access to intelligence is more critical at all levels, and information flows up and down the chain of command more readily.

In traditional warfare intelligence develops a picture of the battlefield by focusing on the military capabilities of an enemy, and intelligence drives operations.\(^2\) Counterinsurgency intelligence, however, must facilitate a different understanding of the operational environment. In addition, operations often are the catalyst for collecting intelligence. The U.S. Army/Marine Corps Counterinsurgency Field Manual establishes a distinct set of collection requirements to develop this understanding. Knowledge of the local populace to include culture, language, customs, and behavioral patterns must be gained. Information on the host nation, and the capabilities of friendly and hostile elements of the host government must be understood. And the nature of the insurgency, its localized nature, and the insurgents’ use of complex terrain must be recognized.\(^3\)

Intelligence collected on an insurgency and the environment it operates in can be useful in developing information structures that can help forecast how the insurgency may act, and react, based on the behavior of locals and host government institutions. Although the scope of information that is collectible in an environment

like Iraq is almost endless, specific data is essential for carrying out a counterinsurgency. US military doctrine highlights a number of specific collection targets important to counterinsurgency operations.

A thorough census serves as a starting point for gathering much of this information. In addition to this, further personal information, such as biometric data, other identifiable features, and vehicle ownership of targeted individuals is needed to begin discerning combatants from non-combatants.

Cultural data, both on individuals and groups can also help troops designate potential enemies within a community. Familial ties along with religious and economic affiliations can serve as possible predictors on what people and organizations may harbor anti-coalition sentiments.

Many of the activities undertaken by insurgent groups are merely criminal activities. The networks used to construct IEDs are such an enterprise. Tracking these

---

networks to find where the materials come from, who the technicians are, and where the users are trained is one important facet of counterinsurgency intelligence.⁷

Environmental data are also imperative. Intelligence on safe houses, hotspots, and possible targets of violent activity are fundamental in drawing conclusions about the capabilities and intentions of insurgent forces. To enhance the usefulness of this information, simple geographic data on the urban environment, such as street layouts, can be layered with the targeted data.⁸

US counterinsurgency doctrine recognizes that valuable intelligence is collected by patrol units that have regular contact with the local population. Many of the requirements given above can only be collected by soldiers in the field. Therefore, components at all echelons must work with the understanding that they should be prepared to collect intelligence through questioning individuals (Target Exploitation, or TAREX), as well as from exploiting documents that may be found in raids or

routine searches (DOCEX). In addition to collecting intelligence, these operational units require situational awareness on the environment they are engaged in.

Conventional warfare requires military intelligence assets provide intelligence preparation of the battlefield, orders of battle, and force templates. Counterinsurgency operations, however, require a more investigative intelligence function. Association matrixes, network analysis, traffic flow analysis, and event pattern analysis are important tools when forces attempt to gain battle space awareness when suppressing an insurgency and supporting a local population.

**Insurgencies and the Third Generation Gang Model**

Traditional counterinsurgency strategy calls for a strong police presence to protect the population, but the evolution of insurgencies in the “information age” has increased the need for a policing presence in counterinsurgency. As insurgencies have taken to a strategy of netwar many of these sub-state organizations have begun to

---


12 Netwar is a term developed by John Arquilla and David Ronfeldt, researchers from RAND. The term refers to a form of low-intensity conflict, wherein the combatants
resemble criminal gangs. Like street gangs, some insurgencies use violence to gain control over a vulnerable community in geographic area where state security services are weak. They then use an ongoing level of violence necessary to maintain protection of the territory from the state and other street-level competitors.13

The third generation gang (3G2) model developed by John P. Sullivan stems from the observation that as local gangs embrace netwar, they can develop into progressively more sophisticated entities with regional and global ties to other violent organizations. As they become more sophisticated, these gangs strive to not only protect their local “turf” and financial markets, but also attempt to further their political agenda through terrorism and quasi-terrorism. A fully evolved third generation gang will have matured from a street level gang, into a second-stage, financially conscious gang, and finally continued to transform into a fully developed netwar organization that can challenge the state.14

While some have depicted the Sunni-led insurgency in Iraq as a “discrete collection of actors motivated by a combination of nihilistic rage, primordial tribal
grievances, or a desire to restore the formal grandeur of the Ba’ath party,” it may prove more useful to conceptualize this insurgency using a gang model.\textsuperscript{15} Using the framework of the 3G2 model addresses the economic, political, and social relationships that are absent from the “tribal” depiction of the insurgency. Of particular interest to the applicability of policing tactics against the Iraqi insurgency are the netwar-like structure of insurgent groups and the relationship between insurgent groups and other street-level actors (i.e. other violent, non-state actors, the local population, and security forces). It is these attributes of the Sunni insurgency that make law enforcement tactics suitable as one tool in suppressing insurgent activity.

A weakened economy along with political and social strife led the formation of a number of local, street level protection groups in Iraq that began to engage in illicit and informal economies to fill the void left by the weakened state.\textsuperscript{16} Such groups were especially prominent in the heavily Sunni areas of Iraq – such as Anbar Province – where many feared oppression from the Shia majority and decreased access to already scarce resources. It is these groups that were responsible for the majority of coalition casualties in Anbar Province prior to the tribal awakening in 2006 and 2007.\textsuperscript{17}

\textsuperscript{17} Haussler, Nicholas I. “Third Generation Gangs Revisited: The Iraq Insurgency” (Masters Thesis, Naval Postgraduate School, September 2005) 50.
The loose affiliation of members of these groups, based on tribal and familial ties, led to a horizontal network structure similar to what would be seen in a typical street-level gang. Small cells of extended family are generally connected to similar cells within a larger tribal, geographic, or market-based relationship. Each of these cells retains a level of autonomy, but they work in conjunction with each other when it is beneficial.\textsuperscript{18}

Less directly involved in insurgent violence are more sophisticated national and transnational violent terrorist enterprises (VTEs). These organizations operate more like organized crime cartels, and consist of both Iraqis and foreign nationals. Such groups develop associations with local insurgent groups, who they mobilize to carry out their criminal enterprises and terrorist violence. This mercenary-like relationship between the two types of groups serves as a force multiplier for the VTEs.\textsuperscript{19} For instance, the strength of Abu Musab al-Zarqawi’s organization was its ability to mobilize semi-autonomous cells with only a loose affiliation to Zarqawi.


\textsuperscript{19} Haussler, Nicholas I. “Third Generation Gangs Revisited: The Iraq Insurgency” (Masters Thesis, Naval Postgraduate School, September 2005) 76.
The fluidity, horizontal structure, and geographic dispersion of “the” Sunni insurgency make establishing networks and patterns difficult for the counterinsurgent. Typical military intelligence operations are not generally set up to develop a nodal network pattern of the enemy. It is this dilemma that faces our troops in Iraq.

The Soldier as a Beat Cop

The asymmetric warfare that resembles gang warfare adopted by insurgents in Iraq, coupled with the intelligence requirements for a counterinsurgency campaign has led the US military to adopt some tactics that resemble a cop on the beat. As David Kilcullen points out, coalition forces and civilians have stepped into the void left by an unstable and weakened Iraqi security and governmental infrastructure, in an attempt to replace the criminal networks that have filled the same vacant space.²⁰

To help protect the local population, coalition troops have taken on the role of a police force in areas where the Iraqi police and military are not able to provide adequate security. Fighting the criminal and insurgent organizations that have developed since the initial US invasion requires “the use of complex police tactics,

special investigative techniques, and the recruitment of indigenous sources…“

that, until recently, US troops have not been trained to undertake.

Recent pre-deployment training protocols for US troops have begun to employ police training. Law enforcement experts have been hired on a contract basis to aid in training Marines in these tactics, and soldiers preparing for deployments have engaged in police ride-alongs to learn the skills used by street cops.

The law enforcement skills being taught to US troops is hoped to aid in meeting the intelligence requirements necessitated by the strategy being undertaken in Iraq. While a Marine may not previously be prepared to collect intelligence on a routine patrol, learning to question suspects and witnesses like a police officer may accustom him to do so. Additionally, troops are being instructed in proper techniques for establishing traffic checkpoints and recognizing deviations in traffic patterns. Such information, when compiled and analyzed, may help commanders at all echelons develop a more complete picture of the battlefield.

---

Requirements of a Law Enforcement Data System for COIN Intelligence

By looking at COIN operations as an evolution toward an urban, law enforcement model, requirements for a system that will aid COIN operators in data collection and exploitation can be established. Any system adopted by counterinsurgency forces needs to facilitate the collection, analysis, exploitation, and sharing of information at all echelons. To do this, the system must be deployable with tactical units, yet robust enough to provide adequate information to analysts at the battalion\textsuperscript{24} level and above.

To be deployable with tactical units, a data collection system must be portable. This requires a lightweight unit that takes up little space and is compatible with current hardware used in mobile units, such as Humvee-mounted IT systems.\textsuperscript{25} Additionally, the data collection unit must be able to sustain activity over long periods of time. This requires a battery with a long life that is able to operate in extreme temperatures.

\textsuperscript{24} A battalion contains between 300 and 1000 soldiers or Marines and is commanded by a Lieutenant Colonel. Battalions are capable of independent operations of limited duration and scope. The US Army chain of command above a battalion consists of brigade, division, corps, and army components, while the USMC consists of regiment, division, and Marine Corps components. Below the battalion level are companies, platoons and squads (and in the USMC teams are the sub-unit of squads).

\textsuperscript{25} High Mobility Multipurpose Wheeled Vehicles (HMMWV or Humvee) serve as one of the main troop transport systems in the Iraq theater. Other troop transport vehicles house IT systems, as well, including Mine Resistant Ambush Protected (MRAP) vehicles.
Finally, the system must be easy to operate. Training time on individual systems is limited, and often soldiers may be asked to learn the system in theater. While the portable element of a data collection system must have a small footprint and be user friendly, the entire system must be robust enough to house enormous amounts of data. As outlined above, the intelligence requirements for counterinsurgency forces are vast. Data on individuals, groups, equipment, and incidents must be gathered and stored. FM 3-24 recognizes the importance of housing such data and calls for the use of vast databases to assist in capturing intelligence.\textsuperscript{26} Beyond being just a depository of information, though, the software included in the system must have relational capability to aid in the building of networks and models in terms of demographics, terrain, infrastructure, and insurgent incidents.

\textbf{Summary}

The adoption of a new field manual for counterinsurgency operations demonstrates that the US military is evolving to combat a new type of enemy. Doctrinal changes such as this have a wide reach, and US troops are being called on to perform new types of duties and communicate within a changing chain-of-command structure. As soldiers and Marines are asked to perform policing functions against

criminal organizations, the DoD will hopefully continue to develop tools, such as integrated database systems, to allow the job to be performed effectively.
Chapter 4. The Citizen and Law Enforcement Analysis and Reporting System

For the purpose of this paper, CLEAR will be defined as a system of interrelated databases and the affiliated technologies used by the Chicago Police Department (CPD) to further enhance and make more efficient its policing practices. This section will give a detailed description of the how the program began, as well as key hardware and software used in the system and what types of police officers and civilians use them.

Community Policing, Police Innovation, and the Development of CLEAR

The era of community policing began to take shape in the 1970’s when public dissatisfaction with police was high. The goal of this initiative was to not only reconnect police officers with the public, but also to improve upon police performance through innovation in techniques and technology. In 1994 the DOJ implemented the Office of Community Policing Services (COPS), which invested money in research for time saving technologies that would help improve community policing initiatives at the local level.27

---

CLEAR was conceived as part of the movement towards enhanced community policing and an expanded use of technology within the CPD. In 1993 CPD Superintendent Matt Rodriguez took lead a program entitled “Together We Can,” a system-wide overhaul of the CPD that included improving relationships with the community and local businesses and implementing technological advances to “support a new, proactive approach to preventing crimes before the occur.”

As part of this program, CPD partnered with Oracle in 1996 to develop the Criminal History Record Information System (CHRIS). CHRIS was the first stage in developing an integrated information system and data warehouse, which made Oracle the logical partner for the CPD to approach for enhancing CHRIS from a database system to a fully integrated enterprise system.

The CPD approached Oracle in 2001 with a proposal for why the partnership would be mutually beneficial. In this meeting, CPD demonstrated the market value of CLEAR to Oracle by demonstrating multi-city interest by getting the Washington, DC Metropolitan Police Department (MPD) to show interest in the program. The pitch

---

28 Daly, Richard M., Mayor of the City of Chicago, “Together We Can” (Chicago, 1993).
was successful in bringing Oracle on board. CPD also secured $35 million in Oracle funding for the project.\textsuperscript{31} In addition to the Oracle investment, an additional $9 million was received from the USDOJ Office of Community Oriented Policing Services (COPS) and private grants were received from outside organizations bringing total initial investment to over $40 million.\textsuperscript{32} CPD began retooling the CHRIS data warehouse in 2000, and Oracle took over the project once the contract was settled.

**Key Applications**

CLEAR consists of a series of interrelated applications that work in concert to collect data and produce police reports. Below is a description of a number of the key applications at the heart of CLEAR.

**Database Warehouse**

The integrated database warehouse is the heart of the CLEAR system. The original database was loaded with 14 years of information that had been compiled in CHRIS. It also serves to compile information from the numerous reporting


applications outlined below, as well as allowing officers to produce a variety of relational reports using “modern, flexible database-query software” by giving officers access to vast repositories of centralized relational data. Officers are able to utilize a series of analytical modules that draw on the data that is stored in the central warehouse to produce these reports.

**Automated Incident Reporting Application**

The Automated Incident Reporting Application (AIRA) is one of the main data entry points for the CLEAR system. It allows officers to fill out automated case reports at the time of an incident using either a portable data terminal (PDT) that is housed in a police cruiser or a LAN-based terminal in the police station. This would replace a slow and inefficient paper-based reporting system. Both systems required not only extensive development of software that could be integrated with the data warehouse, but also the purchasing and updating of hardware, IT infrastructure, and CPD facilities.

---

The mobile implementation of AIRA experienced a number of difficulties when it was first being developed. Both the mobile and LAN-based systems ran on the Police Computer Aided Dispatch system (PCAD) – CPD’s automated dispatch system – and therefore were reliant on that software. The original user interface was far from user friendly, especially on the PDT’s. To remedy this, a Windows-like screen was developed to give the officers a familiar interface to work on. In addition to this, the PCAD software was enhanced to allow officers use one-button options to replace reporting items that had to previously be typed out. Also, communication between PDT’s was improved with an email-based car-to-car messaging system that could store up to 100 messages. A function that allowed storage of dispatch address histories for up to 90 days was also included. Finally, ergonomically awkward stations were updated with touch screens to allow for easier manipulation by officers with larger fingers.\(^{35}\)

Another key problem faced by the mobile system was that the available bandwidth at the outset of the program was low, resulting in slow processing times. The legacy PCAD system ran on a radio-based modem. As one officer explained, “Home dialup modems are 56K. What we’re dealing with is only 9K and the pipe is

Cellular technology was attempted in a pilot program, but deemed too insecure for use with sensitive reporting. The bandwidth problem was eventually solved to a certain degree by installing standalone radio-based modems in each squad car.37

The LAN-based system faced challenges in its implementation, as well. The same software and interface issues came up, and were solved in much the same way. The familiar Windows-like screen was brought online, and more ergonomic workstations were installed. Almost one-third of CPD’s stations did not contain sufficient IT infrastructure for a widespread, online application, though. As these stations were brought online, major infrastructure upgrades were needed.38

The issues outlined above, while significant, proved to be fixable in a domestic law enforcement setting. When looking to apply an electronic incident reporting system to a forward deployed position, though, some of the obstacles may prove more difficult to overcome.

When the AIRA program began, CPD outlined four goals for the system: 1) improve reporting accuracy; 2) improve the quality and completeness of reporting; 3) provide follow-up investigators with timely and complete information; and 4) allow AIRA to interface with other CLEAR applications.

Pilot testing in 2004 showed that AIRA increased reporting of incidents by gang and tactical officers, who generally enter the majority of data at the precinct. By 2007, though, many of the same challenges with performance that plagued AIRA early on were still present. The CPD contemplated replacing the system, but no data suggests a reasonable alternative was developed.

**Automated Arrest**

The Automated Arrest system is another automated data entry application that allows officers to replace a legacy paper-based system with a fully electronic system that can be accessed at terminals throughout the CPD. With this application, an arresting officer is able to enter data about a suspect while in an interview room. The data they enter then interface with digital mug shots and the automated fingerprint

---

identification system (AFIS) to provide a complete workup on the perpetrator. Once the data is entered, desk sergeants and watch officers can approve bookings and releases online. Additional data on a detainee can be entered as they are moved, receive visitors, or are interviewed further by follow up investigators. The information is also made available to prosecutors for pre-trial reports.41

As with AIRA, the Automated Arrest system required an update to stationhouses to install the system. Again, wiring issues were prevalent, but the main obstacle was the procurement of the proper hardware and furniture to house the system. Rugged laptops were needed, and they had to be bolted down to tables, as the stations are located in the interview room with the prisoner.42

Unlike with AIRA, by the end of 2006 the Automated Arrest system was functioning smoothly in station houses. Officers reported that the system sped up the booking process and the system was being used on a regular basis by large numbers of police personnel.43

e Track

E Track is the automated evidence tracking system embedded in CLEAR. As with other data entry applications for CLEAR, e Track replaces an outdated paper system with a streamlined electronic one. The main goal of e Track is to provide electronic tracking for chain of evidence and evidence inventory reporting. It is faster, more accurate, and eliminates the legibility issues associated with a paper tracking system.\textsuperscript{44}

E Track also allows forensic units to electronically store data and produce reports based on the collected evidence. Electronic crime scene processing, digital crime scene photos, DUI kits, and seized gun information can all be uploaded, integrated, and processed, producing automated, relational reports. Additionally, a document scanning application allows for the uploading and storage of ancillary documents.\textsuperscript{45}

COPLINK

COPLINK is an algorithmic software solution that is used to identify associations between objects of interest.\(^{46}\) COPLINK was originally developed by the University of Arizona’s Artificial Intelligence Lab in conjunction with the Tucson Police Department and the Phoenix Police Department with funding from the National Institute of Justice.\(^{47}\) The CPD added COPLINK to the suite of CLEAR solutions in 2007 to enhance the analytic capability of the system.\(^{48}\)

COPLINK adds considerable associative power to the CLEAR system, as it is able to “reach” into multiple databases and draw connections between multiple objects (people, incidents, etc). Five categories of objects are used by the COPLINK structure: person, location, organization, vehicle, and crime. By automatically searching through structured objects in databases, and unstructured information in crime reports, the analysis system is able to associate across and within categories, as well as provide visual mapping of locations. Pattern recognition is also provided by temporal


relationships. Finally, by weighting relationships through the number of connections, COPLINK is able to demonstrate how strongly objects are connected.\textsuperscript{49}

COPLINK has proven successful in domestic law enforcement deployments. Even in its early versions at the Tucson Police Department, 86\% of searches were completed with useable results within three seconds.\textsuperscript{50} An additional benefit of the system is that officers are able to use it with little training, and a significant number of officers in the pilot group were able to fully utilize the search and analysis functions with no training at all.\textsuperscript{51}

**Personnel Suite**

A final application worth noting for its effectiveness in streamlining human resource management is the Personnel Suite. This application allows HR to maintain more complete personnel files, lets officers complete many of their own personnel related tasks, and gives management the ability to monitor behavior and review

performance.\textsuperscript{52} For the purpose of this study, though, we will not explore this application further, as its usefulness specifically in COIN operations is not applicable.

**Evaluation of Effectiveness**

By 2007 the Chicago Community Policing Evaluation Consortium, a group whose research was done in conjunction with COPS, considered the overall CLEAR program’s development rather successful. Surveying of Chicago police officers showed unequivocal acceptance of CLEAR automation and a perceived positive impact on overall policing quality due to automation. Ninety-two percent of all officers queried responded that CLEAR allowed them to work more effectively, made police work more efficient, and improved information quality. Additionally, 84 percent of officers surveyed believed that CLEAR has improved information sharing among the CPD.\textsuperscript{53}

By far, the strongest, and most used, application CLEAR offered was the database warehouse. Eighty-two percent of surveyed officers reported accessing information from the warehouse at least several times a week, with 60 percent using it


on a daily basis. Clearly, this tool gave large numbers of officers access to vast amounts of information.

In addition to receiving high marks from the Consortium, CLEAR appears to meet most of the military standards addressed in Chapter 3 of this paper. Reporting hardware was very mobile, though the communications system it utilizes needs improvement. The PDT’s housed in police cruisers would function well in a military vehicle, though a more portable, handheld unit is needed too. The database warehouse has proven to be a powerful tool for gathering large amounts of easy-to-access information, and COPLINK enhances the analytic capability of CLEAR users. Finally, most users were easily trained on all of the equipment. Training for AIRA and the Automated Arrest system consists of one day of classroom work each.

The entire evaluation of CLEAR was not positive, though. Forty-seven percent of the survey respondents found many of the applications to require redundant data entry. Further, certain applications that began as a strong concept fell short in

---

implementation.\textsuperscript{56} By 2007, mobile AIRA was still experiencing many of the same difficulties designers faced early on.

To further study the true effectiveness of CLEAR, the impact such a system has on the reduction of crime in Chicago needs to be measured. At this time, there are no solid data that represent a causational relationship between the implementation of CLEAR and reduced crime rates in the Chicago metropolitan area.

The CPD has made a commendable effort to become an information-driven organization, and though implementation of the CLEAR system has not reached its full capability, it has proven to be an effective tool to help police officers perform their duties. Key applications have been widely adopted and efficiencies in incident reporting and network pattern analysis have been achieved. It is these successes that make CLEAR an attractive option for a starting point to build a counterinsurgency database system.

Chapter 5. Law Enforcement Data Systems in Counterinsurgency

This section contains case studies of CLEAR-like data integration systems that have been deployed in Iraq or have been tested for deployment to Iraq. First, though, an explanation of legacy systems that have been in use by the DoD are studied to demonstrate what shortcomings they possess and establish what a new system must be capable of to be of added value to military forces in Iraq.

Legacy Systems: BAT and ABIS

The Biometric Automated Toolset (BAT) is a database system originally developed for use in the correction system in Iraq. The system collects and stores biometric data to include fingerprints, retinal scans, and digital photographs, and it can be used to scan ID cards. While the system is able to gather detailed information about individuals, it is not very mobile, and is limited to on-base and static checkpoint applications. Additionally, the system is unable to communicate with other military database systems.

The development of a new criminal information database for use by the US military dates back to 2004 when the DoD Biometrics Management Office contracted with Lockheed Martin to develop an Automated Biometric Identification System (ABIS) based on the successful Lockheed IAFIS used by the FBI.\textsuperscript{60} The contract called for the development of the hardware and software needed to capture biometric information, store it, and allow for the information to be passed back and forth between troops, allowing them to identify known or suspected insurgents.\textsuperscript{61} The Lockheed biometric deal was a five-year contract with an automated fingerprint system to be first developed. Expansion to include facial recognition and other biometric data was also planned. BAT has not been made available at the squad and checkpoint level, though. While information can be entered and stored at a FOB, many soldiers who are interacting with the local population on a regular basis do not have access to the system.

**Case 1: Operation Snake Eater**

In 2006, USMC Maj. Owen West was stationed near Khalidiya, a village of roughly 10,000 in Anbar province northwest of Baghdad. Maj. West was in charge of

---


the joint Marine/Army Military Transition Team (MTT), tasked with training and supervising the Iraqi Army’s 3rd Battalion, 3rd Brigade, 1st Division (3/3-1, also known as the Snake Eaters, resulting in the name of the program). The 3/3-1’s area of operations was a hotbed of insurgent activity in 2006, with Maj. West calling it “the center of gravity for the Fallujah-Ramadi corridor.” The area served as a transit space for foreign and Al Qaeda fighters, who accounted for the majority of the insurgent activity in the region during Maj. West’s tour.

Maj. West was seeing a large number of suspected insurgents released shortly after having been detained by US or Iraqi forces. To track suspected insurgents and detained individuals, Major West developed a system of spreadsheets and power point programs to capture names, addresses, and incidents. He then uploaded pictures taken

---

with digital cameras for additional biometric data. He did not, however, have access to an Iraq-wide, or even region-wide, database. Maj. West saw the 3/3-1 becoming the police in the area and believed his MTT and the Iraqis needed to be armed with up-to-date police technology.

With the BAT system not available to him, and his own makeshift system not sufficient, Maj. West turned to Goldman Sachs – his full time employer and the NGO Spirit of America for help. With funding from both organizations, a biometric data system was developed in conjunction with Computer Deductions, Inc. The system was developed from December 15, 2006 to January 15, 2007, allowing Maj. West a short window of opportunity to engage it before being redeployed stateside.

Biometric data was captured using the MV-100, which combines a fingerprint scanner, digital camera, and magnetic card reader in an integrated PDA. The data packet is then transmitted via Bluetooth to rugged laptops housed in Humvees. There,

67 Maj. West is a reservist in the USMC. He is employed as an energy trader at Goldman Sachs, and is a graduate of Harvard College and Stanford Business School. This was his second tour in Iraq.
COPLINK software analyzes the data and produces incident mapping in the same way it does in a law enforcement system in the US.\textsuperscript{70}

Though Maj. West’s experience with Operation Snake Eater was short-lived, he believed the system gave the MTT and Iraqi troops a decided advantage in information collection. After only one night of using the MV-100 and laptop system, Maj. West declared, “I think we have a chance to tip this city over now.”\textsuperscript{71} The MV-100 proved portable over the duration of a normal patrol, and MTT and 3/3-1 were able to use the equipment within a day of receiving it without training.

West’s troops were able to gather biometric data on a large number of individuals, and though this limited system does not have the capability to gather diverse types of information, it is useful for obtaining personal data on individuals. No attempt was made to integrate this data with upper echelons, but it can be assumed, based on the below studies, that with the proper software this could have been achieved.

**Case 2: The Camp Roberts Test**

Following Maj. West’s implementation of the Snake Eater program, the DoD ran a four-day field-test of another CLEAR-like system, almost identical to the one

\begin{flushleft}
\textsuperscript{70} Henninger, Daniel, “The Snake Eater: Give our troops the tools our cops have,” *The Wall Street Journal* (February 8, 2007).
\textsuperscript{71} Henninger, Daniel, “The Snake Eater: Give our troops the tools our cops have,” *The Wall Street Journal* (February 8, 2007).
\end{flushleft}
used in Snake Eater, using special operations personnel at Camp Roberts, CA. Similar hardware and software as to what Maj. West had available was used, including the MV-100 PDA and a layered database system that included COPLINK. In addition to these components, the soldiers carrying out the test were able to link the collected data to a simulated ABIS database.

Multiple simulations were run, including a medical scenario and a full red-blue force simulation. The main test, though, was the use of the system by soldiers manning checkpoints. In this simulation, soldiers either ran a Fast ID or a Full Encounter ID – the same options available to Maj. West. In both scenarios, soldiers took fingerprints and digital photographs and compared them against a limited data set stored on the PDA. If no match was found, the information was relayed through a laptop in a Humvee and sent to the Tactical Operations Center (TOC). A laptop at the TOC simulated a server level system in which data on the local population resided. The information was then sent to an ABIS simulator in the FBI’s Clarksburg, WV biometrics center.

---

The MV-100 and laptop system employed in the Camp Roberts scenario was nearly identical to that used in Operation Snake Eater, and provided similar data capture capabilities. Additionally, the ID matching that was performed between the two pieces of hardware yielded near-instantaneous feedback. Furthermore, with COPLINK serving as a bridge the local databases were connected to upper echelon systems, allowing real-time ID matching with simulated global databases.\textsuperscript{74}

As with Operation Snake Eater, though, the shortcoming of this system is that it only allows for intelligence on individuals to be collected and communicated. There was no capability to input environmental or incident-related information. Also, other than ID matching, there was no analytic capability embedded in the system.

**Case 3: Al Qaim and Project METRO**

Like Khalidiya, western Anbar and the area surrounding Al Qaim was a nest of insurgent activity in the early stages of Operation Iraqi Freedom. The insurgency in this part of Iraq was a combination of Al Qaeda in Iraq (AQI), other foreign fighters, and local militias. For a while, there was a coalition of sorts formed by the local Sunni population and AQI, but by mid-2005 many of the local tribes began to resist AQI and

\textsuperscript{74} The longest response time between the PDA and other databases was 3 minutes 35 seconds. Keegan, Matt, Giles Kyser, and Samuel A. Musa, “Applying Law Enforcement Technology to Counterinsurgency Operations,” *Joint Force Quarterly* (Issue 46, Summer 2007) 38.
assist US troops. The “tribal awakening,” as it would become known, began to spread throughout Anbar in 2006 and 2007.\textsuperscript{75}

The Al Qaim deployment of COIN Surveillance serves as the most comprehensive rollout of a CLEAR-like system by the military in Iraq, utilizing the tools from the Snake Eater project and Camp Roberts, and adding robustness with additional CLEAR-like applications and hardware. Termed Project METRO (Mobile Embedded Target and Reconnaissance Operation), this endeavor was the culmination of a US$2.5 million Lockheed Martin contract with the DoD.\textsuperscript{76} Marines of the 1\textsuperscript{st} Battalion 7\textsuperscript{th} Regiment, under the command of Lt. Col. Nick Marano deployed to Al Qaim armed with a CLEAR-like system to help in their counterinsurgency effort.

As in Operation Snake Eater and the Camp Roberts test, Project METRO involved supplying US troops – in this case a Marine battalion – with biometric collection hardware and information - storing PDA’s.\textsuperscript{77} Integrated, layered databases, based on CLEAR, were used, and analytic tools including COPLINK and a hot spot mapping feature, were embedded.\textsuperscript{78} Another feature that surpassed the previous two

test cases was the inclusion of a vehicle checkpoint and tracking system, which could link vehicles to individuals and incidents.\textsuperscript{79}

Not all intelligence collection for the system was manual, either. Lockheed supplied the Marines with additional, automated overt and covert sensors. Surveillance cameras were placed at known IED hotspots to alert troops of activity, and acoustic sensors were set up outside known safe houses and possible insurgent meeting areas. While much of the data were used for real-time surveillance, it was also captured digitally and stored in the databases for future analysis.

Not all of the information used was collected by the new manual or automated sensors. Census data that were gathered previously was uploaded, as well. Unlike prior operations, though, the census data were fed into COPLINK and integrated with the new incoming intelligence. The integrated information was then analyzed to develop linkages and patterns.\textsuperscript{80}

A human capital investment was also made in Project METRO. At the start of the implementation, the S-2 component of the 1-7 contained 4-6 analysts. Over the coming months, that number was increased to 30, greatly enhancing the battalion’s

human analytic capabilities.\textsuperscript{81} US law enforcement personnel were also employed to train the Marines of the 1-7 on the equipment, as well as in various law enforcement techniques.\textsuperscript{82}

Project METRO proved to be a successful implementation of a counterinsurgency intelligence system. The COPLINK database was fused together with surveillance and data collection hardware and the police training the Marines of the 1-7 received. This system, though deployed prior to the release of FM 3-24, incorporated much of what is now military doctrine.

Foot patrols similar to those used by law enforcement undertaken by the Marines, combined with the data capture technology they possessed led to an unprecedented amount of intelligence collection by roving units. These units were also able to gather cultural data on the region by having regular contacts with the locals. A flexible battalion command allowed for free flow of information up and down the chain of command, giving all echelons fast and easy access to all the information that was processed.

The use of CLEAR-like technology enhanced the effectiveness of this operation. A data warehouse was filled with thorough census data from the area


\textsuperscript{82} Hilburn, Matt, “Policing the Insurgents,” \textit{Sea Power} (March 2006).
of operation. Along with biometric and census data on individuals, vehicle registrations were housed in this database as well. This robust data set allowed the Marines to crosscheck information throughout their deployment.\textsuperscript{83}

While it was noted that not all of the technology employed in Project METRO worked as well as hoped, the suite of collection sensors coupled with the COPLINK system reduced the production time of target packages from several hours to several minutes. The analytic products that were included in these packages included incident matrixes and network analysis that helped decrease the level of IED attacks in hotspots.\textsuperscript{84}

The sensors proved to meet the needs of the Marines by being portable with a long battery life. The hardware and software systems used by patrols were interoperable with those at other points in the chain of command, allowing for communication and feedback across multiple echelons.

Though Project METRO was the earliest field deployment of a CLEAR-like system, it was the most robust. It allowed the Marines to collect “data on a


systematic basis to build structural awareness,”85 as opposed to information being collected in stovepipes and not flowing throughout the organization. While a number of applications involved in this project did not meet expectations, the key components helped establish a model that was followed closely in similar projects.

<table>
<thead>
<tr>
<th>Case</th>
<th>Hardware</th>
<th>Databases/Software</th>
<th>Intelligence Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Snake Eater</td>
<td>MV-100 PDA</td>
<td>COPLINK</td>
<td>Performed by Maj. Owen and his limited staff using COPLINK and data collected</td>
</tr>
<tr>
<td></td>
<td>MV-100 PDA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Humvee mounted laptop system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOC-based PCU unit with associated databases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camp Roberts</td>
<td>MV-100 PDA</td>
<td>COPLINK</td>
<td>Almost entirely automated. Verification and crosschecking of ID done by layered databases.</td>
</tr>
<tr>
<td></td>
<td>Humvee mounted laptop system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOC-based PCU unit with associated databases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Al Qaim (Project METRO)</td>
<td>MV-100 PDA</td>
<td>COPLINK</td>
<td>Combination of human and automated analysis. An increased S2 component utilized automated pattern recognition software to analyze raw intelligence</td>
</tr>
<tr>
<td></td>
<td>Humvee mounted laptop system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Surveillance cameras</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Acoustic Sensors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Additional overt and covert sensors</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 1** – A sampling of the hardware, software and analytic methods used in each case study demonstrates an evolution of the automated data integration projects carried out by DoD in Iraq.
Chapter 6. Conclusions and Policy Implications

Implementations of CLEAR-like systems have been limited to rollouts with individual military components. While CLEAR has been expanded to allow access to other police forces throughout the state of Illinois and Midwest region, but it is unlikely the military will share the same ease of success with expanding the program. As with all other intelligence and information systems, the US will likely experience difficulties in having different branches of the military communicate with each other. A trial in Joint Task Forces (JTF’s) and among different service branches must be conducted before the true effectiveness of such programs can be evaluated.

Additional information-sharing issues are sure to arise when interfacing with foreign coalition partners. We have seen difficulties with inter-departmental communication in the use of BAT and other proprietary, sensitive, or classified systems. Difficulties are sure to arise when deciding which of our partners should have access to the CLEAR-like system, and once they are deemed worthy, setting up systems that will talk to each other will form a further obstacle.

Ideally, US and coalition forces would be able to train Iraqi security forces on the technology they use, and leave it behind for use in maintaining stability after they withdraw. Unfortunately, while the ISF proved capable with the technology used in the above case studies, Iraqi law enforcement has been slow to adopt information
technology solutions for use in criminal investigations. Anecdotally, in the criminal justice facilities I visited in the Baghdad area, use of computers was almost universally dismissed. More than one Iraqi investigator mused that they had not turned on the computer on their desk since the Americans had given it to him or her.

Additionally, there is an ethical question about whether we should give such a tool to the Iraqi security forces. The Iraqi police and military have already shown a tendency to target individuals for violence and oppression based on ethnic and religious affiliation without access to large amounts of personal data on individuals. We must therefore question whether it is wise to provide these same entities with technological solutions that could further promote these types of activities.

What the case studies above have demonstrated, though, is that an enterprise system that can be accessed throughout the theater at levels ranging from squads to headquarters is needed to form an integrated common operational picture of the battle space. The CLEAR system, as implemented by the police in Chicago, has helped metropolitan police fight violent and gang-related crime, especially in high crime areas.

---

86 The author spent over a year in Iraq from 2006 to 2007 working for the US Department of Justice, first with the Regime Crimes Liaison’s Office, then the Office of the Justice Attaché. In both positions, he worked closely with Iraqi counterparts to improve the rule of law in Iraq. Frequent visits were made to various criminal justice facilities throughout the Baghdad area, including the Central Criminal Court of Iraq (CCCI) and the offices of the Iraqi High Tribunal (IHT).
volume areas. By using similar technology, and tailoring it to meet specific military and counterinsurgency needs, the US military would benefit from such a system.
References


