Intelligence Operations in U.S. Organized Crime Rings

Jacob Knox
Campbell University
Buies Creek, NC 27506
jtknox0104@email.campbell.edu

Abstract

In the United States, law enforcement agencies (LEAs) collect intelligence on organized crime rings (OCRs) to determine the best way to contend with the threat of OCRs. While LEAs intelligence collection methods are commonly known, the methods and sources of OCRs are often overlooked. This paper's focus is to discuss intelligence methods OCRs use against LEAs and the shortcomings in each method. All organizations collect and use intelligence for some reason or another. Due to certain constraints, OCRs are limited in their ability to effectively collect certain types of intelligence such as SIGINT and IMINT and almost incapable of collecting MASINT and GEOINT. Additionally, OCRs use all types of intelligence for specific functions within the crime ring. Within the United States, certain measures will need to be taken to counter act intelligence operations conducted by organized crime rings.

Key Words: Organized Crime Rings, Criminal Intelligence Collection, Counter Intelligence, SIGINT, IMINT, HUMINT, MASINT, GEOINT, OSINT

Introduction

During the 2014 United States (U.S.) intelligence community's worldwide threat assessment, James Clapper (Director of U.S. National Intelligence) listed transnational organized crime as one of the U.S. intelligence community's top ten threats (Clapper, 2014). While the term transnational implies multiple nations involved in certain criminal activities, one does not have to look past U.S. borders to find organized crime rings that are threatening to the U.S. intelligence community (Ibid). Crime rings may have certain shortcomings that would hinder their intelligence operations, but organized crime rings (OCRs) still employ all intelligence methods that law enforcement agencies (LEAs) execute.

Before one can study or observe how crime rings conduct intelligence operations, one must first understand why crime rings are a threat to all levels of U.S. infrastructure. Organized crime is defined by the Federal Bureau of Investigation as:

> …any group having some manner of a formalized structure and whose primary objective is to obtain money through illegal activities. Such groups maintain their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion, and generally have a significant impact on the people in their locales, region, or the country as a whole (FBI, 2013).

Looking at the definition, it quickly becomes apparent that the activities of organized crime rings can cause damage at all levels. Damage is caused by the root of their actions, which

is to obtain money through any means possible (Ibid). These means include violence, coercion, sabotage, and even collecting intelligence on anyone posing a hindrance to OCR operations.

Before one can study or observe intelligence methods used by LEAs or OCRs, one must first understand what intelligence is. Martin Bimfort defines intelligence as:

> … the collecting and processing of… information… which is needed by a government for its foreign policy and for national security, the conduct of non-attributable activities abroad to facilitate the implementation of foreign policy, and the protection of both process and product, as well as persons and organizations concerned with these, against unauthorized disclosure (Bimfort, 1995).

There are two things to note about intelligence. First, there is always a customer for intelligence (Ibid). In the example above, it is possible to replace the term "government" with "crime ring" or "law enforcement agency" and change all following terms to match the context. Additionally, intelligence must be collected and processed. Law enforcement agencies regularly collect intelligence from all sources using all methods. Crime rings, however, are limited in their ability to use intelligence methods to the same capacity as LEAs.

Limitations on Crime Ring Intelligence Operations

An intelligence source simply tells the source of the intelligence. There are six common sources of intelligence, which are signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), human source intelligence (HUMINT), open source intelligence (OSINT), and geospatial intelligence (GEOINT) (ODNI, 2014). SIGINT is intelligence that is gathered through intercepted signals (be it communication, data, radar, etc.) (Ibid). IMINT is intelligence comprised of an image (including satellite imagery, drone/aircraft imagery, thermal imagery, radar imagery, etc.) (Ibid). MASINT focuses on data signatures and characteristics of a given piece of information (Ibid). HUMINT is intelligence that focuses on the interpersonal dynamics of personnel (Ibid). OSINT is intelligence that is collected through open sources such as newspapers, scholarly articles, etc (Ibid). GEOINT is intelligence that is gathered through geospatial assets (Ibid). All six of these intelligence sources are used in some way, shape, or form by personnel concerned with U.S. national security.

OCRs use many of the same sources as LEAs and U.S. security personnel. One such example is that of Scarpelli in the 1980s with the crime ring known as The Outfit (Lombardo, 2012). Scarpelli was responsible for overseeing warehouses, accounts, and book makers (Idib). Scarpelli was also responsible for seeking out people that might have been hindering The Outfit's operations (Ibid). He would use HUMINT (by leveraging personal networks), SIGINT (by tracking electronic accounts), and OSINT (by checking open networks) so The Outfit would stay competitive (Ibid).

On the other hand, OCRs suffer from intelligence limitations for two reasons; feasibility and budget. Look at IMINT for example. Many high gain IMINT resources require special access and a large budget. It is estimated that it costs the U.S. somewhere between $55 million to $90 million U.S. to put a new terminal satellite (which is crucial for IMINT and SIGINT operations) into orbit (Magnuson, 2014). In 2012, a simple unmanned aerial vehicle (UAV) with forward looking infrared (FLIR) capabilities (which is essential for IMINT operations) was

estimated to cost between $25 million to $100 million U.S. (Boyle, 2012). Italian-American mafia Camorra is estimated to have made $4.9 billion from fiscal year 2013 to 2014 (Matthews, 2014). Someone could point out that the OCR has enough money to purchase military grade intelligence systems, but money must first go to other places. All OCR revenue is highly budgeted. OCRs rarely budget enough revenue to purchase high grade intelligence systems. The issue of feasibility still stands. Most providers of intelligence systems conduct extensive background checks on interested personnel. While it is possible, it is highly infeasible that it would happen.

Certain sources are not impacted by these limitations. OCRs can execute HUMINT and OSINT to the same capacity as LEAs. HUMINT and OSINT do not depend on technological abilities, but IMINT, SIGINT, MASINT, and GEOINT, are critically dependent on technology. Due to the technological nature of these four sources, OCRs do not operate to the fullest potential capacity. This idea raises a substantial question. To what extent to OCRs use different intelligence sources?

Crime Ring Use of SIGINT

As stated earlier, SIGINT is an intelligence source that focuses on intercepted signals (ODNI, 2014). OCRs collect SIGINT through telecommunications collection and digital collection. Phone taps are simply devices that collect telecommunication transactions from a phone. There are two common types of phone taps, tethered and wireless. A simple tethered phone tap that is plugged into the telephone system can be purchased for approximately $80 U.S. (B&H Photo and Video, 2014).

A plethora of malicious software is available for use on smart phones that collect telecommunications traffic. It was estimated in the third quarter of 2013 that approximately 204 million of all new smart phones shipped were Android based smart phones (Whitney, 2013). On 27 September 2014, chief executive officer for InvoCode Pvt Ltd was arrested by the FBI for the, "… conspiracy and sale of a surreptitious interception device… [that] could intercept communications to and from mobile phones and was marketed as largely undetectable and untraceable…" (FBI, 2014). A program with these capabilities would be beneficial for an OCR in gathering intelligence against any agency that might harm a crime ring's operations.

Past telecommunications digital intelligence is a substantial source of information for any interested party. Digital communication is essential for success in any organization. Due to its rising essentiality, interception and collection of digital communications is a great source of intelligence. Two methods for collecting digital communication are hardware collection and software collection.

Hardware collection is physically taking hard resources (such as computers, phones, media players, cameras, networking gear, etc) and collecting any useful information from the digital device (Perry, 2009). Hardware collection is a difficult and time consuming way of collecting intelligence due to its highly technical and specialized nature. There are few reported instances of OCRs employing this method, but it is still highly effective. A thug merely has to steal a laptop, phone, thumb drive, radio, or other piece of electronic gear and analyze it for useful information. Some may argue that most law enforcement equipment is encrypted or protected, but it is possible to bypass most protective measures with a basic technical knowledge or software.

One such example is the theft of personal data from an insecure Veteran's Affairs (VA) computer in 2006. An unencrypted VA computer containing the personal information of approximately 26.5 million veterans and veterans' families was stolen from the home of a VA employee (EPIC, 2006). It was estimated that no one was personally impacted by the data lost, but the information would have been invaluable for an OCR intelligence operations (Ibid).

Instances of hardware collection are few and far between, but software collection is much more prevalent. Software collection on digital resources can be done a multitude of ways. The most dangerous method toward LEAs is similar to that used on wireless communications; a virus. Malicious software, or malware, can be installed onto a workstation to monitor communication or data and send that information to third party for analysis.

Another effective method is to hack a LEA work station. One example is a large scale hack launched against LEAs in 2011. A group of hackers stole approximately 10 gigabytes worth of personal information from more than 70 LEAs and posted the information publicly (Millis, 2011). Those responsible for the data leak were brought to justice, but the incident brings to light the seriousness of digital assets.

As serious as these instances seem, OCRs are limited in their ability to employ SIGINT for a few reasons. The technical skill and experience to collect and analyze SIGINT is astounding. Second, it is difficult to acquire the resources necessary to accomplish these tasks. Many high end software packages for decryption, hacking, or surveillance are strictly controlled and are difficult to obtain. Lastly, many digital assets have counter measures put in place. Network security engineers' sole purpose is to protect digital assets from individuals interested in breaching digital assets.

Crime Ring Use of IMINT

As stated earlier, IMINT is any form of intelligence that depends on an image for intel (ODNI, 2014). These images include radar images, thermal images, and standard camera based images (ie, satellite, drone, or human based photography) (Ibid). OCRs are limited on radar and satellite based imagery but are capable of drone and human based photography.

Unmanned Aerial Vehicles (UAVs), or drones, are defined by the U.S. Department of Defense (DoD) as, "… powered, aerial vehicles that do not carry a human operator, use aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload…" (Bone & Bolkcom, 2003). DoD application of drones are much different than that of an OCR, but the principle is the same. As the definition states, a drone "can carry a lethal or nonlethal payload…" (Ibid). The nonlethal payload of a drone could be an imagery pod capable of infrared or standard imagery capabilities. In the United Kingdom, criminals are reported using commercially purchased drones with infrared capabilities to locate marijuana farms and steal the crops (Withnall, 2014). Drones with these capabilities cost approximately $2,000 U.S. for the drone and 5745 euros for the camera system, totaling approximately $10,000 U.S. (Drone Jungle, 2014 & Steadi Drone, 2014).

OCRs have endless uses for a drone system like the one listed above. These applications are not limited to peer-to-peer operations, but could also be used against LEAs. Scott Stewart, VP of Tactical Analysis for STRATFOR, discusses in his article "Recognizing Criminal Surveillance" a cycle in which criminals conduct surveillance on a target before acting upon their target (Stewart, 2014). Criminals heavily rely on having eyes on a target before executing an

operation (Ibid). A drone could be used to assist with the surveillance component of an operation.

Human based photography is not as effective as satellite or drone based photography, but is still a valuable source of IMINT for any organization. Human based photography relies on someone collecting IMINT through the use of a hand held camera. Due to the close nature of human based photography, its applications are limited and narrow. Most human photography operations require an individual to be very close to the object of interest, creating a situation where the risk of obtaining a useful picture is not worth the cost of failing.

Crime Ring Use of Other MASINT and GEOINT

As stated earlier, MASINT is measurement and signature intelligence and GEOINT is geospatial intelligence (ODNI, 2014). MASINT focuses on the signatures and characteristics of a given piece of information and GEOINT is any intelligence gained through geospatial assets (Ibid). MASINT and GEOINT are shrouded in a cloud of secrecy due to their technical and dangerous nature. Due to the high cost and exclusivity of these two INTs, OCRs can only use them in a highly limited capacity, although it is more common that then cannot use them at all.

What would it look like if OCRs could use these assets? If an organization had information regarding the specific signature of a radio transmission (an application of MASINT) they could block or sabotage the signal. One step further, if an organization has information about the signature of a city's power source (another application of MASINT) they could bring a town/city/district/state/nation to its knees by crippling the power grid. Furthermore, if an OCR had access to GEOINT resources, they could use IMINT and SIGINT to the same level as military and government agencies. This would result in more damage than could be effectively explained. Not only would OCRs have the resources they needed to collect intelligence against LEAs, but they would also have the necessary resources to protect their information against LEAs. The end result would be OCRs operating at a military level.

OCR Use of OSINT and HUMINT

OCR use of OSINT and HUMINT is very similar to that of LEAs. OSINT is open source intelligence that focuses on collecting information from open sources such as press releases, news broad casts, scholarly publications, and any information posted in an open arena (ODNI, 2014). A strong example of OSINT is this paper. All information in this paper was taken from public domain, making it an assimilation of open source information. Information such as L.E.A. locations, work forces, ethics, equipment, areas of operation, organizational structure, and even phone numbers can be found using simple OSINT search techniques.

OSINT can provide a lot of information, but there are two things to recognize about OSINT. Information obtained by OSINT is not always accurate. Many organizations recognize that OSINT is a productive intel method, therefore counter measures are put in place to protect sensitive information. Additionally, OSINT by itself is not very useful. OSINT can support other intelligence operations in giving an organization direction or in edifying information, but can rarely provide enough information to make a sound operational decision.

HUMINT is human intelligence, or intelligence that was gained through interpersonal interaction (ODNI, 2014). HUMINT could be information obtained by listening to a law enforcement officer discussing operational plans or capturing a law enforcement member and

interrogating him/her for valuable information. HUMINT is a source that produces some of the most valuable information. Due to the interpersonal nature of HUMINT, OCRs use it almost identically as law enforcement organizations. OCRs collect HUMINT through covert actions (under cover informants), simple collection (having a collector observe people), and counter actions (baiting and observing the reaction), just as LEAs conduct HUMINT operations.

Conclusion

In summary, organized crime rings are capable of executing many of the same intelligence techniques as law enforcement agencies with the exception of a few resource intensive methods. OCRs are limited in SIGINT, IMINT, MASINT, and GEOINT due to the price and exclusivity of these sources whereas they are highly capable of executing HUMINT and OSINT operations.

OCR SIGINT operations include but are not limited to observing telecommunications traffic and collecting digital intelligence from LEAs. When observing telecommunications traffic, OCRs are capable of intercepting tethered communications through the use of a wire tap and wireless communications through the use of malicious software. When collecting digital intelligence, digital intelligence falls into the category of hardware collection and software collection. Hardware collection is when an individual removes a physical component of a digital device and extracts useful information from it. Software collection is when an individual either hacks or uses malicious software to break into someone's computer and steal their information.

IMINT operations include drone and human operations. Drone operations require a UAV equipped with an imagery pod (normal or thermal) which the OCR uses to collect an image of an area. Human operations require a person on the ground taking pictures of an item of interest. There are no recorded instances of OCRs using MASINT or GEOINT, but it could be detrimental if an OCR executed either. Finally, OCRs are highly capable of executing OSINT and HUMINT to the same capacity as LEAs.

When looking at the entire intelligence situation with OCRs, it becomes apparent that OCR capabilities are a national threat to LEAs. In order to remedy this threat, LEAs should increase counter intelligence operations, have measures in place to intercept possible OCR collection, and insure all personnel are educated in proper operational security (OPSEC) procedures. According to the Office of the National Counter Intelligence Executive, the spirit of counter intelligence is to defensively protect an organization's information by offensively disrupting another organization's intelligence collection (ONCE, 2010). It could be argued that LEAs are already disrupting OCR intelligence collection, but more should be done in all areas to secure information. Whether it be closely controlling information which LEAs publish, encrypting digital work stations, or being aware of assets that could be observed, all essential areas should be more secure.

Beyond securing information, there is much to be said about intercepting criminals when they are trying to collect information. SIGINT assets could be secured by employing software countermeasures to intercept possible information breaches before they occur. Another strategy for interception is to correlate information and leverage the correlation to better focus intelligence operations for the LEA. The possibilities for interception are endless, but it is undisputed that more measures should be in place.

Counter intelligence operations and intercepting criminal collection are two excellent ways of hindering OCR operations, but if there is no operational security protocol, no counter

operations will succeed. The U.S. Department of Defense Education Authority defines operations security (OPSEC) as, "the process by which we protect unclassified information that can be used against us…" (DoDEA, 2014). In essence, OPSEC is the practice of securing key operational details at all levels, be it interpersonal, digital, or hard resources such as paper (Ibid). Many LEAs have OPSEC practices, but there should be a drastic increase. Many people are familiar with the household saying, "loose lips sink ships…" In any organization, carelessness can lead to an operational downfall.

At the end of the day, understanding how OCRs conduct intelligence operations is important because with an understanding of what they are doing, it is very easy to disrupt their operations. In the article *Demystifying the Criminal Planning Cycle*, Scott Stewart brings to light a fundamental concept that many people miss (Stewart, 2014). Stewart asserts that if an individual or organization can disrupt the criminal cycle before an action is conducted, much damage can be avoided (Ibid). Understanding the ways OCRs operate allows LEAs to better disrupt OCR operations, thus better protecting and serving the population as a whole.

References

Bimfort, Martin. "A Definition of Intelligence." Central Intelligence Agency. September 18, 1995. Accessed November 3, 2014.

Bone, Elizabeth, and Christopher Bolkcom. Report for Congress; Unmanned Aerial Vehicles: Background and Issues for Congress. 2003.

Boyle, Ashley. "The US and Its UAVs: A Cost-Benefit Analysis." American Security Project. July 24, 2012. Accessed November 4, 2014.

Clapper, James R., *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence,* Washington: Office of the Director of National Intelligence, 2014

DoDEA. "Operations Security (OPSEC)." U.S. Department of Defense Education Activity. 2014. Accessed November 12, 2014.

EPIC. "Veterans Affairs Data Theft." Electronic Privacy Information Center. 2006. Accessed November 10, 2014.

FBI. "The Federal Bureau of Investigation: Organized Crime Glossary of Terms." The Federal Bureau of Investigation. 2013. Accessed November 3, 2014.

FBI. ”FBI Arrests StealthGenie Mobile Spyware App Maker, Disables Website." FBI. September 30, 2014. Accessed November 10, 2014.

"JK Audio CellTap - Wireless Phone Interface from Cellphone to Audio Input Devices." B&H Photo and Video. January 1, 2014. Accessed November 10, 2014.

Lombardo, Robert. Organized Crime in Chicago : Beyond the Mafia. Champaign: University of Illinois Press, 2012. 151-159.

Magnuson, Stew. "Military Wrestles with the High Cost of Satellite Terminals." National Defense Magazine, February 1, 2014.

Matthews, Chris. "Fortune 5: The Biggest Organized Crime Groups in the World." Fortune, September 14, 2014.

Millis, Elinor. "AntiSec Hackers Post Stolen Police Data as Revenge for Arrests." CNET, August 6, 2011.

ODNI. "ODNI FAQ: About the Intelligence Community." Office of the Director of National Intelligence. 2014. Accessed November 4, 2014.

ONCE. "What Is Counter Intelligence?" Office of the National Counterintelligence Executive. September 1, 2010. Accessed November 11, 2014.

Perry, William. Information Warfare: Assuring Digital Intelligence Collection. Hurlbert Field: JSOU Press, 2009. 4-8.

Stewart, Scott. "Demystifying the Criminal Planning Cycle." STRATFOR. April 3, 2014. Accessed November 12, 2014.

Stewart, Scott. "Recognizing Criminal Surveillance." STRATFOR. April 10, 2014. Accessed November 11, 2014.

"Tali H500 Drone." Drone Jungle. 2014. Accessed November 10, 2014. http://www.dronejungle.com/tali-h500-drone/.

"Thermal Imager Optris PI 400 Lightweight Kit." Steadi Drone. January 1, 2014. Accessed November 10, 2014. http://www.steadidrone.eu/product/optris-pi-400-lightweight-kit/.

Whitney, Lance. "Android Snags Record 81 Percent of Smartphone Market." CNET. October 31, 2013. Accessed November 10, 2014.

Withnall, Adam. "Criminals ‘Using Unmanned Drones and Infrared Cameras to Find Illegal Cannabis Farms’ – and Then Steal From the Growers." The Independent. April 17, 2014. Accessed November 10, 2014.