LEARNING LAW ENFORCEMENT INTELLIGENCE

Vaibhav Goutham Suresh
Amit Verma
Aaditya Arora

ALEXIS PRESS
JERSEY CITY, USA

LEARNING LAW
ENFORCEMENT INTELLIGENCE

LEARNING LAW ENFORCEMENT INTELLIGENCE

Vaibhav Goutham Suresh

Amit Verma

Aaditya Arora

ALEXIS PRESS

ALEXIS PRESS

Published by: Alexis Press, LLC, Jersey City, USA
www.alexispress.us

First Published 2022

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication Data

Includes bibliographical references and index.

Learning Law Enforcement Intelligence by *Vaibhav Goutham Suresh, Amit Verma, Aaditya Arora*

ISBN 978-1-64532-365-5

CONTENTS

CHAPTER 1

OVERVIEW OF LAW ENFORCEMENT INTELLIGENCE

Vaibhav Goutham Suresh, Assistant Professor, Department of General Management,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email Id- vaibhavsuresh@cms.ac.in

ABSTRACT:

Law enforcement intelligence is a critical tool used by law enforcement agencies to prevent and investigate criminal activity. It involves gathering, analyzing, and disseminating information about criminal activity and potential threats to public safety. This information is used to develop strategies and tactics to prevent crime, apprehend criminals, and ensure public safety. Law enforcement intelligence is collected from a variety of sources, including human intelligence, open-source intelligence, and technical intelligence. The information collected is analyzed by trained analysts who use specialized software and techniques to identify patterns, trends, and potential threats. This analysis is then shared with law enforcement agencies at the local, state and federal levels to aid in their investigations.

KEYWORDS:

Analysis, Collection, Crime Analysis, Criminal, Fusion Centers, ILP (Intelligence-Led Policing), Intelligence Function Operations.

INTRODUCTION

Current federal, state, municipal, and tribal programs aim to create a "culture of information sharing" to safeguard the United States against threats to our security and sovereignty.1 This is a major problem that requires the incorporation of new legislation, regulations, policies, practices, training, and organizational changes [1]–[3].

Five guiding concepts serve as the foundation of the National Strategy for Information Sharing:

1. Strong collaborations across federal, state, local, and tribal agencies, business sector groups, and our international partners and friends are essential for effective information sharing.
2. When coupled with information from apparently unrelated sources from other sources, in line with current legislation, information obtained for one purpose or under one set of authorities may provide new insights. In order to assist counterterrorism operations, we must consequently promote an awareness-based culture in which individuals at all levels of government stay aware of the roles and needs of others.
3. Information sharing has to be integrated into all facets of counterterrorism activity, such as proactive and defensive measures, actionable reactions, criminal and counterterrorism investigative operations, preparation for large-scale events, and the handling of their aftermath.

4. The policies, practices, and systems that facilitate information sharing must integrate and build upon current technological capabilities while adhering to established rules and obligations.
5. Fusion centers in states and large cities are an important resource for information sharing and should be included in the framework for national information sharing. Fusion centers will need to have a basic level of competence to collect, process, exchange, and use information as well as to conduct business in a way that respects people's right to privacy and other legal rights guaranteed by U.S. laws.

Every law enforcement agency in the United States, regardless of size, must be able to comprehend the consequences of information gathering, analysis, and sharing in order to create the culture of information sharing. Each agency needs a methodical way to gather and handle intelligence as well as a way to communicate with other law enforcement organizations and exchange crucial information. Additionally, it is crucial that law enforcement organizations establish channels of communication and information-sharing protocols with the private sector, especially with organizations connected to critical infrastructure as well as with private entities that could become targets of terrorist attacks and criminal activities [4].

Not all agencies have the personnel or funding to establish a formal intelligence section, and smaller organizations don't always need one. A law enforcement agency must be able to successfully consume the information and intelligence products supplied by a broad variety of entities at all levels of government, even without the presence of an intelligence section. State, local, and tribal law enforcement will be most successful when a single source, whether it be the Lansing Police Department's lone intelligence analyst, the Los Angeles Police Department's Terrorist Intelligence Unit, or the patrol sergeant who speaks the language of intelligence and is the information-sharing contact in the Mercedes Police Department, is the conduit of crucial information. No matter how big or how organized, every law enforcement agency has to be aware of its capacity for managing intelligence.

This paper articulates a standard knowledge of ideas, topics, and terminology for law enforcement intelligence and defines common language and methods for creating and deploying an intelligence capability in SLTLE agencies throughout the United States. Even though terrorism is the most ubiquitous concern, this Guide's coverage of intelligence is focused on "all crimes, all threats, and all hazards." As a result, the concepts of intelligence covered in this article also apply to all types of organized crime and business crime.

For instance, money laundering and drug trafficking continue to provide considerable challenges for law enforcement. Due to the high frequency of criminal incidences, SLTLE agencies are increasingly being asked to investigate transnational computer crime, including Internet fraud, identity theft cartels, and the worldwide black marketeering of stolen and counterfeit products. Similar to this, local law enforcement is becoming more involved in illegal immigration, human trafficking, and the often-linked crimes involving the falsification of identification papers including passports, visas, driver's licenses, social security cards, and credit cards. Even the trafficking of artwork and artifacts has grown, often introducing a new kind of criminal to the world of business crime. The use of intelligence to combat the ubiquitous violence in American communities has lately received significant attention. The continuance of previous organized crime operations like vehicle theft, cargo theft, and pretty much any other scheme that may generate revenue for an organized criminal enterprise all need cognitive capability for SLTLE.

The terminology used in the context of intelligence must be interpreted consistently by the law enforcement community if it is to be successful. Common standards, regulations, and procedures will also hasten intelligence sharing while safeguarding individual privacy rights and sustaining long-established community policing ties.

Perspective

Law enforcement personnel must first comprehend the meaning of law enforcement intelligence, how it differs from national security information, and the possible issues that might arise when the two forms of intelligence cross over. A law enforcement executive must comprehend what a "intelligence function" is and how various organizational structures might be used to carry out that role. Related executive choices, especially those made when there are financial constraints, center on personnel. Two additional intelligence roles that have developed complicate this mission: Information sharing with national security and homeland security partners as part of the Information Sharing Environment. establishing a capability for Homeland Security or "all-hazards" Intelligence.

Making ensuring that these new intelligence programs effectively respect everyone's civil rights and privacy is another significant and pervasive challenge. The Guide discusses important topics and fresh efforts for this duty, with one section dedicated only to this subject. These problems bring up a number of crucial questions, including: What kind of data are required by the federal government for the law enforcement agency to combat terrorism most successfully?How are those requirements decided? How is the data being asked for? Will the information be obtained when and how? Will reviewing the material requested by an executive need a security clearance? What other kinds of risks might a community face today? How are these dangers recognized?What risks fall under the "all-hazards" intelligence umbrella? What are the best resources and techniques for comprehending these dangers and gathering information that can be used? How can we include the public and commercial sectors in the gathering of intelligence? What restrictions apply to information gathering and sharing between law enforcement, the public, and business? The solutions are not simple, but they are doable.

What does "information sharing" entail in terms of policies and procedures? What kind of data may be gathered? What kinds of information are kept in criminal intelligence records systems? How long are the records allowed to be kept? When does a person cross the line from exercising their rights to endangering public safety? What tools are available to help an SLTLE agency achieve its intelligence objectives? How is it possible to incorporate the whole law enforcement organization into the intelligence function? The answers to these questions must be the result of written policy for a law enforcement agency to be successful.

DISCUSSION

The purpose of this text is to provide solutions to these problems, or at the very least options. Every law enforcement official must first acknowledge that sharing intelligence and information may be useful in thwarting terrorism and combating organized crime. But in order to accomplish these goals, law enforcement at all levels of government needs the following from the intelligence process:Redesigning a portion of the organization's structure and procedures to conform to national goals and national guidelines for best practices in law enforcement intelligence. Forming a common understanding of the terrorist or criminal danger. Establishing an agreement to take part in and act on danger information. Overcoming the conceptual

challenges that certain staff members have with intelligence methods. Directing a company's resources, time, and effort into its intelligence division. Establishing guidelines and procedures to safeguard people's civil rights and privacy.

taking use of and using modern technology, such as secure online communications and computerized information access. Using proactive individuals who are creative thinkers to determine "what we don't know" on terrorism and global organized crime. Requiring a law enforcement organization to behave locally while thinking internationally. Forming public-private collaborations in the field of intelligence.In the last four years, there has been an extraordinary level of change in the way law enforcement gathers information. From an operational, policy, and financial standpoint, the tasks and responsibilities for state, municipal, and tribal law enforcement are problematic. Despite these obstacles, thorough strategies and fresh tools are now at our disposal to safeguard our communities.

Concepts and Definitions of Modern Intelligence for Law Enforcement Organizations

In its most basic form, intelligence is the result of an analytical process that weighs data gathered from various sources, combines it with other pertinent data to form a logical package, and uses the scientific method to solve problems to come to a conclusion, estimate, or forecast about a criminal phenomenon. Therefore, intelligence is a synergistic product designed to provide law enforcement decision-makers significant and reliable actionable information about complex crime, criminal enterprises, criminal extremists, and terrorists.

The two main goals of the law enforcement intelligence function are as follows:

1. Developing or acquiring knowledge about potential terrorist or criminal threats, then utilizing it to track down criminals, fortify targets, and use countermeasures is known as prevention. There are two well recognized forms of intelligence that are particularly focused on prevention:

a. **Strategic Intelligence:**Actionable threat information is shared with a law enforcement agency's line functions in order to formulate and put into practice preventative and/or mitigating reaction plans and operations.

b. **Intelligence used Operationally:**Long-term threat information that may be utilized to create and put into practice preventative measures. Operational intelligence is most often employed for lengthy investigations into alleged illicit businesses and intricate multijurisdictional crime.

2. In order to develop response strategies and adjust resource allocations as needed to achieve effective prevention, planning and resource allocation inform decision-makers about the evolving threats, their characteristics and methodologies, and emerging threat idiosyncrasies.

The term "strategic intelligence" refers to this. It gives management of a law enforcement agency an evaluation of the evolving danger landscape for the aim of creating strategies and assigning resources to handle new threats. Even though information gathering and intelligence gathering are obviously connected to investigation1, the intelligence role is often more exploratory and widely oriented than a criminal investigation per se. A law enforcement organization could, for instance, have a solid suspicion that a person or group of persons has the motivation, capability, or determination to conduct a criminal or terrorist attack. Even in the case of an arrest for a criminal attempt or conspiracy, the evidence may not meet the required level of reasonable cause.

Additionally, there could be a strong cause for community safety to continue looking into potential weapons and other criminal offenders, particularly leaders.In order to discover and capture criminal criminals for prosecution in a criminal trial, "investigation" is defined as the pursuit of information based on leads and evidence related with a specifically specified illegal conduct.In the context of law enforcement intelligence, "information collection" refers to the gathering of information and data to ascertain if suspicious actions have a criminal relationship and/or to comprehend the workings of crime phenomena.This is not the only way to classify intelligence. One may think of "business intelligence," "geospatial intelligence," or "cyber intelligence," among others, to further categorize the field of intelligence. For instance, National Security Intelligence may be separated into "policy intelligence" and "military intelligence." The classification used above serves as the greatest example to highlight important ideas for the present topic.The term "law enforcement intelligence" is used by the author since "criminal intelligence" as it pertains to the criminal personality and the tendencies and processes by which criminals act is a topic of research in the area of criminal psychology.

Rigid rules must be observed due to this wider function, the need to protect information, and the need to retain records that identify people and organizations for whom there is uncertainty or tangential evidence of criminal involvement3. These rules are intended to protect people' constitutional rights while enabling law enforcement to conduct an investigation for the sake of public safety. Because threats from terrorism and organized crime are essentially cross-jurisdictional, the standards are also created to make it easier for law enforcement agencies to share accurate and secure information. In addition, if police enforcement organizations atInformation sharing may be more widely diffused when all levels of government adhere to the same rules since it is clear that the security and integrity of the data will stay intact no matter with whom the information is shared.

How to Define Intelligence

There are a lot of misunderstandings concerning the definition and use of "intelligence," both among the general public and inside law enforcement. Officer Jones gathered some solid intelligence, for example, but most usages of the phrase lack specificity and are unable to take into account the wide range of applications and norms connected with the intelligence function [5], [6].There are two major categories of intelligence. The "discipline" of intelligence, which is the first category, refers to the vocabulary, procedures, and norms that make up the intelligence function. This Intelligence Guide is dedicated to the study of intelligence alone. There are three categories of intelligence that are relevant for the current debate within the discipline: Criminal justice intelligence, "All-hazards" homeland security, intelligence, and three. spying on national security. These three groups have a lot in common, yet they are also quite different from one another. The precise relevance of these important elements to state, municipal, and tribal law enforcement organizations is covered throughout this Guide.

Various Intelligence Classes

The "application of intelligence," which deals with information pertaining to a certain crime type, is the second broad category. Using improvised explosive devices by jihadists as an example, intelligence analysis that uncovers information about new techniques and indicators in this area is called "application of intelligence." Another example would be indicators discovered through an examination of global financial transactions that are indicative of a money-laundering operation.

Understanding the nature and component parts of the relevant criminal phenomena is a necessary prerequisite for the use of intelligence. To effectively combat the crime issue, analysts and officers must have a thorough understanding of the gang culture, signs, symbols, hierarchy, and other gang-specific traits. As an illustration, if a community is threatened by multijurisdictional gang activity that functions as a criminal enterprise. Despite the fact that they are closely connected for the objectives of training and despite this, it is crucial to comprehend the specifics of any program.The definitions of each kind of intelligence will come into focus after the categories are understood.

Criminal Justice Intelligence

The definitions used in this guide are those that have been universally acknowledged as best practices and standards by the local, state, and tribal law enforcement intelligence communities. This is not to say that alternative definitions of terms are incorrect; rather, this method offers a shared understanding of terms and ideas that is most pertinent to the audience for this Guide.It is crucial to comprehend the definition of "information" in the context of this process before defining intelligence. Information is defined as "pieces of raw, unanalyzed data that identify persons, organizations, evidence, events, or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event."6 As will be seen, information is gathered as the currency that produces intelligence.

The term "law enforcement intelligence," which is used interchangeably with "criminal intelligence," refers to the duty of law enforcement to uphold the criminal code. The term is often misused, and too frequently, intelligence is mistakenly thought of as bits of knowledge about people, locations, or events that may be utilized to shed light on criminality or crime risks. It is made more difficult by the inability to differentiate between the many forms of intelligence.Information obtained from a variety of sources, including wiretaps, informants, financial records, or surveillance, is sometimes just raw data with a limited intrinsic value. When a variety of unprocessed data are examined for relevance to the problems at hand, validity, and dependability, and meaning is provided via the use of inductive reasoning, this is when intelligence is shown.

or inductive reasoning. Therefore, law enforcement intelligence is "the product of an analytical process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality."7 Because both policy and operational decisions are made using intelligence, it is imperative that carefully analyzed, reliable information be available. As a result, a vigilant process must be in place to ensure that decisions are made on objectivity.People who are unaware of the complexities and significance of the issue sometimes use "information sharing" and "intelligence sharing" interchangeably. Since there are different regulatory and legal implications for "intelligence" than for "information," care should be taken to use terms appropriately. As a result, the finer points of language can play a significant role in the management of a law enforcement agency's intelligence records.

Statements of ideologies, beliefs, and practices: A report by an analyst that makes judgments regarding a person's criminal responsibility based on a comprehensive study of various data gathered by researchers and/or investigators. An examination of crime or terrorism patterns with recommendations about the kind of criminals, likely future crimes, and potential countermeasures A prediction made concerning probable exposure to terrorism or crime based on

an evaluation of little facts when an analyst draws their conclusion from prior experience A projection of an individual's earnings from a criminal operation based on a market and trafficking study of illicit goods.

Concepts and Setting

State and local law enforcement have consistently stated that "analysis" is a necessary component of law enforcement intelligence before any information is referred to as "intelligence." For instance, the International Association of Chiefs of Police Criminal Intelligence Sharing plan funded by the Office of Community Oriented Policing Services states that: "intelligence is the combination of credible information with quality analysis information that has beenSimilar to this, the Global Intelligence Working Group, an Office of Justice Programs-funded project that is a part of the Global Justice Information Sharing Initiative, discusses law enforcement intelligence by noting: the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision-making at both the tactical and strategic levels.

The International Association of Law Enforcement Intelligence Analysts believes that intelligence is an analytical process: generating meaning from truth, adhering to a unifying vision. It involves using data gathered during an inquiry, from internal or external files, to arrive at something more than was previously obvious. This might include evidence in a case, a more accurate assessment of a crime issue, a projection of future crime rates, a theory about who could have committed a crime, or a plan to stop crime.The Commission on Accreditation for Law Enforcement Agencies attempts to give detailed advice on policies and procedures that promote effectiveness and liability protection on all facets of law enforcement tasks when developing standards for state, municipal, and tribal law enforcement. According to CALEA's requirements, intelligence is:An intelligence function should carry out a number of crucial tasks, such as a process that allows for the continuous flow of unprocessed data from all sources into a central location; a secure records system in which evaluated data are properly cross-referenced to reflect relationships and to ensure complete and quick retrieval; and an analysis system capable ofgenerating intelligence from the records system as well as from other data sources; a mechanism for distributing information to the right components.

The fact that information must be analyzed before it is classified as intelligence is evident not only from these discussions but also from the history of law enforcement intelligence from different national crime commissions looking into intelligence-related activities at the state and local level. It will demonstrate that there is a primary cause for this: laws governing state, municipal, and tribal intelligence data must fulfill evaluation criteria that do not apply to federal agencies. As a result, the analytical part of the definition is crucial.It's a common adage that every rule has an exception. This concept is supported by the notion of law enforcement intelligence. The FBI Directorate of Intelligence classifies intelligence in a particular way for practical reasons. As one FBI DI officer noted in a private interview:Information regarding people who would damage us via terrorist attacks or other crimes, including violent or property crimes, is important to law enforcement and national security. enables the creation of both "raw" and "finished" intelligence products.

Law enforcement executives need to be aware of the different roles and the different context when interpreting information. These differences are not in conflict; rather, they coexist to support the different missions and responsibilities of agencies at all levels o. Given the nature of

the FBI DI's responsibilities and the need to get the critical threat information into the hands of the law enforcement community quickly.Similar to this, the FBI and SLTLE need distinct approaches to the "Intelligence Cycle" because to differing intelligence demands.

The solution is straightforward: Those in charge of the intelligence function must be aware of these distinctions and implement techniques and policies that are best suitable for the various forms of intelligence being generated and absorbed [7].

CONCLUSION

In general, law enforcement agencies rely heavily on law enforcement intelligence as a tool to protect the public and deter crime. To keep ahead of changing criminal risks and safeguard communities all across the globe, this information must be developed and used continuously. The use of law enforcement intelligence has grown in significance over the last several years as criminal behavior has gotten more sophisticated and complicated. To stay ahead of these shifting dangers, law enforcement organizations must constantly modify and advance their approaches. This calls for a highly qualified staff with experience gathering, analyzing, and disseminating intelligence data.

REFERENCES

[1] G. Cascavilla, D. A. Tamburri, And W. J. Van Den Heuvel, “Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review,” *Computers And Security*. 2021. Doi: 10.1016/J.Cose.2021.102258.

[2] C. Cath, “Governing Artificial Intelligence: Ethical, Legal And Technical Opportunities And Challenges,” *Philosophical Transactions Of The Royal Society A: Mathematical, Physical And Engineering Sciences*. 2018. Doi: 10.1098/Rsta.2018.0080.

[3] K. Gradoń, “Crime In The Time Of The Plague: Fake News Pandemic And The Challenges To Law-Enforcement And Intelligence Community,” *Soc. Regist.*, 2020, Doi: 10.14746/Sr.2020.4.2.10.

[4] N. Petit, “Artificial Intelligence And Automated Law Enforcement: A Review Paper,” *Ssrn Electron. J.*, 2018, Doi: 10.2139/Ssrn.3145133.

[5] A. F. Rahmat And U. Pribadi, “Delivering Artificial Intelligence For Electronic Traffic Law Enforcement In Yogyakarta Region: Current Effort And Future Challenges,” In *Iop Conference Series: Earth And Environmental Science*, 2021. Doi: 10.1088/1755-1315/717/1/012016.

[6] C. Easttom, “Conducting Investigations On The Dark Web,” *J. Inf. Warf.*, 2018.

[7] P. Roffey And M. Gahan, “Responses To Security Sensitive Biological Agents (Ssba) Risks By The Australian Federal Police,” *Microbiol. Aust.*, 2020, Doi: 10.1071/Ma20034.

CHAPTER 2

HOMELAND SECURITY INTELLIGENCE

Dr. Xavier V.K., Professor, Department of General Management,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email Id-xavier_vk@cms.ac.in

ABSTRACT:

Homeland Security Intelligence is the collection, analysis, and dissemination of information used to protect the United States against terrorist threats, espionage, and other criminal activity that could harm its citizens, infrastructure, and institutions. It is a critical component of the U.S. national security strategy and is used to inform the development of policies, strategies, and operations to counter threats and prevent attacks. Homeland Security Intelligence is collected from a variety of sources, including human intelligence, signals intelligence, geospatial intelligence, and open-source intelligence. The information is analyzed by trained analysts who use specialized tools and techniques to identify potential threats and trends. This analysis is then shared with law enforcement agencies, government officials, and other stakeholders to inform decision-making and response efforts.

KEYWORDS:

Border Security, Counterterrorism, Critical Infrastructure Protection, Cybersecurity, Domestic Intelligence, Emergency Management.

INTRODUCTION

Despite being a relatively new term, "homeland security intelligence" incorporates long-standing law enforcement duties, most notably the "order maintenance" duty. The homeland security framework has given rise to these new intelligence obligations, which mandate that intelligence operations at the state, municipal, and tribal levels evaluate dangers presented by "all hazards." While there are clearly gray areas in this framework, it is crucial for law enforcement authorities to concentrate on dangers presented by hazards that have consequences for duties related to maintaining order and the safety of the public. Homeland security intelligence is defined by the author in this context as the gathering and analysis of data pertaining to noncriminal domestic threats to critical infrastructure, community health, and public safety with the aim of preventing the threat or lessening its effects [1]–[3].

For example, a law enforcement agency will be required in a public health emergency or a natural catastrophe to help preserve order and carry out activities to keep the public safe until the crisis is addressed. As a result of the catastrophe or disaster, community safety vulnerabilities may be discovered by homeland security intelligence, which may then be shared with law enforcement organizations so that the necessary safeguards may be put in place. And in still other situations, information may start out as homeland security intelligence before transitioning to law enforcement intelligence, like in the instance of a generic danger to vital infrastructure that transforms into a threat involving a specific person. If a person is linked to a danger to a vital

infrastructure, there is a good chance that a criminal nexus has developed, and law enforcement and homeland security intelligence inquiries may go forward together.

Because it is not exclusively criminal but addresses duties that law enforcement organizations must handle within their communities, this kind of information poses a number of difficulties. Despite the lack of precise legal or policy definitions, homeland security intelligence is becoming more common due to the influence of Department of Homeland Security duties, notably in the area of critical infrastructure.

As previously said, there may be instances when homeland security and law enforcement intelligence are combined. A real case study on a danger posed by zebra mussels that affects both homeland security and criminal activity is included at the end of this document as evidence. The case study's contribution is to demonstrate how law enforcement intelligence may be used to counter a non-traditional danger while simultaneously illustrating homeland security intelligence.

DISCUSSION

National Security Intelligence

SLTLE agencies may benefit from some national security intelligence perspective in order to comprehend the vast field of intelligence. This primer is not designed to be a thorough exposition; rather, it is aimed to acquaint the law enforcement reader with fundamental vocabulary, ideas, and problems.The definition of NSI is "the collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors as well as the maintenance of the United States' sovereign principles"15. NSI works to keep the United States as a free, capitalist republic with its laws and constitutional foundation unaltered and to recognize and counter threats or actions that could threaten this position [4], [5].Both policy intelligence and military intelligence are represented by NSI. Military intelligence concentrates on hostile entities, weapons systems, combat capabilities, and the order of battle, while policy intelligence is concerned with the threatening behaviors and activities of entities hostile to the United States. Military intelligence has developed to deal with the nature of new threats after the demise of the Soviet Union and the advent of threats from terrorist organizations. The Intelligence Community is the collective name for the entities in charge of NSI.

The IC is a confederation of 16 executive branch agencies and organizations that carry out threat assessment and intelligence activities necessary for successful international relations and the preservation of US national security within the scope of their individual missions as well as cooperatively. These include the following actions:gathering of data required for the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials to carry out their tasks and responsibilities, production and distribution of intelligence relevant to national security, as well as defense of American sovereignty against outside intervention. Gathering data on, and carrying out actions to prevent, intelligence activities targeted at the United States, international terrorist and international drug trafficking activities, and other hostile activities targeted at the United States by foreign powers, organizations, people, and their agents. The administrative and support tasks required to carry out approved operations, such as commerce, diplomacy, and the defense of our allies' interests, both domestically and internationally. Other intelligence gathering and actions that the President may order in connection with national security and relations between the United States and other countries.

The following organizations make up the 16-member IC:

1. Intelligence for the Air Force.
2. Defense Intelligence.
3. Agency for Central Intelligence.
4. Information from the Coast Guard.
5. Agency for Defense Intelligence.
6. Office of Energy.
7. Homeland Security Department.
8. Division of State.
9. The Treasury Department.
10. The Drug Enforcement Agency.
11. The Federal Bureau of Investigation.
12. Intelligence from the Marine Corps.
13. agency for national geospatial-intelligence.
14. Office of National Reconnaissance.
15. Agency for National Security.
16. Naval Intelligence.

There is no jurisdictional concern for crime, as can be observed from the definition and descriptions of NSI. Therefore, the constitutional limitations on information gathering, record keeping, and information usage in a raw capacity that apply to criminal cases that law enforcement encounters do not apply to IC duties when there is no criminal investigation.Although SLTLE agencies do not directly oversee NSI, this does not imply they will not come into contact with NSI or be assigned collecting responsibilities to assist NSI. Indeed, there is a good chance that SLTLE officers working on a Joint Terrorism Task Force may come into contact with or be exposed to NSI given that the Federal Bureau of Investigation is a member of the IC. Officers on an Organized Crime Drug Enforcement Task Force may also come across this information as the Drug Enforcement Administration is also a part of the IC. In both cases, the officers will normally have Top Secret or Secret security clearances, giving them access to papers that are classified and may provide more details about the material, including its source and method of gathering. However, it would be risky for SLTLE officers to utilize this data in a criminal investigation since there is a good chance that the procedures used to gather the NSI would not pass constitutional test in a court of law.

Even if it seems as if constitutional requirements may be satisfied, there are still additional possible issues with utilizing the data in a criminal investigation. A criminal defendant has the right to face his or her accusers; nevertheless, exercising this privilege may jeopardize confidential information and procedures. Although there is a method to deal with the procedure provided by the Classified Information Procedures Act, some view it to be inefficient and worry that it could cause more issues than are required.The topic of constitutional law is the following. Based on the "Fruits of the Poisonous Tree Doctrine," it is probable that any further evidence discovered during that inquiry would be covered by the Exclusionary Rule if the data was obtained through NSI sources in a way that violated the Constitution. As a result, the evidence would not be allowed.

The last worry with regard to state, municipal, and tribal authorities' access to NSI is liability. It is possible that the officer and the chain of command of that officer's agency could be held

accountable under 42 USC 1983, Civil Action for Deprivation of Civil Rights, if SLTLE officers used NSI that was gathered in a way that violated constitutional standards or if that information was kept as intelligence records that were under the custodianship of a state, local, or tribal law enforcement officer. According to this clause, as the majority of officers are fully aware, if a state or local cop abuses a person's civil rights while working in accordance with state law, the officer and those in his or her chain of command may be held liable in federal court. The relevant question is whether the officer is paid by and subject to the employment laws of his or her state or local employing authority, even if they may be serving on a federal task force under the direction of a federal official, such as an FBI Supervisory Special Agent.

Using the National Security Act of 1947, presidential Order 12333, a number of presidential orders, and U.S. The FBI is the leading organization for gathering domestic intelligence, according to Attorney General Guidelines. The difference between the ability of IC agencies to gather and store information and that of SLTLE agencies must be understood by SLTLE.The Information Sharing Environment established by the Intelligence Reform and Terrorism Prevention Act of 2004 presents a new problem. The ISE aims to disseminate all information on risks to the motherland, as will be covered in the following. The problem is exacerbated if SLTLE authorities gather or keep data on a danger to national security rather than criminal activity.The SLTLE agency' exclusive ability to handle intelligence matters stems from their legislative right to uphold the law. As a result, their procedures are subject to intense court examination and strict constitutional requirementsis gathered and stored in a system of criminal intelligence records. In contrast, the acquisition and storage of material by the IC is not subject to the same constitutional safeguards. These organizations have more freedom in the information they may collect as a consequence. The procedures for gathering domestic intelligence about dangers to national security are made even more difficult. The DHS, the FBI, and the NSA have the main duty for gathering domestic data for national security.DEA, which may gather information to be shared with SLTLE. SLTLE agencies, however, should rely on their relationship with the DHS, the FBI, and the DEA on matters of domestic intelligence, including when those matters involve international terrorism activity. U.S. foreign intelligence agencies, however, are prohibited from working with state and local law enforcement in a manner that could be interpreted as "tasking intelligence collection." Comparing the National Security Intelligence Authority with law enforcement to make sure that SLTLE agencies do not keep inaccurate information on people and organizations in their records system as a result of the ISE, effective policies and practices must be put in place and enforced. The on civil rights will go into more depth on these topics.

Three things may be gleaned from this short examination of national security intelligence:

1. Officers of state, municipal, and tribal law enforcement are not allowed to collect or handle NSI.
2. Due to civil rights safeguards, the use of NSI in a criminal investigation by a state, municipal, or tribal law enforcement official may prevent the prosecution of a case.
3. An SLTLE officer may be subject to civil liability from a 1983 lawsuit if they use NSI in a criminal investigation and/or keep it in their personal files or in a records system.

Homeland Security-Related Emerging Intelligence Initiatives/All-Hazards IntelligenceAlthough there are many potential operations that fall within the purview of homeland security

intelligence, the Fire Service Intelligence Enterprise and Public Health/Medical Intelligence are progressing more quickly than the others.

Enterprise Fire Service Intelligence

This statement from Fire Chief magazine, which is representative of the Fire Service Intelligence Enterprise, a new project that is still in its infancy:

Is there a place for the fire department—or emergency services in general—in the field of intelligence? Prior to September 11, 2001, this question probably would have never been posed, but it is being raised today. The answer is unquestionably affirmative, since firemen are often the first responders in the nation to terrorist attacks, natural catastrophes, workplace accidents, and other emergencies.Law enforcement does not respond with the same fervor when asked about the role played by the fire department in intelligence operations. Most of the time, this is due to uncertainty: law enforcement is unsure of the information types they may communicate with the fire service and if the fire service has any special responsibilities outside of the private sector.

The FSIE experimental project is the product of investigation. The idea is being further investigated based on a test program from the Fire Department of New York and combined efforts from the Intelligence & Analysis Directorate and the Federal Emergency Management Agency under DHS. Although not a nationally recognized entity or organization, the State and Local Program Office's guidance and assistance to the FDNY and FEMA's United States Fire Administration led to its foundation by state and local fire service leaders and industry organizations. A draft strategy for state and local fire services to exchange danger and associated information with the nation's almost 1.2 million firefighters and EMS clients was influenced by this connection. I&A continues to collaborate with the National Fire Academy in Emmitsburg, Maryland, and the US Fire Administration to integrate intelligence training into their curricula and make sure that our first responders have a better understanding of the circumstances surrounding or preceding their involvement in an incident.

The goal of FSIE is to provide a direct information channel between local law enforcement, DHS, and the fire department, primarily via a fusion center. In accordance with a National Response Plan instruction, the law enforcement organization would seek a direct information-sharing partnership with the fire department.According to the National Response Plan, federal coordinating structures, capacities, and resources must be coordinated into a single, cross-disciplinary, all-hazards strategy to domestic event management.

Situational awareness will be improved to assist the preparation efforts of both local fire departments and the DHS via the exchange of pre-event information and intelligence as well as real-time incident updates. Establishing a consistent operating picture at the local and national levels during a large disaster also depends on quick and thorough information exchange [6], [7].The FSIE idea has challenges since it primarily falls within the "all-hazards" paradigm of intelligence, where law enforcement is still trying to define and resolve its intelligence function. Furthermore, it is still challenging to come to a clear consensus on the problems of information sharing and civil rights.

Similar to how some firefighters are less than thrilled about being involved with the law enforcement intelligence role.The fusion idea and the all-hazards approach to intelligence must be combined, which necessitates a rigorous evaluation of operational procedures, accountability,

and roles. The FSIE's potential for success is still up in the air. The FSIE idea should be understood, however, and intelligence commanders and executives should consider if it has any place in the local law enforcement intelligence organization.

Protecting the public's health with Medical Intelligence

Threats to public health are becoming a larger part of homeland security intelligence's "all hazards" mission. Medical intelligence evaluates factors that may have an impact on a community's health, including trends, organizations, and associated events. The military has seen a tremendous increase in medical intelligence, which now has a wider emphasis and specifically looks at international medical trends. These websites provide comprehensive materials on medical intelligence:

1. The Military Intelligence Medical Center24
2. The collection on epidemiology in the WWW Virtual Library25
3. Database for Biodefense and Public Health26
4. The WONDER Database of Health and Risks from the Centers for Disease Control and Prevention.

The important details to remember are as follows:

1. Medical intelligence is increasingly being used as a tool to help safeguard our communities.
2. The all-hazards requirement will make medical intelligence an increasingly significant intelligence role.
3. Threats to the public health may be identified with the help of resources.

Intelligence on gangs

The application of existing legislation, regulation, policy, and practice for law enforcement intelligence is complicated by gang intelligence. Intelligence, as previously said, is the result of analysis; nevertheless, among individuals with expertise in gang investigations, the word "intelligence" is sometimes used more widely. Typically, "indicators" are used by gang experts.

Information concerning gang habits, gang signs and symbols, gang tactics, and trends in various gang activities, for instance, would fall under the category of intelligence. Frequently, a large portion of this data is not evaluated, or is processed but not in a sophisticated way comparable to the intelligence process. The acknowledgment of this reality is a practical component of the conversation, thus it will be utilized when talking about gang intelligence in the sense that gang investigators often use the word.

Analysis plays a crucial role when dealing with gangs, although less often than it should, gang data and information are subjected to analysis. This ought to improve as a consequence of the Global Intelligence Working Group's acceptance of the Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces28, as well as the increase of analytical competence inside law enforcement organizations, particularly via fusion centers.

The FBI provided the following details:

Gangs are more vicious, well-organized, and prevalent than ever before. There are 800,000 members in 30,000 gangs in the United States, which have an influence on 2,500 towns.In

addition to expanding to rural and suburban areas, Latino gangs are causing violence and crime in major cities like Los Angeles, Chicago, and New York.It is estimated that MS-13 has between 8,000 and 10,000 hard-core members and is becoming more sophisticated, widespread, and violent. MS-13 is primarily made up of immigrants from El Salvador, Honduras, and Guatemala and "has a significant presence in Northern Virginia, New York, California, Texas, as well as places as disparate and widespread as Oregon City, Oregon; and Omaha, Nebraska."

Information exchange and threat analysis are crucial since many criminal gangs are becoming to resemble trans-jurisdictional criminal businesses. When it comes to dealing with gang issues successfully, intelligence tools and resources may play a significant role.The application of existing legislation, regulation, policy, and practice to gang intelligence presents difficulties for law enforcement intelligence. The result of the analytical process is intelligence, as was previously said. However, "intelligence" in gang investigations is often seen in a broader sense, and generally includes data on gang activity, indications, modus operandi, and trends that are mostly obtained from raw material gathered from investigations rather than analysis. The minor difference between what gang investigators understand by "intelligence" and what members of the law enforcement intelligence community mean by the term should be acknowledged as a practical aspect of this topic.

How Do Gangs Work?

The first image that comes to mind when hearing the term "gang" is a group of young men who are generally active in "turf battles" in the inner city, spray-paint gang emblems on buildings, and engage in violent, sometimes fatal, altercations with other groups of young men. Usually, such image includes a representation of the well-known "Crips" and "Bloods" gangs from Los Angeles. Although there are gangs of this kind, gangs are considerably more widespread.

The distinction between gangs and organized crime may be hazy, as these categories show. Similar to this, it may be difficult to distinguish between terrorist groups and gangs since both often rely on intimidation and fear to further their objectives.While each state has its own legislative definitions of a gang, the majority follow a pattern like that of the National Crime Information Center's file on violent gangs and terrorist organizations. In accordance with VGTOF regulations, a gang member must fit at least two of the following descriptions.

a. Has been shown to be a member of a gang by a trustworthy source.
b. Has been identified as a member of a gang by a person of uncertain credibility, and that information has been strongly verified.
c. Has been seen by law enforcement to frequent the territory of a known gang, to associate with known gang members, and/or to adopt the dress code, tattoos, hand signals, or emblems of that gang.
d. Has a history of many arrests that are consistent with gang participation and involves known gang members.
e. Has acknowledged being a member of a gang at any point except their present arrest or imprisonment.

As can be shown, exchanging intelligence and information may be a valuable technique for identifying and categorizing individuals as gang members. This is especially significant given that gangs often cross jurisdictional boundaries. Law enforcement organizations may benefit from crucial information regarding gang threats and trends from both tactical and strategic

intelligence.The National Gang Intelligence Center and the Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces are two projects that have been created to improve the use of intelligence while addressing the gang issue.

Center for National Gang Intelligence

The National Gang Intelligence Center serves as a centralized intelligence resource for gang information and analytical support by integrating the gang intelligence assets of all Department of Justice agencies and forming partnerships with other federal, state, and local organizations that have gang-related information. This makes it possible for gang analysts and investigators tolinks between gangs and gang investigations, further identifying gangs and gang members, learning the full scope of their criminal activities and enterprises, figuring out which gangs pose the biggest threat to the US, identifying trends in gang activity and migration, and directing the appropriate officials in coordinating their investigations and prosecutions to disrupt and dismantle gangs. The goal of the NGIC is to assist law enforcement agencies by providing timely and accurate information exchange, as well as strategic and tactical analysis of federal, state, and local law enforcement intelligence, with a particular focus on gang growth, migration, criminal activity, and association that pose a serious threat to communities across the country.

The NGIC focuses on national gangs that exhibit criminal connectedness among groups with shared identities. The NGIC will also concentrate on a few regional-level gangs since many violent gangs do not operate on a national scale. The NGIC creates intelligence assessments, intelligence bulletins, joint agency intelligence products, and other nonstandard intelligence products for its clients in an effort to optimize efficacy.The Gang Guidelines, created by the Global Justice Information Sharing Initiative's Gang Intelligence Strategy Committee, aim to create an integrated strategy to deal with gangs by logically connecting task forces' operational and intelligence responses to gang threats. The Gang Guidelines emphasize the value of analysis when it comes to intelligence and suggest using the intelligence process to handle and evaluate unprocessed data. Similar to this, all gang intelligence programs should follow the National Criminal Intelligence Sharing Plan, according to the Gang Guidelines. Finally, by better guiding task forces' reactions to gang threats, the Gang Guidelines acknowledge the significant role that intelligence may play.Although the Gang Guidelines are new, having been adopted in late 2008, their broad adoption by law enforcement agencies, fusion centers, and gang task forces is likely as a result of its support by the Criminal Intelligence Coordinating Council [8]–[10].

CONCLUSION

All things considered, homeland security intelligence is a vital instrument for defending the US against terrorist threats and other criminal activities. To preserve the safety and security of the American people and to stop assaults on American soil, it is crucial to continue developing and using this information. The purpose of this was to provide the reader a better understanding of what intelligence is, how it differs from other forms of intelligence, what it does, and some of the issues that might arise when using the word. For instance, the FBI and DEA interpret law enforcement intelligence significantly differently than SLTLE agencies. The explanation for the discrepancy is based on the information sources the FBI and DEA utilized as well as the duties these federal law enforcement organizations bear for swiftly communicating distinctive essential information. The key idea is that the customer just has to be aware of the many definitions and contexts. With this information, information may be utilized and understood most efficiently.

REFERENCES

[1] D. C. Alexander and J. L. Johnson, "The Creation of a U.S. Homeland Security Intelligence Academy," *Journal of Applied Security Research*. 2009. doi: 10.1080/19361610903176336.

[2] H. M. Greenberg, "Is the department of homeland security an intelligence agency?," *Intell. Natl. Secur.*, 2009, doi: 10.1080/02684520902819644.

[3] J. Kim and W. M. (Bill) Allard, "Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Intelligence Analysis," *SAIS Rev. Int. Aff.*, 2008.

[4] D. E. Lambert, "Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter's Leading Change Model," *Crim. Justice Policy Rev.*, 2019, doi: 10.1177/0887403418786555.

[5] D. L. Carter and J. G. Carter, "Intelligence-led policing: Conceptual and functional considerations for public policy," *Crim. Justice Policy Rev.*, 2009, doi: 10.1177/0887403408327381.

[6] A. M. Randol, "Homeland security intelligence: Perceptions, statutory definitions and approaches," in *Focus on Terrorism*, 2010.

[7] N. Agarwala and R. D. Chaudhary, "Artificial Intelligence and International Security," in *International Political Economy Series*, 2021. doi: 10.1007/978-3-030-74420-5_11.

[8] L. M. Schaible and J. Sheffield, "Intelligence-led policing and change in state law enforcement agencies," *Policing*, 2012, doi: 10.1108/13639511211275643.

[9] C. Perrow, "The Disaster after 9 / 11□: The Department of Homeland Security and the Intelligence Reorganization," *Homel. Secur. Aff.*, 2006.

[10] M. W. Studeman, "Strengthening the shield: U.S. Homeland security intelligence," *Int. J. Intell. CounterIntelligence*, 2007, doi: 10.1080/08850600601079925.

CHAPTER 3

LAW ENFORCEMENT INTELLIGENCE: PAST PRACTICE AND RECOMMENDATIONS FOR CHANGE

Dr. Preetha Chandran, Associate Professor, Department of Finance,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email id- preetha.chandran@cms.ac.in

ABSTRACT:

Law enforcement intelligence has been an important tool in preventing and investigating criminal activity for many years. However, past practices have been criticized for their lack of transparency, accountability, and potential for abuse. Recent events, such as the 2020 protests and the use of intelligence to monitor peaceful protests, have highlighted the need for change in law enforcement intelligence practices. Recommendations for change in law enforcement intelligence include increased transparency and accountability, greater oversight, and improved training for intelligence personnel. The development of policies and procedures that ensure that intelligence activities are conducted in a lawful, ethical, and effective manner is also crucial.

KEYWORDS:

Fusion Centers, ILP (Intelligence-Led Policing), Intelligence, Lawful, Leader Commitment, Open-Source Intelligence (Osint).

INTRODUCTION

Law enforcement intelligence has been the subject of debates in the past because in certain cases, even when no crimes were being committed, the police kept records on people' activities that were seen as controversial, unconventional, suspicious, or perceived as anti-American. Of course, doing so offends the American sense of justice towards governmental intrusion and undermines key constitutional protections. Unfortunately, there is ambiguity in the border about the kinds of data that the police may gather and keep. It may be difficult to apply the law to real-world circumstances, and certain legal rules lack clarity. Law enforcement's early intelligence programs sometimes lacked a clear purpose and maintained a customary veil of secrecy, in addition to the potential legal repercussions. These past events may teach us valuable lessons that put today's law enforcement intelligence in perspective and give direction [1]–[3].

These concerns were made worse by the ambiguous connection between national security intelligence and law enforcement intelligence, which has altered continually since the middle of the 20th century. As these projects seek to adapt to shifting sociopolitical events in American history, most notably via post-9/11 counterterrorism operations, they have generated controversy on both the political and judicial fronts. To obtain context and comprehend the lessons learnt, it is useful to study certain periods of history from the perspectives of both forms of intelligence.

The Development of Law Enforcement Intelligence Over Time

Dossier systems were utilized by early law enforcement intelligence teams dating back to the 1920s. In essence, intelligence files were nothing more than dossiers files comprising a variety of raw data—about individuals who were deemed to be criminals, suspected to be associated with criminal activity, or those who were deemed to pose a danger to public safety and order. The usual types of people on whom police agencies-maintained dossiers included bootleggers during prohibition and many of the notorious criminals of the early 20th century, including Bonnie and Clyde, the Barker Gang, Machine Gun Kelly, and Al Capone.

Little was accomplished in the field of law enforcement intelligence during the 1930s slump. There were bigger priorities; the economy, not crime, posed the greatest danger to the nation. As communism—or the "Red Scare"—became prevalent in the latter half of the decade, circumstances started to alter. The dossier was the only system the police were familiar with.The House Committee on Un-American Activities' first chairman was American Representative Martin Dies in 1937. Dies, a supporter of the Ku Klux Klan, stoked fears of communism in the United States by branding individuals as being Communists if they seemed to be "un-American," which often led to their dismissal from their positions and functional exclusion from society. Though widespread, concern over communism was of secondary importance in the 1940s due to World War II. The Red Scare reappeared after the war, when the Soviet Union was created and its nuclear armament was established, and it did so with much more fury.

Senator Joseph McCarthy, who was utilizing this national issue as the cornerstone of his faltering reelection campaign to the Senate, considerably fueled the flames in 1950. McCarthy raged against the American Communist Party and demanded that everyone who was an outspoken Communist or Communist sympathizer be barred from employment in the government, the educational system, and the entertainment sector. The public's dread of the Soviet Union contributed to the war against communism's strong resonance.Local law enforcement agencies started compiling intelligence files, known as "Red Files," on people who were thought to be Communists and sympathizers in response to public and governmental statements of alarm. As a result, law enforcement organizations were collecting information on those who were expressing their political views and others who were known to be sympathetic to them. It was believed that the existence of and support for communism inside the country posed a danger to the national security of the United States, despite the fact that these individuals were just expressing their constitutional rights and had not broken any laws.

It was only natural for law enforcement to depend on this well-established system for gathering and preserving information when new major issues appeared since the dossier system had established itself as a reliable resource for law enforcement intelligence. The Civil Rights movement and the anti-Vietnam War movement were two obstacles for law enforcement in the 1960s, and intelligence dossiers seemed to be a useful tool in both cases. Participants in both situations seemed to be outside of society's norms.

They were outspoken about their opinions, and many saw their exhortations and behavior as being "un-American." Other societal factors made this worse: When the World War II baby boomers were in their teens and 20s, they were adding to the stereotype of the "long-haired, dope-smoking, commie-hippie spies"—a sure target for a traffic stop—by discovering their own newly defined world of "sex, drugs, and rock n' roll" and experimenting with it [4]–[6].

DISCUSSION

An overlap among these social movements was viewed by many as conspiratorial.Furthermore, the quickly shifting ideals, which were mostly stratified along racial and age lines, gave off a feeling of instability that threatened the majority. In retrospect, we know that it wasn't culturally us; it was just societal progress. Since there is a discord in theLaw enforcement agencies started compiling dossiers on activists and protestors in the 1960s under the largely unfounded assumption that many of them "might" commit crimes or "might" pose threats to our national securityinvestigate in the future. There is no question that law enforcement compiled and maintained these dossiers in an effort to safeguard the community from actions that were considered dangerous at the time, but good intentions do not excuse illegal actions.

Because of the U.S.'s activism at this time, there was further worry. Chief Justice Earl Warren's tenure on the Supreme Court. Regarding the current discussion, perhaps most significant was that the Warren Court led a generation of judicial activism and expanded interpretations of the Constitution, which led to many of the "liberal decisions" of the Warren Court being met with disapproval and the frequently expressed opinion that the Court's decisions2 were "handcuffing the police." Additionally, it served as a symbolic catalyst for activist lawyers of the 1960s to test out fresh approaches to the defense of constitutional rights. One of the more effective strategies was using a seldom utilized Civil Rights Act clause.Act of 1871, which became U.S. Code Title 42. Civil Action for Rights Deprivation under the 1983 Code.

This clause, which is sometimes referred to as "1983 suits," simply states that anybody who, acting in accordance with state or municipal law, deprives a person of rights protected by the U.S. Civil liability might apply to the US Constitution or federal law. The earliest legal disputes centered on whether a city, police force, and individual officers could be held liable for denying someone their constitutional rights. According to the Supreme Court, they could. The fact that the police may be sued for "misuse of power possessed by virtue of state law and made possible only because the wrongdoer is clothed with the authority of state law"3 was a major component of the case that opened the door for litigation against law enforcement.Initial legal actions centered on numerous patterns of bad behavior by police, including using excessive force and violating due process. With judgements stating that the police chain of command might be held vicariously accountable for the activities of people under their command as well as their parent jurisdiction, the scope of lawsuits against law enforcement expanded. Such litigation shifted targeting police enforcement intelligence groups in the late 1960s and early 1970s.

Law enforcement organizations were found to be maintaining intelligence files on individuals for whom there was no proof of criminal activity. It was determined that it was inappropriate to maintain intelligence dossiers on a contingency basis since it served no significant state purpose and violated the constitutional rights of those persons. As a consequence, courts often mandated that intelligence files be removed from police records, and in many instances, police agencies were required to compensate plaintiffs for damages. The rulings also made it possible for anyone to view their own records. Many activists made their intelligence files public as a badge of pride, often embarrassing the police.4 As a consequence of the humiliation and expenses related to these unsuccessful cases, law enforcement intelligence activities were drastically reduced or discontinued. The lessons from this period recommend care while creating intelligence records; data must be gathered, held onto, examined, and distributed in a way that is compliant with moral and legal requirements [7]–[9].

The Church Committee, which was named after its chairman, Frank Church, held in-depth hearings on domestic intelligence, most notably the Federal Bureau of Investigation's Counter Intelligence Program, which ran from 1959 to 1971, and its findings which are supported by the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities provide further insight into this lesson. The committee's judgment was thatAmerican freedoms of expression, association, and privacy are under assault and being compromised by domestic intelligence operations. The main reason it has done so is because the Constitution's method of preventing abuse of power has not been used.There was widespread worry over all facets of intelligence. The result of these several causes working together led to the U.S. Guidelines for the administration of criminal intelligence records kept by state and local law enforcement agencies were to be developed by the Department of Justice.

The criminal intelligence systems that are run by or on behalf of state and local law enforcement agencies and that are financed with federal monies are governed by the criminal intelligence systems operating policies that are codified as 28 CFR Part 237 Criminal Intelligence Systems Operating Policies8. The 1979 rule was born out of a change made to the 1968 Omnibus Crime Control and Safe Streets Act.The Justice System Improvement Act of 1979 prompted regulatory changes, including the formation of this, and made substantial modifications to DOJ entitiesby the Office of Legal Policy of the DOJ. The policy was created in response to concerns about aggressive information gathering and intelligence operations by state and local law enforcement organizations, which commonly entailed gathering and keeping records on people who were expressing unpopular opinions but weren't engaging in illegal activity.

Since the federal government cannot impose policy on state and local governments, the only way to influence them was to make compliance with the policy a requirement for receiving federal funding. The rule outlines procedures for gathering, keeping, reviewing, disseminating, and deleting criminal intelligence records. The regulation basically states that there must be enough evidence to establish a reasonable suspicion that an individual is engaging in criminal behavior before information that identifies an individual or an organization may be retained in the criminal intelligence records system of a state or local law enforcement agency. Many people believed that this would be a substantial obstacle to efficient intelligence operations when the rule was first adopted. But looking back, it's clear that the legislation is a crucial instrument for upholding individuals' civil rights without unduly restricting intelligence operations.

Investigations into Intelligence Activities by Congress

Inquiries into the intelligence community during this time period shifted from evaluating the effectiveness of intelligence operations to evaluating the legitimacy and propriety of the actual activities carried out. As will be shown, the suggestions made by three congressional committees would have a significant impact on the authority and responsibilities of IC members in the areas of national security intelligence and law enforcement. The two sorts of intelligence activity would thus be kept apart, creating the infamous "wall between domestic and international intelligence."The Rockefeller Commission suggested restricting the CIA's ability to carry out domestic intelligence activities in 1975. The group also suggested that the FBI director and the director of central intelligence establish the parameters of each agency's authority. The House Select Committee on Intelligence issued suggestions in 1976 to further reduce the areas where national security organizations' jurisdictions overlappedagencies that are mainly in charge of law

enforcement intelligence. However, the suggestions made by the Church Committee had the most impact on the creation of the wall of separation.

The U.S.-created Church Committee is an investigation. Unlike the Rockefeller Commission, the Senate reviewed the actions of the IC in 1976 in more detail. The suggestions provided by this investigation resulted in jurisdictional reformationswith the IC. The majority of the suggestions focused on giving the FBI and CIA additional operating parameters. The following 183 recommendations from the committee highlight how law enforcement and national security intelligence were separated: The group suggested that organizations like the National Security Council andMilitary branches, the CIA, and the Agency lack the authority to carry out domestic intelligence operations. Particular focus was placed on the CIA's function, with the statement that "the CIA should not be allowed to undertake domestic security operations inside the United States.

The group proposed that the FBI be given "sole responsibility" for looking into American citizens for domestic intelligence purposes.Every agency should take precautions to prevent erroneous intelligence activity.It is generally acknowledged that the Church Committee's recommendations were a key factor in separating national security information from law enforcement intelligence. However, the request for this division did not imply that the organizations' collaboration should end. In fact, the Church Committee suggested that the CIA and FBI maintain intelligence sharing and make

an improved attempt to align their objectives. How can the two agencies collaborate and coordinate efforts when there are significant restrictions on the categories of information that may be gathered and shared? This was a challenging operational issue. What part, if any, did the intelligence of tribal, municipal, and state law enforcement play in this arrangement? Increased division of labor between agencies and within each agency was the outcome.13 Recommendations to enhance law enforcement intelligence, however, have nothave only applied at the federal level. These suggestions have also been given to regional and local law enforcement organizations.State, local, and tribal law enforcement intelligence is evolving as a result of national crime commissions and new initiatives.

Since 1931, 15 national crime commissions have looked at a variety of criminal concerns in the US, from drug trafficking and street crime to organized crime and terrorism. The majority of them have offered evaluations and suggestions pertaining to some component of law enforcement intelligence.Understanding the commissions' overarching goals before looking at those with particular intelligence recommendations reveals a long history of creating law enforcement intelligence operations that are unbiased, analytical, and considerate of people's rights to privacy. Although the ideas show forward thinking, not all of them were adopted right once, mainly because they constituted a shift in the era's police occupational culture. However, crucial ideas were developed that served as the basis for modern law enforcement intelligence techniques.

The Commissions and Why They Exist

From 1928 to 1931, the National Commission on Law Observance and Enforcement published a number of studies and memos that looked at all facets of severe crime in the US. The goal was to counter the rise in violent crime and organized crime, which looked to be linked to increasing urbanization and industrialisation. The Commission also tried to comprehend why law

enforcement, the legal system, and the correctional system failed to handle America's crime issue successfully. There were no significant national committees looking into crime during the next three decades, undoubtedly in large part due to Americans' preoccupation with the Great Depression, World War II, and post-World War II worries about the Soviet Union's escalating nuclear threat. In fact, the Wickersham Commission's recommendations were mainly not adopted as a result of these world events.President Lyndon B. Johnson established the Warren Commission after President John F. Kennedy was assassinated in November 1963. The Commission's objective was to ascertain the events preceding up to the killing, although the less contentious findings of the Commission were scrutinized

the connections, communication, and overall capacity of federal, state, and local police enforcement to collaborate for a shared goal protecting the President of the United States. Unaware of it at the time, the murder foreshadowed a turbulent and paradigm-shifting decade.Due to the rise in violence, the rise in drug usage, and the increasing knowledge of crime, the 1960s saw an increase in worry about crimeof organized crime, as well as worries about unfair judicial practices, especially those affecting minorities. President Johnson established the President's Commission on Law Enforcement and Administration of Justice in 1965 to address these issues; this commission was intended to complement President Johnson's domestic social agenda, known as "The Great Society." In a series of task force reports published in 1967, the President's Commission looked into all facets of the criminal justice system as well as specific inquiries into narcotics and organized crime.

There were worries about issues ranging from violence, riots in our cities, increases in the use of narcotics, a growth in the use of illegal dangerous drugs, and concerns about moral decay, which were frequently illustrated by the increased presence of pornographic materials. It was acknowledged that the 1960s were the "decade of social revolution" on many fronts. The National Advisory Commission on Civil Disorders was established in an effort to comprehend the dynamics of civil disobedience and civil disorders as well as to assess the government's response in 1967 after a string of violent demonstrations in American cities spurred by the Civil Rights Movement. The National Commission on the Causes and Prevention of Violence and the U.S. Commission on Civil Rights were both established in 1968 and the Commission on Pornography and Obscenity.

According to prior commission investigations, among the numerous elements that contributed to the social turmoil of the 1960s was a marked increase in drug consumption. As a consequence, a further investigation was made expressly to look into this matter more thoroughly; the U.S. Cannabis and Drug Abuse Commission.The effort to professionalize all facets of the criminal justice system was one of the defining features of the 1967 President's Commission. The National Advisory Commission on Criminal Justice Standards and Goals of the Justice Department, as well as a number of studies by working groups of that commission known as the National Advisory Committee on Criminal Justice Standards and Goals, followed this example.

National investigations that strive to understand the reasons behind different crimes as well as provide top-notch guidance on the finest ideas, suggested approaches, and programsto combat crime. These organizations included the President's Commission on Organized Crime, the Attorney General's Commission on Pornography, the Attorney General's Task Force on Violent Crime, and the Justice Department's National Advisory Committee for Juvenile Justice and Delinquency Prevention.

The national commissions on crime concerns that were so common in the preceding three decades did not exist throughout the 1990s. The National Institute of Justice, the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the newest Justice Department organization, the Office of Community Oriented Policing Services, all saw a notable increase in government-sponsored research and program development on a wide range of crime-related issues.The output of these bodies served as a stand-in for the national commissions in many respects.

The U.S. military strikes, the bombings of the American embassies in Africa, and an overall rise in terrorist acts throughout the Middle East contributed to an increase in worry about terrorism in the late 1990s. Consequently, the U.S. Congress authorized a 5-year, yearly investigation into whether the US is vulnerable to strikes utilizing WMDs. In 1999, the advisory panel to evaluate domestic preparedness for terrorism using WMDs released its first assessment.The National Commission on Terrorist Attacks Upon the United States, the most recent notable commission, released its findings in 2004. The criminal justice system was affected, but it also included a broad range of other concerns. Later on in this, they are covered.

The Law Enforcement Intelligence and National Crime Commissions

Although not all of these commissions directly addressed intelligence, they all called for greater use of a variety of analytical techniques to comprehend crime and criminal justice as well as to help predict crime for the purpose of prevention, which is a key element of the intelligence process.The Wickersham Commission found it necessary to investigate and comprehend the criminal environment as a crucial instrument for apprehending criminals. The 1964 President's Commission on the Assassination of President Kennedy made one of the first clear recommendations for intelligence and information sharing between federal agencies and state and local law enforcement 33 years later. Although the Secret Service and the FBI received the bulk of the Commission's recommendations, it was also suggested that these organizations collaborate more closely with local law enforcement. The Commission specifically urged improved communication and information sharing between regional and federal institutions.

Many of the same criteria were underlined in the President's Commission on Law Enforcement and Administration of Justice's 1967 findings, which also included a great deal more study, detail, and specific recommendations. In addition, the Omnibus Crime Control and Safe Streets Act of 1968, which was approved by Congress the year after the President's Commission findings were made public, made it possible to execute many of the Commission's recommendations. The President's Commission made the following recommendations on intelligence:Every major city's police force should create a specialized intelligence division whose main purpose is to track down organized crime and gather data on any potential involvement of cartels in local criminal activities.

It's interesting to note that the President's Commission said that "criteria for evaluating the effectiveness of the units, other than mere numbers of arrests, must be developed"16. This controversy persists. The President's Commission continued by advising the Department of Justice to provide financial supportto promote the creation of effective mechanisms for acquiring, collecting, and disseminating regional intelligence. About ten years later, the Justice Department established the Regional Information Sharing System, which includes six regional intelligence centers.The President's Commission's intelligence concentration was mostly on organized crime and to a lesser degree on drug control, while the Kerner Commission's focus

was on violent civil disturbances and civil disobedience. The Kerner Commission noted this on the riots and civil disturbances that occurred in American cities:No one kind of control worked well in every circumstance. The variable efficacy of control tactics highlights the need of prior preparation, intelligence systems that are competent, and understanding of the Further, the Kerner Commission advised that law enforcement authorities should conduct the following:Create an intelligence system to provide law enforcement and other public authorities trustworthy information that might aid in preventing the onset of a disturbance and in putting in place efficient control measures in the event that a riot breaks out.Similar findings were made by the National Commission on the Causes and Prevention of Violence.

Lack of a solid intelligence system is one of many police forces' biggest weaknesses. Police and government personnel have been severely hindered in their ability to foresee potential problems, prevent them from happening, and reduce and manage an existing disturbance. This occurs mostly as a result of a failure to learn about and comprehend local issues and complaints as well as to get trustworthy information on local leaders and organizations. An efficient program to combat false and inflammatory rumors that might fuel unrest and violence is also required in relation to this issue. Reliable mechanisms are required to track, gather, and analyze rumors.The understanding that intelligence may be a useful tool for anticipating risks and combating sophisticated crime was gradually emerging as a broad variety of

These nationwide investigations looked at a variety of systemic societal issues relating to crime. The National Advisory Commission on Criminal Justice Standards and Goals' most extensive suggestion, which demonstrated how intelligence was being considered more widely than ever before. Ironically, the National Advisory Commission created a standard specifically for intelligence operations called Standard 9.11, which reads in part:Every police department and state must immediately develop and maintain the capacity to collect, analyze, and share intelligence in a way that respects each person's right to privacy while reducing organized crime and public unrest.

A suggestion from the National Criminal Intelligence Sharing Plan, which was published 31 years later, is very similar to the norm. It's interesting to observe in the standard that "information" is gathered and "intelligence" is spread.

The prior commission reports did not adequately define this reference to analysis. Additionally, the standard's emphasis on respecting individual privacy is a crucial component of all current law enforcement intelligence operations.

The National Advisory Commission also made suggestions in its report about the organization and management of the intelligence operations for state and municipal law enforcement organizations. These suggestions included the following:

Developing Intelligence-Related Functions

Each state should establish a centralized law enforcement intelligence function that includes all of the state's police forces. To improve the protocols for exchanging criminal information, nations should think about creating regional intelligence networks among neighboring states. Each local law enforcement agency should create its own intelligence division in line with the intelligence division of its respective state [10]–[12].

CONCLUSION

In general, the suggestions for modifying law enforcement intelligence are meant to make sure that it is carried out in a way that respects the rights and dignity of every person while simultaneously offering efficient instruments for thwarting and looking into illegal activities. To address the problems of contemporary law enforcement and preserve the public's confidence in law enforcement authorities, law enforcement intelligence procedures must be continuously developed and improved. Additionally, it's important to make sure that law enforcement information isn't being used to track people or organizations based on their color, ethnicity, religion, or political opinions, but rather on actual dangers to the public's safety. This necessitates precise criteria for the gathering and use of intelligence data, as well as protections to prevent unjustified invasions of people's civil rights and privacy.

REFERENCES

[1] D. L. Carter, "Brief history of law enforcement intelligence: Past practice and recommendations for change," *Trends Organ. Crime*, 2005, doi: 10.1007/s12117-005-1037-5.

[2] D. Derencinovic and A. M. Getos, "Co-operation of law enforcement and intelligence agencies in prevention and suppression of terrorism - european perspective," *Rev. Int. Droit Penal*, 2007, doi: 10.3917/ridp.781.0079.

[3] A. Gregg, "Autonomous Police Vehicles: The Impact on Law Enforcement," *Homel. Secur. Aff.*, 2019.

[4] C. A. Meissner, S. Oleszkiewicz, F. Surmon-Böhr, and L. J. Alison, "Developing an evidence-based perspective on interrogation: A review of the U.S. government's high-value detainee interrogation group research program," *Psychol. Public Policy, Law*, 2017, doi: 10.1037/law0000136.

[5] P. Andreas and R. Price, "From war fighting to crime fighting: Transforming the American national security state," *Int. Stud. Rev.*, 2001, doi: 10.1111/1521-9488.00243.

[6] J. Morrison, G. Watts, G. Hobbs, and N. Dawnay, "Field-based detection of biological samples for forensic analysis: Established techniques, novel tools, and future innovations," *Forensic Science International*. 2018. doi: 10.1016/j.forsciint.2018.02.002.

[7] L. K. Johnson, "MAGTF Intelligence Production and Analysis," *Development*, 2010.

[8] E. Bruenisholz *et al.*, "The Intelligent Use of Forensic Data: An Introduction to the Principles," *Forensic Sci. Policy Manag. An Int. J.*, 2016, doi: 10.1080/19409044.2015.1084405.

[9] K. W. Steiner, "Green Eyes: the current role of intelligence in African counter-poaching," *African Secur. Rev.*, 2020, doi: 10.1080/10246029.2020.1781671.

[10] A. Thibault, "A Prescription for Information Sharing Between Law Enforcement and The Medical Community to Improve Threat Assessments," *Homel. Secur. Aff.*, 2018.

[11] P. Baines, N. O'Shaughnessy, and N. Snow, *The SAGE Handbook of Propaganda*. 2020. doi: 10.4135/9781526477170.

[12] J. L. Schecter, " Loch K. Johnson (ed.), The Oxford Handbook of National Security Intelligence ," *Intell. Natl. Secur.*, 2012, doi: 10.1080/02684527.2012.688318.

CHAPTER 4

INTELLIGENCE FUNCTION OPERATIONS

Dr. Vinoth. S, Professor, Department of Finance,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email Id- dr.vinoth@cms.ac.in

ABSTRACT:

Intelligence function operations refer to the processes and activities involved in gathering, analyzing, and disseminating information to support decision-making and achieve organizational goals. Intelligence functions are critical for government agencies, military organizations, law enforcement, and private sector organizations, as they provide key insights into potential threats, risks, and opportunities. Intelligence function operations typically involve the collection of data from a variety of sources, including human intelligence, signals intelligence, open-source intelligence, and geospatial intelligence. The data is then analyzed using various techniques, such as data mining, statistical analysis, and pattern recognition, to identify patterns, trends, and potential risks. This analysis is then used to produce intelligence products, such as reports, briefings, and assessments, which are disseminated to decision-makers.

KEYWORDS:

Counterintelligence, Counterterrorism, Cryptography, Cybersecurity, Data Mining, Intelligence Cycle.

INTRODUCTION

Every state and local intelligence agency should assist the federal government.To guarantee efficacy and efficiency, operational rules and procedures should be created for each municipal, state, and regional intelligence role.There should be a designated representative from each agency who controls all intelligence activities and reports to the head.Each agency should establish protocols to make sure that intelligence-related material is properly screened, secured, and distributed. The National Advisory Committee on Criminal Justice Standards and Goals developed the idea and operational procedures for intelligence in 1976. Organized Crime-Task Force Report on Organized Crime, a publication of the Committee, contains information that goes into more depth than any commission or investigation that has come before it. In addition to suggestions for the establishment of an intelligence unit, the standards also call for the preservation of confidentiality, the use of "need-to-know" and "right-to-know" criteria for information dissemination, guidelines for the destruction of intelligence records, and the necessity of maintaining both individual and organizational accountability in the intelligence function.

Many of the standards and discussions of intelligence from 1976 are consistent with the current vision of good practice in law enforcement intelligence, even though the recommendations emphasize organized crime, including drug trafficking, as opposed to the "all crimes, all hazards" approach used by law enforcement in the post-9/11 environment [1]–[3]. The President's

Commission on Organized Crime was established in 1983 and conducted a thorough investigation into every facet of organized crime, from "traditional" organization crime to drug cartels, sophisticated money-laundering schemes, and entrepreneurial crime of all kinds and commodities. The goal was to provide readers a thorough understanding of organized crime, including its structure, impact, and most effective methods of control. It acknowledged the need of good intelligence analysis as a weapon for law enforcement to effectively combat multijurisdictional complex crime.

By the middle of the 1980s, criminal businesses had expanded significantly and included a wide range of unlawful pursuits, including the trafficking of drugs and the counterfeiting of consumer goods. Investigators and intelligence agencies lacked the knowledge and manpower necessary to successfully control the issue. This was made worse by the fact that law enforcement agencies at all levels of government did not effectively share information with one another and did not typically comprehend the nature of organized crime.30 Organized crime was described as a "rapidly changing subculture" that was eluding law enforcement's capacity to keep up with it. Organized crime was increasingly seen as primarily a federal issue that state and local law enforcement would assist via information exchange and involvement in task teams [4]–[6].

The Attorney General's Commission on Pornography understood that intelligence operations would be a helpful instrument for halting interstate commerce in obscene and pornographic materials, much like the problems with organized crime. State and local law enforcement, on the other hand, tended to see this as a low priority and a poor use of their time and resources.

Questions about the United States mainland as a terrorist target and the capacity of the U.S. to effectively foresee, manage, and respond to an attack "at home" particularly an attack involving WMD—started to surface in the 1990s after an increase in terrorist attacks in the Middle East, particularly after the bombings of U.S. embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya. The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction was established as a consequence in 1999 by order of the U.S. Congress. The yearly reports, which were published between 1999 and 2003, extended beyond WMD and examined terrorism more generally especially in the wake of 9/11 as well as what the U.S. Government could do to successfully defend the country. The Gilmore Commission urged policymakers to go beyond simply responding to the terrorist attacks of September 11 and develop forward-thinking efforts by government at the federal, state, and local levels, as well as by the private sector, in addition to recommending more robust intelligence and information sharing. The Gilmore Commission concluded in its 2002 report that successful counterterrorism depends on timely collection, careful analysis, and proper distribution of intelligence. We have said that "more can and must be done to provide timely information up, down, and lateraly, at all levels of government to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats." from the beginning of our discussions. That message was reaffirmed in a staff report from the National Commission on Terrorist Attacks Against the United States, especially with respect to intelligence sharing. The FBI's ability to share information with state and local law enforcement was one area of worry. The following is an excerpt from the staff report for the commission:

There have been suggestions that the FBI still needs to release a lot more case-specific, operational information. Michael Sheehan, the deputy commissioner for counterterrorism at the NYPD, hypothesized that one of the reasons for this information sharing's shortcomings may be

that the FBI doesn't always understand what information would be crucial to others. Officials from the Los Angeles Police Department complained to us that the FBI provides them with diluted reports. According to information provided to us, the FBI intends to adopt a "write to release" strategy that would enable more rapid and extensive unclassified intelligence disclosure.

Through the National Criminal Intelligence Sharing Plan and, more particularly, the creation of law enforcement intelligence "requirements" by the FBI, these challenges are being addressed. The initiatives of the FBI Office of Intelligence also included a revised report-writing style that would immediately facilitate information sharing, including sharing with intelligence customers who did not have security clearances, as former FBI Executive Assistant Director for Intelligence Maureen Baginski stated in remarks at the 2004 COPS Office National Community Policing Conference.

It's interesting to note that many of the problems and observations mentioned in earlier commission reports from the preceding 40 years were included in the 9/11 Commission's staff report on reforming the intelligence function. The difference is that real change is in fact taking place, primarily as a result of the tragedy of September 11, 2001. Numerous suggestions about intelligence were made in the 9/11 Commission Report. Their main proposals focused on collaborative partnerships, the merger of intelligence services, and a broad reengineering of the intelligence community. The Commission discussed the function of tribal, municipal, and state law enforcement organizations. The role of state and municipal law enforcement is expanding. They need additional instruction and collaboration with federal agencies if they are to work together more successfully with those authorities in tracking down terrorism suspects.

Following that, the 9/11 Commission acknowledged the following:

The FBI makes up a very minor portion of the nation's law enforcement community, which is mostly made up of state and local law enforcement organizations. The information-sharing network and the work of the FBI through regional Joint Terrorism Task Forces should develop a mutually beneficial relationship where state and local agents are aware of the information the FBI is seeking and receive some of the information being developed about what is occurring or potentially occurring in their communities in return.

A new domestic intelligence organization should be established, according to the 9/11 Commission, and it should forge "relationships with state and local law enforcement."36 The Commission recommended the establishment of a new National Counterterrorism Center, saying that it should "outsource to knowledgeable officials in state and local agencies throughout the United States."37

The Commission's proposals make it clear that terrorism is a local issue that requires crucial state and local engagement in prevention and response. The themes that run through all of the investigations into crime and justice, from the Wickersham Commission to the 9/11 Commission, are to attack the root causes of crime, comprehend all facets of the crime dynamic, approach crime holistically, collaborate with other agencies and share information, move beyond conventional approaches, and protect people's civil and human rights.

These ideas hold true whether the crime is terrorism or armed robbery. Undoubtedly, in the wake of 9/11, law enforcement intelligence practitioners have listened to and taken note of these lessons.

DISCUSSION

Law Enforcement Intelligence Initiatives in the Post-9/11 Environment

The terrorist events on September 11, 2001 have sparked a number of notable projects that have had a large and quick impact on the development of law enforcement intelligence. The most important changes taking place at this period.The International Association of Chiefs of Police conducted its annual convention in Toronto, Ontario, Canada in October 2001, roughly six weeks after the 9/11 attacks. The Police Investigative Operations Committee there highlighted the necessity for national leadership to provide norms and guidelines for SLTLE agencies as well as the need for SLTLE agencies to reengineer their intelligence function. Following this gathering, the IACP conducted the Intelligence Summit in March 2002 with financial assistance from the COPS Office. A strategy for exchanging criminal information was created during the conference, and intelligence-led policing was approved.

The Global Justice Information Sharing Initiative, a U.S. Office of Justice Programs-funded organization, already existed and was tasked with creating procedures and guidelines for effectively exchanging information across the criminal justice system. The Global Intelligence Working Group was established as a new subgroup in response to the IACP Intelligence Summit in 2002. The GIWG's mission was to carry out the summit's recommendations. The National Criminal Intelligence Sharing Plan was the first output of the GIWG [7], [8]. The National Criminal Intelligence Sharing Plan was formally unveiled in a national signing ceremony in the Great Hall of the U.S. Department of Justice on May 14, 2004, and it represented a crucial aspect of intelligence sharing for all law enforcement personnel. The NCISP offered a crucial basis for state, local, and tribal law enforcement agencies to build their intelligence programs on thanks to official approvals from the DOJ, DHS, and FBI. The plan's goal was to provide SLTLE organizations the resources and tools they needed to produce, acquire, access, receive, and share information.

The NCISP40 created a set of national standards that are now publicly acknowledged as the function and procedures for law enforcement intelligence by the professional community. Organizational restructuring, the idea of information sharing, and training in American law enforcement are all being significantly impacted by the strategy.The Criminal Intelligence Coordinating Council was to be established in order to create the links required to improve intelligence and information sharing among all levels of government. The NCISP also recognized the significance of local, state, and tribal law enforcement agencies as a key component in the nation's intelligence process. The CICC, which is made up of representatives from law enforcement agencies at all levels of government, was officially founded in May 2004 to provide guidance about the introduction and improvement of the NCISP. Members of the CICC assist local law enforcement agencies' efforts to gather and disseminate criminal information in order to advance public safety and protect our country. They also act as advocates for local law enforcement. SLTLE must be included in the creation of laws and regulations that support the exchange of information and intelligence because of the crucial role they play in homeland security. By advising the U.S. Attorney General and the Secretary of Homeland Security on the best way to utilize criminal intelligence as well as the capabilities and restrictions of SLTLE agencies with regard to information sharing, the CICC acts as the voice for all levels of law enforcement agencies.

The development of multijurisdictional intelligence capabilities by numerous states and regions in a variety of ways occurred concurrently with these initiatives. These capabilities were designed to maximize the variety of raw information input for analysis and look into potential acts of terrorism that may occur within regions. The DHS accepted the units, known as "fusion centers," and started paying some of the centers so they could function. The idea of "intelligence fusion" quickly gained popularity as a productive and successful method for creating intelligence goods. The centers' focus widened to "all crimes" as a result of the realization that other crimes, such financial crime and weapons violations, may have a connection to terrorism. Additionally, as a result of the DHS's expanding mandate and increased financial support, the fusion centers' scope was expanded to include "all crimes, all hazards, and all threats."

In order to develop a set of recommendations and best practices for law enforcement agencies taking part in the intelligence fusion process, the GIWG created the Fusion Center Guidelines42 after realizing the advantages of standardization in improving the quality of work being done by the fusion centers. The Guidelines, although largely concentrating on criminal intelligence, also pay attention to public safety problems associated with homeland security intelligence as well as the connection between law enforcement and the business sector in terms of information sharing. As many law enforcement agencies as possible are encouraged to participate in the fusion process as information-sharing partners. As law enforcement engagement rises, more varied information will be fed into the analytical process, resulting in more robust analytical findings. It is obvious that a key component of greater agency cooperation with fusion centers is the suggestion from the NCISP and the second COPS/IACP Intelligence Summit that all agencies, regardless of size, should build an intelligence capability.

The Homeland Security Presidential Directive-8 mandates the DHS's objective, which is "to prevent, respond to, and recover from threatened and actual domestic terrorist attacks, major disasters, and other emergencies." Determining the essential information, abilities, skills, and procedures that law enforcement and emergency services professionals needed in order to fulfill these responsibilities was a crucial component of this endeavor. The Target Capabilities List44 has a detailed description of these capabilities. The TCL is a national-level, generic model of operationally ready capabilities defining all-hazards preparation, and it is designed to safeguard the country from all threats. The list is divided into many "areas" pertaining to prevention and reaction. Two particular intelligence-related target capabilities are part of the "Prevent Mission Area": "Information Gathering and Recognition of Indicators and Warnings" and "Intelligence Analysis and Production." The emphasis of the "information gathering" capacity is on "the continuous gathering of only pure, unexamined data." that may be utilized in the intelligence gathering process to detect dangers and signs of threats. Effective analysis depends on this kind of information, and fusion centers rely on law enforcement agencies to provide it to them via tips, leads, reports of suspicious activities, and the monitoring of terrorist or criminal indications.

The "intelligence analysis" target capability entails "the integration of data and information for the aim of analyzing, connecting, and distributing timely and actionable intelligence with a focus on the overall threat landscape for public safety and homeland security. For tactical, operational, and strategic purposes, this procedure concentrates on the consolidation of analytical results among the intelligence analysis units at the Federal, State, local, and tribal levels. This capacity also entails the analysis of unprocessed data to spot potentially dangerous trends, spot threat images, or connect questionable linkages to find possible indicators or warnings. Both the NCISP and the Fusion Center Guidelines are mentioned as standards and procedures to complete these

two target capabilities in the Target Capabilities List. A culture of information sharing that integrally involves state, municipal, and tribal law enforcement is what the integration of these projects aims to establish. The Intelligence Reform and Terrorism Prevention Act of 2004 was approved by Congress, building on these measures as well as other recent programs and activities in the intelligence community and the 9/11 Commission's recommendations. The establishment of the Office of the Director of National Intelligence, a Directorate of Intelligence within the FBI, the National Counterterrorism Center, and the requirement for the creation of the Information Sharing Environment are just a few of the many significant aspects of this legislation that are significant for the current discussion.

The establishment of the ODNI was the first element of the IRTPA regulations that dealt with SLTLE. The Director of National Intelligence is responsible for leading the intelligence community and serving as the President's top national security adviser. The official acknowledgement that SLTLE plays a part in both homeland security and national security is one of this office's novel features. An Assistant Deputy Director of National Intelligence for Homeland Security and Law Enforcement works for the ODNI. Although the ADDNI's role and responsibilities are constantly developing, in general, the ADDNI is in charge of decisions regarding information sharing policies between the Intelligence Community and SLTLE. Additionally, the ADDNI counsels the Intelligence Community on national security-related law enforcement capabilities, activities, and limitations.

The establishment of the FBI Directorate of Intelligence to oversee all FBI intelligence operations was the second element. The FBI's National Security Branch is where the DI is structured, and it is integrated into all areas of criminal, terrorist, counterintelligence, WMD, and cyber investigations.48 Threat identification and information exchange with SLTLE organizations and the Intelligence Community are important duties of the DI. The DI aspires to become a "full and trusted partner who can be relied upon to proactively bring FBI resources to the to help resolve threats."49 The IRTPA mandate firmly established and increased the DI's jurisdiction over the administration of the FBI's intelligence activities, including coordination of human resource development and management and monitoring of field intelligence operations.

The third factor was the creation of the National Counterterrorism Center.

With the exception of domestic terrorism, the NCTC is the main institution responsible for collecting and assessing all information relating to terrorism. The NCTC also supports government-wide counterterrorism initiatives by acting as the key knowledge repository for information on terrorism. The primary goal of this organization is to "get the right counterterrorism information into the right hands of the right people" within DHS, the FBI, the Intelligence Community, and, indirectly, SLTLE. The NCTC aims to gather information from several departments of the federal government in one location for analysis and integration before providing clients with the combined data.

The development of the information sharing environment is the last IRTPA aspect that SLTLE is concerned with. In accordance with the IRTPA, the President was obligated to create an ISE "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." It also mandated the selection of an ISE program manager, who would be in charge of organizing and supervising the administration and execution of the ISE.

A letter requesting the identification of a major fusion center was issued to the governors of each state in November 2007 and was jointly signed by the U.S. Attorney General and the Secretary of Homeland Security. The letter included the phrase "To coordinate the gathering, processing, analysis, and dissemination of terrorism, law enforcement, and homeland security information in an all-crimes approach, DOJ and DHS will work with governors or other senior state and local leaders to designate a single fusion center that will act as the state's or region's hub to interface with the federal government. Your office has to choose one fusion center to act as the state's hub immediately. Please take into account creating an inclusive approach that is compatible with the government initiatives to establish the ISE when choosing a single fusion center.

The Information Sharing Environment Implementation Plan51 aims to strengthen the exchange of terrorism-related information among the 16 members of the Intelligence Community, as well as between them and the business sector, law enforcement organizations at all levels of government, and international partners. The ISE aims to "...implement a culture of effective, widespread information sharing, balanced with the need for security and the protection of privacy and civil liberties."52 State, municipal, and tribal law enforcement are expected to play a large role in the ISE, and the Implementation Plan outlines the stages and process in detail. Additionally, according to the Implementation Plan, each state must designate a principal state fusion center that would serve as the hub for information exchange between the federal ISE and SLTLE entities.

Information sharing has developed into the essential tenet of intelligence procedures to safeguard the United States, as is shown from the aforementioned activities. Information sharing across governmental levels remained challenging in spite of new initiatives, laws, and rules. As part of the new Interagency Threat Assessment and Coordination Group54 inside the NCTC, important decision-makers and officials from all levels of the ISE were required to regularly convene and address information-sharing issues. The DHS, the FBI, members of the intelligence community, and representatives from state and local law enforcement agencies make up the ITACG. Supporting NCTC's initiatives to create "federally coordinated" terrorism-related information products for distribution to state, local, and tribal agencies as well as business partners is a significant responsibility of the ITACG.

Members of the ITACG, especially those at the state and municipal levels, aid in identifying the intelligence products required by various consumer types. Members of ITACG provide advice, counsel, and subject matter expertise to the Intelligence Community regarding the operations of SLTLE agencies, including how such organizations use terrorism-related information to fulfill both their counterterrorism obligations and their core mission of protecting their communities. This is because each level of government has different priorities. In addition to these duties, the ITACG's coordination of the creation and prompt delivery of certain intelligence products to SLTLE authorities is a crucial function. The following is a list of the intelligence products:

Situational awareness reporting on important occurrences or actions at the global, national, state, or local levels. Strategic evaluations of the dangers and challenges posed by terrorism to the United States.The ISE was transitioning from a strategy to real policy and procedures. The White House published the National Strategy for Information Sharing in October 2007 as the next stage. The Strategy will help the Administration make sure that Federal, State, local, and tribal government employees who are in charge of defending our country from attacks in the future or

assisting in the event of an attack are aware of its goals and plans for enhancing the gathering and sharing of information about terrorism. The plan continues by noting:

According to the President's directives, State, local, and tribal authorities are crucial to our country's efforts to thwart other terrorist strikes. As counterterrorism and homeland security operations become more and more a part of state, municipal, and tribal missions, so do their informational requirements. They specifically need access to timely, reliable, and actionable intelligence about people and groups planning to launch attacks within the United States, their organizations and funding, potential targets, pre-attack warning signs, and significant events or circumstances that could affect State, local, and tribal preventive and protective postures [9], [10].

CONCLUSION

Operations in the intelligence function are crucial for firms to accomplish their goals and successfully manage risks. Organizations may take action to accomplish their objectives while limiting risk by using data and information to get insights into possible risks and opportunities. Organizations need well-trained individuals, transparent rules and processes, and the right technology and tools to guarantee the efficacy of intelligence function activities. To guarantee that intelligence is utilized to guide and assist decision-making, the intelligence function must also be tightly connected with other organizational activities, such as operations, planning, and risk management.

REFERENCES

[1] B. Feng and Q. Ye, “Operations management of smart logistics: A literature review and future research,” *Front. Eng. Manag.*, 2021, doi: 10.1007/s42524-021-0156-2.

[2] M. U. Tariq, M. Poulin, and A. A. Abonamah, “Achieving Operational Excellence Through Artificial Intelligence: Driving Forces and Barriers,” *Frontiers in Psychology*. 2021. doi: 10.3389/fpsyg.2021.686624.

[3] D. K. Baroroh, C. H. Chu, and L. Wang, “Systematic literature review on augmented reality in smart manufacturing: Collaboration between human and computational intelligence,” *J. Manuf. Syst.*, 2021, doi: 10.1016/j.jmsy.2020.10.017.

[4] R. Wolniak, “The concept of operation and production control,” *Prod. Eng. Arch.*, 2021, doi: 10.30657/pea.2021.27.12.

[5] W. J. Niu, Z. K. Feng, B. F. Feng, Y. W. Min, C. T. Cheng, and J. Z. Zhou, “Comparison of multiple linear regression, artificial neural network, extreme learning machine, and support vector machine in deriving operation rule of hydropower reservoir,” *Water (Switzerland)*, 2019, doi: 10.3390/w11010088.

[6] I. Szabadföldi, “Artificial Intelligence in Military Application – Opportunities and Challenges,” *L. Forces Acad. Rev.*, 2021, doi: 10.2478/raft-2021-0022.

[7] I. González-Carrasco, J. L. Jiménez-Márquez, J. L. López-Cuadrado, and B. Ruiz-Mezcua, “Automatic detection of relationships between banking operations using machine learning,” *Inf. Sci. (Ny).*, 2019, doi: 10.1016/j.ins.2019.02.030.

[8] D. A. Suleiman, T. M. Awan, and M. Javed, "Enhancing digital marketing performance through usage intention of ai-powered websites," *IAES Int. J. Artif. Intell.*, 2021, doi: 10.11591/ijai.v10.i4.pp810-817.

[9] M. Lohse, "Sharing national security information in Finland," *Inf. Commun. Technol. Law*, 2020, doi: 10.1080/13600834.2020.1759277.

[10] K. Sombultawee and S. Boon-itt, "Marketing-operations alignment: A review of the literature and theoretical background," *Operations Research Perspectives*. 2018. doi: 10.1016/j.orp.2017.11.001.

CHAPTER 5

ROLE OF STATE, LOCAL AND TRIBAL LAW ENFORCEMENT INTELLIGENCE

Dr. Rajiv Umeshchandra Kalaber, Assistant Professor,
Department of Finance, CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email id-prof.rajiv@cms.ac.in

ABSTRACT:

The role of state, local, and tribal law enforcement intelligence is to gather, analyze, and disseminate information to support law enforcement agencies in their efforts to prevent and investigate criminal activity. This includes a wide range of activities, from collecting data on criminal organizations and their activities to tracking individuals who may pose a threat to public safety. State, local, and tribal law enforcement intelligence play a critical role in detecting and preventing crime, as they are often the first line of defense in identifying potential threats and taking action to prevent them. They also work closely with federal law enforcement agencies to share intelligence information and coordinate responses to national security threats.

KEYWORDS:

Counterterrorism, Crime Analysis, Criminal Investigations, Fusion Centers, Intelligence Cycle.

INTRODUCTION

With the second IACP/COPS Intelligence Summit, post-9/11 intelligence advancements in many respects completed a circle. Despite the fact that law enforcement intelligence has undergone several significant and significant developments, the 2008 Summit Report noted the following: However, it was made evident by the attendees of the follow-up IACP Criminal information Sharing Summit that many of the country's law enforcement organizations do not take part in the criminal information sharing plan. It would seem that too many state, municipal, and tribal agencies undervalue their contribution to the criminal intelligence sharing process, exaggerate the difficulties of full involvement, or are oblivious to how they may help with the crucial tasks of the plan [1]–[3]. Along with the aforementioned projects, a number of additional efforts were either already underway or in the planning stages. These actions stand out because they have contributed to making the objectives and procedures of the aforementioned methods more attainable.

Working Group for the Coordination of Counterterrorism Training

The CTTWG was established in 2002 to support information sharing, interagency collaboration, and sharing of creative training initiatives among federal agencies engaged in counterterrorism and terrorist training. Later, the committee was enlarged to include representatives from the major law enforcement and training institutions. The CTTWG was further expanded to include policy-level agency officials from a variety of federal agencies, as well as academic institutions

and law enforcement groups engaged in federal, state, local, and tribal law enforcement training. The CTTWG acknowledged that more and more training-related concerns and initiatives that were brought to their attention focused on the field of intelligence. As a consequence, more emphasis was paid to intelligence training and how to make the most use of the available resources by making sure that the training is consistent, of high quality, does not duplicate other training, adheres to national standards, and fulfills the demands of law enforcement. An online Law Enforcement Intelligence Master Training Calendar was one of the new intelligence efforts. Version 2.0 of the Minimum Criminal Intelligence Training Standards was also prepared by the organization.

Minimum Standards for Criminal Intelligence Training61 The CTTWG created the Minimum Criminal Intelligence Training Standards after realizing that the intelligence capabilities of America's law enforcement sector could not be achieved without efficient training. The guidelines specify six law enforcement focus points that are essential to the performance of intelligence operations: Chief Executive, Intelligence Commander/Manager, Intelligence Analyst, Criminal Intelligence Officer, General Law Enforcement Officer, and Train-the-Trainer. The learning goals and essential information, skills, and abilities required to carry out intelligence tasks were outlined for each area by a group of seasoned law enforcement intelligence specialists. The desire and capacity to actively participate to the ISE rises dramatically as position-specific understanding of the intelligence process develops across the law enforcement community. The standards' Version 2.0 was accepted in October 2007.

Extensible Markup Language Data Model for Global Justice Many criminal justice information systems developed in a way that would not readily support electronic information exchange due to the administrative independence within and between each component of the criminal justice system. Information often needed to be shared in hard copy or reentered since it frequently relied on proprietary data models from suppliers. The challenge of creating a single data model that could be utilized as a standard by all system components was taken up by the Global Justice Information Sharing Initiative. Law enforcement, public safety organizations, prosecutors, public defenders, and the judicial branch now have a tool for efficiently and promptly exchanging data and information thanks to the Extensible Markup Language standard known as GJXDM.62 The Data Dictionary, Data Model, and Component Reuse Repository are the three main components of GJXDM. The data model was created with the intention of improving the exchange of criminal justice information, but it has since been used as a way to improve the electronic exchange of criminal intelligence data. Consequently, the GJXDM acts as a crucial technical element to support the ISE.

DISCUSSION

National Information Exchange Model

The Homeland Security Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Homeland Security Presidential Directive were all addressed by the combined DOJ and DHS program known as NIEM, which used the GJXDM data model. NIEM focuses on cross-domain information exchanges between important domains and communities of interest across all levels of government, whether between individual local law enforcement agencies, law enforcement and emergency service agencies, and other domains, or between local, state, tribal, regional, and federal agencies. This is in contrast to national database integration of all local, state, tribal, and federal databases.

The creation of a common data standard and a model for data sharing is unquestionably a crucial thread that runs throughout the information sharing culture.Grants for Technology, Training, and Assistance. The DOJ and DHS have made a commitment to assist the intelligence mission via grants from a number of their departments and bureaus. The growth of the information-sharing culture has depended heavily on the funding of a broad range of intelligence training programs, specific initiatives to give technical help, and aid in procuring technology and information systems consistent with GJXDM and NIEM. The fact that many intelligence-related efforts have included cooperation between the DOJ and the DHS is a crucial one. Beyond the assistance that these programs have offered, this partnership shows knowledge sharing in action [4], [5].

Implications

A study of the activities covered above shows that substantial progress has been achieved, despite the fact that the ISE Implementation Plan specifies that it is necessary to "promote a culture of information sharing across the Information Sharing Environment." The adjustments that have been accomplished in a very short period of time constitute substantial advancements and crucial milestones, even if the ISE will still confront obstacles in reaching its ultimate objective.Together, these projects have altered the law enforcement intelligence philosophy, which now reflects the following:

a. a dedication to information exchange between and within legal systems
b. enforcement organizations
c. The need to create a serious, impartial intelligence function with uniform national professional standards
d. acknowledging the significance of state, municipal, and tribal law enforcement in ensuring both homeland security and national security
e. a procedure dedicated to combating multijurisdictional crime and terrorism
f. a dedication to carrying out the intelligence job in a way that respects civil liberties and privacy.
g. Intelligence Gathered by Law Enforcement at the Tribal, State, and Local Levels

Although the various national crime commissions' recommendations aimed to improve law enforcement's ability to combat organized crime, by the mid-1980s, criminal enterprises had grown significantly and included such a wide range of illegal activities that SLTLE agencies' ability to address these issues was constrained. Investigators and intelligence agencies lacked the knowledge and manpower necessary to successfully control the issue. Organized crime was described as a "rapidly changing subculture" that was outpacing the capacity of law enforcement to control it66. This was made worse by a failure of law enforcement to generally understand the nature of the problem and by poor information sharing among law enforcement agencies at all strata of government. Law enforcement intelligence teams were thus often reduced to serving as nothing more than a repository for information or, in certain circumstances, were seen as a failed venture.

Many in the law enforcement community continued to value the intelligence role for law enforcement agencies despite its lack of effectiveness. However, one major shortcoming of state and municipal intelligence agencies was their failure to go beyond information gathering to a methodical manner of data analysis. The answer was for "the analytical function to guide the data collection" as opposed to the other way around.The fact that many law enforcement executives

either did not understand the usefulness of intelligence or lacked the skills required to utilize intelligence products effectively was another restriction of law enforcement intelligence.

Additionally, intelligence workers lacked the analytical abilities necessary to provide insightful intelligence products. It still is believed that training is a key component of the answer to this issue.A past problem was that intelligence agencies tended to be reactive in character and were often seen as sensitive information repositories rather than as proactive resources that might provide information vital for deterring crime and capturing perpetrators. In a similar vein, intelligence agencies often lacked reliable, well-defined output. Instead, intelligence reports often address important issues on an as-needed basis.

The failure to quickly and comprehensively distribute intelligence products was a last drawback. This was likely the biggest setback since organized crime's nature was continuously evolving different goods were being trafficked, the methods of operation tended to vary, and the people involved in the enterprise's operation often changed. It was believed that one essential element for enhancing law enforcement intelligence operations was the need for timely and relevant information.While the bulk of previous proposals were on the creation and management of intelligence units, suggestions have also been made with respect to the moral dilemmas posed by state and local intelligence activities.

Potential abuses of power were a worry at the state and municipal levels, too, in a manner similar to the worries that prompted the creation of the Church Committee at the federal level. As a result, suggestions were made to guarantee that people' civil rights be upheld. The Law Enforcement Intelligence Unit File Guidelines, for instance, were developed to provide a useful policy and procedures that were designed to make

Asuccessful intelligence procedure that adhered to 28 CFR Part 23 and safeguarded people' rights. Similar to this, the CALEA standard identified the need for law enforcement agencies to develop procedures to ensure that data collection on intelligence information is "limited to criminal conduct that relates to activities that present a threat to the community" and to develop methods "for purging out-of-date or incorrect information."70 The National Criminal Intelligence Sharing Plan and its suggestions are included into the most recent iteration of the CALEA intelligence standard.

Later on, it will be clear that the National Criminal Intelligence Sharing Plan and the establishment of the idea of intelligence-led policing represent significant turning points in the history of law enforcement intelligence. State, municipal, and tribal law enforcement intelligence is becoming increasingly specialized by developing both an overall intelligence concept and a standard for operations. Because of 9/11, it is adopting more advanced techniques, fostering better coordination within the law enforcement intelligence community, and working with a greater sense of urgency.

The Process of Intelligence for Tribal, State, and Local Law Enforcement

The Intelligence Process is the only activity-permeating function, regardless of the sort of intelligence.This procedure offers safeguards to guarantee the reliable administration of the data needed to provide intelligence. An outline of the intelligence process is provided here. The remainder of this guide will go into further depth on many of the concerns that were presented here.Throughout the intelligence literature, the intelligence process has been ed in a number of

different ways. Depending on the model employed, there may be a difference in the process's number of stages, but each model's goal is the samehaving a methodical, scientific, and logical technique to thoroughly analyze information to guarantee that the most precise, usable intelligence is created and sent to the individuals who give an operational reaction to thwart a criminal danger.

The procedure is the same for any illegal activity, including terrorism, drug trafficking, gang activity, and other illicit enterprises. In fact, the approach aids in identifying situations when there is a connection between these many offenses.Training Suggestions for the Intelligence Process: National Criminal Intelligence Sharing PlanRecommendation 18: All levels of law enforcement employees participating in the criminal intelligence process should receive training. The National Criminal Intelligence Sharing Plan's training requirements are to be taken into consideration as the minimum requirements for all impacted workers. In accordance with the National Criminal Intelligence Sharing Plan, beneficiaries of criminal intelligence training should also be acknowledged and given certificates for successfully completing the program.

The model utilized in this discussion is the one recommended in the National Criminal Intelligence Sharing Plan in order to be compatible with recognized national standards. Although they are often referred to as "steps," the various componentssteps of the process, and as information is processed and disseminated, there is a continuous ebb and flow of information between phases. Because of this, the intelligence process is not a set of independent steps that are mechanically processed in a rigid sequential order, but rather a recipe for intelligence and information sharing that will frequently change depending on the availability of "ingredients" and the "nutritional needs" of the consumer.Each stage may be divided into smaller procedures that work together to produce a successful information management and analysis system.

NCISP Intelligence Process

The intelligence gathering process resembles a community radar sweep in many respects. In order for operational units to formulate reactions, the procedure aims to detect possible risks, assess the severity of suspicious conduct, and offer signs of crime. An example of the ebb and flow of the intelligence process is the description of specific indications in an intelligence bulletin. When an officer notices actions that are consistent with these signs, they gather additional data to be processed through the cycle, giving the analyst more knowledge. Raw data to aid in the analysis's refinement. It is more likely to provide operational units with more clear information that they can utilize to stop a crime or a terrorist act when a more refined analysis is once again communicated to them.

Processes and Subprocesses in Intelligence

An intelligence brief, for instance, discusses the danger posed by Eastern European organized crime running protection networks in a significant midwestern city. An upsurge in thefts and property damage to small companies that are mostly run by immigrants has been seen by a police officer patrolling areas with high concentrations of Russian immigrants. The officer informs the intelligence section that offenses have been reported in light of the intelligence bulletinbecause what seem to be minor thefts and property damage in this part of the city may really be "enforcer" actions of Eastern European organized criminal protection organizations. In an updated report, the analyst adds the new material after correlating it with activities of the

organized criminal gang in other cities. This constant two-way flow of information is necessary for the Intelligence Process to function at its peak efficiency.

Planning and Guidance

Coordination of several tasks is a key component of intelligence. Similar to intermeshed gears, there must be a strategy for how each moving component will work with other components and how the gears will all handle an environmental change. The planning and direction phase of the cycle is when the Intelligence Process's gears are prioritized and synchronized.

It is crucial to recognize not only the threats that have been identified, but also dynamic threats where evidence indicating their presence may appear accidentally, as former FBI Executive Assistant Director for Intelligence Maureen Baginski frequently said, "The absence of evidence is not the absence of a threat." Personnel must be educated to be alert in searching for threats' evidence since threats might arise inside a jurisdiction or territory for a number of reasons. But this has to be a practical procedure. While it is often believed that the Intelligence Process should adopt a "all-crimes/all-threats approach," practically speaking, these threats are not "equal" and must be prioritized in light of their likelihood of occurrence and the kind of damage they might do to a community. Threat prioritization is a step of the first phase's "Direction" component, and it is thoroughly explained there. This is accomplished by regular threat assessments that are improved upon by data that has been put through the intelligence cycle. A threat has to be evaluated based on many factors.

Threat identification is the initial element of a threat. The Intelligence Process must determine where a danger falls on a multivariate probability continuum when evidence of a threat is discovered. While quantifying a danger would increase its accuracy, most threat-related factors can only be assessed on an ordinal scale. For instance, based on qualitative data, a threat variable's relative value on a scale of 1 to 10 may be determined. The information's quality is measured by the first two factors. The likelihood of the threat's result is gauged by the following two criteria. Together, they provide direction for making decisions. A reasonable evaluation of the information's quality might result in a different operational difference between the points on the scale. For instance, the top 20 teams will be ranked in college sports. However, the rating does not imply that the top-ranked squad is 20 times superior than the 20th-ranked team. reaction when the danger becomes more serious. Prior to making an operational reaction, a better quality of information could be sought as severity declines. Basically, this approach weighs trade-offs between risks and outcomes.

Threat Assessment Components for Planning and Direction

The evaluation of potential targets' vulnerabilities is the next phase. The range of targets is often reduced when a danger is discovered. Regardless of whether there are many or few targets, certain assessments of the targets' susceptibility may be made. The severity of the danger also grows as susceptibility rises. Consider, for instance, that a tiny gang of eco-terrorists intends to firebomb the sales inventory of several car dealerships that sell big trucks. The majority of dealership sales lots are open 24 hours a day. As a result, the danger grows and so does their susceptibility. Assume that in a different situation, the same eco-terrorist gang intends to firebomb tanks at a military facility to protest fuel consumption and environmental harm caused by the tanks passing through their practice range. Because the tanks on the military installation are inaccessible and can resist Molotov cocktails if the invaders get close to them, the target

vulnerability in this situation is minimal. Target vulnerability is a crucial factor in any threat assessment, as should be clear. A risk assessment is performed once threats and target vulnerabilities have been determined. The question "What is the probable result if the vulnerability is exploited?" perfectly captures risk. In the aforementioned example, the risk to the auto dealers may be high and the risk to the military installation may be low; however, more information is needed to support judgments and ascertain whether there are any additional, previously unknown, compounding factors before a risk conclusion may be made. This procedure aids in defining further intelligence requirements, information that must be gathered to fully comprehend the danger.

In essence, the threat assessment process aims to distinguish between intelligence targets who are "making a threat" and those that are "posing a threat." Since this is plainly subjective, as much data as is practical should be gathered and examined on these three criteria. Most of the time, there won't be enough data to evaluate each element of the threat assessment model meaningfully. As a consequence, the "requirements" questions' responses will assist make the danger scenario more clear. By detecting and removing inaccuracy, obtaining more information can improve intelligence.The possibility of newly emerging dangers should also be acknowledged. The existence of a specific target may attract a threat, changes in a community's character may spark new dangers, or the threat may just materialize as a consequence of the cumulative impact of several causes. The important thing to remember is that law enforcement officials need to be taught to recognize behaviors that go beyond the simple suspicion, document the behaviors as precisely as they can, and pass this information on to the intelligence analysts.

The capacity to prioritize resources and operational efforts for those crimes and situations that pose the greatest danger to public safety and security is the key benefit of the threat assessment model in Planning and Direction. The Intelligence Process often searches for pictures using an out-of-focus lens. The two-way flow of information helps narrow the focus and determine if a danger is there and how much risk it represents. The Planning and Direction process continuously assesses environmental changes, defines shifting objectives, and identifies new requirements for two-way information exchange.

To concentrate awareness training for police on how to perceive all risks, Planning and Direction demands the identification of threat priority in addition to resource concerns. In order to provide the organization, the flexibility to react to the shifting threat environment, policy and procedural frameworks are also necessary. The Planning and Direction phase is characterized by an ebb and flow of information that offers insight so that the changing threat environment may be controlled effectively, much like the Intelligence Process itself.

Collection

Collection is the process of acquiring unprocessed data that analysts will use to create reports and other intelligence-related products. Law enforcement agents will often collect information in five main formats to better understand the Collection phase of the process:

1. An answer to an intelligence request.
2. A reaction to signs of terrorism or criminal activity.
3. Unusual Behavior reports of actions seen by or brought to the attention of police.
4. Information that cops discover when looking into unrelated situations.
5. Suggestions from the public, informants, or business community.

Information that is actively sought for with the goal of providing particular answers to certain inquiries serves as the response to intelligence needs. This data may be gathered from public sources or the result of police enforcement techniques including interrogations, surveillance, undercover work, or other legal procedures. Law enforcement agents would gather information in response to indications by observing situations or actions they identify based on knowledge they acquired through training and/or intelligence bulletins that outline such signs. Typically, indications might be things like graffiti, the logo of an extremist organization painted on a wall or a vehicle, or odd behavior at a place that fits the description of a threat activity in an intelligence assessment.

Typically, information gathered via SARs is based on behavior seen by law enforcement personnel who, based on their training and experience, think the person may have been engaged in criminal action in the past or would likely be involved in criminal activity in the future, even when a particular criminal link is not discovered. Leads are details that police learn about a potential new danger that is mainly unconnected to the investigation at hand but becomes apparent throughout the investigation. Tips are observations made by the public that are sent to a law enforcement agency for further investigation.

Disciplines Used by the Intelligence Community for Information Gathering Even though it is often not used by law enforcement intelligence, it is advantageous to grasp some of the language used in the intelligence community given the information sharing environment. The IC uses five standard "collection platforms" or "collection disciplines" for information gathering:

1. Using human beings to gather or verify information using overt, covert, or clandestine procedures is known as human intelligence.
2. The phrase "signals intelligence" refers to a variety of techniques for collecting and using electronic signals, whether they are collected by satellite, aircraft, or the ground. SIGINT comes in three different forms:

a. The gathering and use of communications signals, such as wireless devices, fax machines, wireless networks, and voice over Internet protocol, is known as communications intelligence.
b. Radar, transponders, motion detectors, and other non-communications signals are intercepted by electronic intelligence.
c. The intercepting and use of performance and tracking data collected during the testing of military systems and spacecraft is known as foreign instrumentation signals.

3. Visual photography, infrared image capture, lasers, electro-optics, visual radar, and satellite imagery are some of the sources of imagery intelligence.
4. Dimension and signatures Analysis of electronic emissions from devices is intelligence, which looks for information patterns in a new region of the electromagnetic spectrum that haven't yet been picked up by other techniques.
5. Free Software Intelligence is the examination of publicly accessible information without the use of illegal or clandestine means.

Any individual or group mentioned in criminal intelligence data must be connected to crime in some way throughout the gathering process. This connection is known as a criminal predicate. Reasonable suspicion, which goes beyond mere suspicion that the named individual is committed or about to commit a crime, is the criterion for that criminal predicate. In reality, law enforcement organizations gather data on people even when there is no evidence of illegal

activity [6], [7].SARs, hints, and leads are a few examples. Although it could seem contradictory, this is a natural element of the intelligence process and has a resolution. It is the responsibility of the law enforcement agency to assess the credibility of any criminal claims included in SARs, leads, or tips. The two-tiered "Temporary File" and "Permanent File" records system utilized for intelligence records serves this function. The crucial problem for proving the criminal predicate in practice is the retention of the material that has been gathered.The reader should be aware that great effort was made to make it clear that the criminal predicate must be shown in order to collect and store information that identifies individuals or groups. The crucial thing to remember is that when identification is established, constitutional rights attach.The intelligence gathering process will also look to gather non-identifying data that aids in describing and comprehending criminal phenomena, such as crime patterns, criminal operation techniques, extremist group beliefs, and other non-identifying information. These kinds of information do not fall under the criminal predicate rule since no specific people are mentioned.Operations security is the last problem with Collection and the whole intelligence process. OPSEC focuses on locating and safeguarding data that might provide an intelligence target knowledge about a probe and allow the target to defeat the probe. The security of collecting sources, processes, and material must be maintained to safeguard the intelligence inquiry's integrity [3], [8].

CONCLUSION

The rise in domestic terrorism and other threats to public safety in recent years has brought attention to the value of state, municipal, and tribal law enforcement intelligence. Law enforcement organizations need quick, reliable, and relevant intelligence data to deal with these threats. State, municipal, and tribal law enforcement intelligence do have certain difficulties, however. These organizations must strike a compromise between the preservation of individual civil liberties and privacy rights and the need for intelligence collecting and analysis. They must also make sure that their intelligence operations are carried out in a way that is responsible, transparent, and compliant with the law. In order to ensure public safety and deter crime, state, municipal, and tribal law enforcement intelligence play a critical role. To successfully meet the difficulties of contemporary law enforcement, these organizations must continue to adapt and enhance their intelligence capabilities as threats and dangers continue to change.

REFERENCES

[1] S. Chermak, J. Carter, D. Carter, E. F. McGarrell, and J. Drew, “Law Enforcement’s Information Sharing Infrastructure: A National Assessment,” *Police Q.*, 2013, doi: 10.1177/1098611113477645.

[2] D. Carter, S. Chermak, E. McGarrell, J. Carter, and J. Drew, “Understanding the Intelligence Practices of State, Local, and Tribal Law Enforcement Agencies,” *Police Chief*, 2012.

[3] A. M. Randol, “Homeland security intelligence: Perceptions, statutory definitions and approaches,” in *Focus on Terrorism*, 2010.

[4] D. L. Carter, “The Law Enforcement Intelligence Function: State, Local, and Tribal Agencies,” *FBI Law Enforc. Bull.*, 2005.

[5] R. E. Dolan, “Philippines: A Country Study,” *J. Asian Stud.*, 1993.

[6] S. Goldstein, "Comparative Analysis of Fusion Center Interaction to Fire & EMS Agencies," *Homel. Secur. Aff.*, 2015.

[7] R. A. Best, "Securing America's borders: The role of the intelligence community," in *U.S. Border Security*, 2012.

[8] R. A. Best, "Securing America's borders: The role of the intelligence community," in *U.S. Border Security*, 2011.

CHAPTER 6

A STUDY ON LAWFUL COLLECTION METHOD

Dr. Sireesha Nanduri, Assistant Professor, Department of Finance, CMS Business School,
JAIN (Deemed to-be University), Bangalore, India,
Email id-sireesh_n@cms.ac.in

ABSTRACT:

Lawful collection methods refer to the processes and techniques used by law enforcement and intelligence agencies to gather information in a manner that is consistent with the law and respects individual privacy rights. These methods are critical for ensuring that intelligence and evidence are obtained legally and can be used in court to support criminal prosecutions. Lawful collection methods include a wide range of activities, such as conducting surveillance, intercepting communications, and conducting searches and seizures. These activities are subject to various legal and regulatory frameworks, such as the Fourth Amendment to the U.S. Constitution, the Foreign Intelligence Surveillance Act (FISA), and the Electronic Communications Privacy Act (ECPA), which provide guidelines for when and how law enforcement agencies can conduct these activities.

KEYWORDS:

National Security Letters, Pen Registers, Probable Cause, Search Warrants, Subpoenas, Surveillance.

INTRODUCTION

There are four primary actions in the Processing/Collation phase of the intelligence process. The first step is to assess the raw data from the gathering phase and decide if it will be useful for analysis. An evaluation should start by looking at the validity of the information's source. Ideally, a declaration of dependability from the main collector should be recorded. The significance of this evaluation is related to the amount of assurance that analyst will offer the data while making decisions throughout the analysis. When utilizing data from an entirely trustworthy source, an analyst will arrive at a different conclusion than when using data from an untrustworthy source [1], [2].

The veracity of the raw data is examined in the next evaluation step. The phrase "Does the information actually portray what it seems to portray?" best captures the meaning of validity. The collector or the analyzer may determine the validity of the data. The information gatherer can think that if information is rational and comes from a credible source, its validity is high. On the other hand, the analyst can have conflicting data that calls into doubt the reliability. In these situations, the analyst should specify what extra intelligence is needed to be collected in order to get the most accurate raw data possible for a thorough analysis. Therefore, despite the fact that this is just the third phase, the Intelligence Cycle begins again.

Using ordinal measures comparable to those, source dependability and information validity are often first evaluated. Despite their simplicity, these basic scales provide crucial core principles for evaluating intelligence. As a result, while gathering data for the Intelligence Cycle, law enforcement employees should be taught to provide these evaluations.The technique used to acquire the data was evaluated as a second kind of examination to make sure it complies with constitutional requirements. The National Criminal Intelligence Sharing Plan recommends that all parties take action to guarantee that the law enforcement community upholds people' right to privacy and constitutional rights throughout the intelligence gathering process.

The evaluation of the data collecting process is one of the first challenges in information gathering. A law enforcement agency must adhere to legal procedures while gathering data; for instance, data gathered on a person should be compliant with constitutional requirements.Three factors make the topic of legal collecting practices crucial: First, law enforcement personnel have sworn to safeguard a constitutional promise. Second, if the intelligence target is criminally prosecuted, crucial evidence may be omitted from the case if it was not gathered legally. Third, if a pattern of information about people being gathered consistently that does not adhere to constitutional requirements develops, this might expose the agency to legal culpability for breaches of civil rights. This evaluation is necessary for professional reasons, but it is also crucial in the event that the intelligence target is charged with a crime. Once again, training should aim to guarantee that the data was legitimately gathered and that the details surrounding the acquisition are well recorded.Integrating new data with old data is the third task in the collation/processing phase. Throughout this procedure, taking into account all other data gathered.The answers to these questions will aid in defining the inquiry's criteria and objectives. To standardize the data fields and improve the capacity to accurately compare data, this procedure also includes arranging and indexing the data.

The technique or mechanism used to establish whether various law enforcement organizations are looking into the same person or crime is known as "deconfliction," and it is the last action in this stage. This is done in a number of methods, one of which is the use of deconfliction information systems like the Drug Enforcement Administration's National Drug Pointer Index. In addition to determining if there are numerous inquiries, the deconfliction procedure informs each agency involved of the case's common interest and offers contact information using a system like NDPIX. This procedure of exchanging information and intelligence aims to reduce interagency disputes and increase the efficacy of the investigation. the Intelligence Cycle's Processing/Collation phase is crucial for two reasons: Through the process, it aims to give information quality control, and it also offers crucial insights into establishing intelligence needs. Consent, the Plain View Doctrine, a search ancillary to a legitimate arrest, an exigent situation, and consent are listed in that order. Instead of forecast, the term "prediction" is sometimes used. A prediction is a firm proclamation of the future that is almost impossible to know in actuality. Given the probabilistic nature of intelligence analysis, the word "forecast" is used to express what is most likely to occur given the data that are now known [3], [4].

DISCUSSION

Analysis

The core of the intelligence process is analysis. Critical thinking techniques and analytical procedures have been the subject of whole books. The goal of the present discussion is not to repeat this knowledge, but rather to provide the intelligence consumer some insights into the

duties associated with analysis. In essence, the analytical process is the scientific method of problem resolution.In order to develop a knowledge of the phenomena being studied, established research methodologies both quantitative and qualitative seek to objectively integrate linked factors in a body of raw data. The finished analysis delivers knowledge more than just a list of facts; it is synergistic in nature. However, the result is only as good as the caliber of the data that was initially provided for analysis, and the caliber of the study.

For the intelligence function to work well and create strong and actionable intelligence, effective training, policy guidance, supervision, and an operational strategy are crucial.For law enforcement, the term "actionable intelligence" has two main uses. The first category is tactical, where the results of the analysis must include enough specific information so that operational units may formulate a course of action. In certain instances, the reaction is modest, such as when patrol police are given signs of terrorism or criminal activities to look out for. Making arrests in other situations could require a complicated operational action. A jurisdiction or region's danger landscape may alter due to changes in crime kinds, criminal tactics, or both in the second use of actionable information that is strategic in nature.

Reports, also known as intelligence products, are the end result of the analytical process. The intelligence analyst will produce specific conclusions about the criminal business throughout the study in order to comprehend its impacts. These are often included in the products' explanations as findings, projections, and estimations.

A conclusion, as the phrase implies, is a conclusive declaration concerning the operation of a criminal organization, its important players, and each of their criminal culpability. An enterprise's future, changes in the business or its members, and potential dangers are all described in a forecast6. It also defines the projected consequences of the illegal activity. A criminal enterprise's estimated financial impact, commodity transaction changes, and/or potential future effects are all taken into account. These effects can include profits from a new criminal enterprise, financial losses from a terrorist attack, or an increase in contraband if new smuggling techniques are employed [5]–[7].

There are several intelligence consumers, and each has relatively distinct requirements. Line officers need information that clearly identifies criminal indications, suspects, locations, crime tactics, and vehicles believed to be connected to a criminal business. Administrators and managers need knowledge about the evolving threat environment since it affects how staff are used and how resources are allocated. Analysts need a whole set of data, including the sources of unprocessed data, techniques, and intelligence needs. Information that is just speculation, assumption, hearsay, or potential criminal situations is not considered "actionable."

Dissemination

In the absence of a system that can provide the appropriate data to the appropriate individuals in a manner that adds value to the report's content, an intelligence product is essentially worthless. This objective is what dissemination, or sharing of knowledge, aims to achieve. The various intelligence and information records systems, privacy concerns, information system security concerns, operations security of shared information, dissemination methods, interoperability concerns, and the Global Justice Data Standards are just a few of the topics that could be discussed in relation to dissemination.7 However, the goal of the current discussion is to outline the general tenets and guidelines of intelligence dissemination.

Prior to September 11, "operations security" tended to be the main focus of intelligence dissemination. As a result, intelligence records were not widely disseminated for fear that important information would end up in the wrong hands, endangering the investigation as well as possibly endangering undercover agents, informants, and collection methods. These concerns are still crucial, but the post-9/11 mindset is quite different. In fact, law enforcement aims to provide as many people access to as much information as possible approved those who need it to stop threats from materializing. The basic premise is that the chance of recognizing and halting a danger increases with the number of individuals who get the information. Who is deemed to be an authorized person is maybe the most important issue." Even with this revised perspective, crucial distribution criteria still look for: to safeguard people's civil rights, and when necessary, ensure operational security.The initial rules of distribution provide standards for choosing who should get the intelligence in order to achieve these objectives. The acceptable standard is evaluated using two criteria:

1. Does the person to whom the information is being sent possess the a right to informational knowledge? This depends on the recipient's official position and/or legal right to receive the requested information.
2. Does the person receiving the information really need to know it? The receiver of the information will find it relevant and essential to stop or lessen a danger, or to help with and support a criminal investigation.

The goal of widely disseminating intelligence products that give details on criminal indications and procedures is to make officers aware of these elements while they go about their regular duties. One may generally presume that anybody employed in law enforcement satisfies the right-to-know and need-to-know requirements for these kinds of information. The release of intelligence reports pertaining to a particular criminal investigation that name specific people or groups would be far more constrained. Only the police involved in a specific part of the investigation need to know the material, even if all law enforcement personnel would have the right to know it.

The application of right to know and need to know has changed from the pre-9/11 era in part because of the evolving intelligence philosophy and the acknowledged need to include the private sector and nonlaw enforcement government personnel in the ISE. For instance, anyone in law enforcement has the right to know intelligence. Similarly, even if they are not employed by law enforcement, a member of the National Guard or a Department of Homeland Security intelligence analyst who works in a state fusion center would have the right to know information as a result of their assignments. In an alternative scenario, the corporate security director of a nuclear power station would have the authority to access information that is only relevant to his or her duties as the site's protector.

Once again, a far wider spectrum of law enforcement officials have a need to understand intelligence as a result of the new intelligence philosophy. As previously indicated, the justification is that all cops must be informed of dangersto raise the likelihood that the danger will be stopped. Non-law enforcement personnel's need for specific intelligence should be assessed on a case-by-case basis. For instance, it is highly unlikely that a DHS analyst needs to be familiar with intelligence regarding auto thefts; however, due to the importance of communications between the DHS analyst and other federal agencies like the DEA or

Immigration and Customs Enforcement, the DHS analyst would need to be familiar with intelligence regarding a criminal enterprise smuggling cocaine from Colombia.

3rd Agency Regulation

The Third Agency Rule, as it is often known, imposes still more limitation on the sharing of information. In essence, if an officer obtains information from an intelligence source, that officer is prohibited from sharing that material with a third party without the original source's consent. Officer Adam, for instance, gets information from the Central Fusion Center. Officer Adam must first get approval from the Central Fusion Center before passing the information straight to Officer Baker. With a few exceptions that will be covered later, this is a general guideline that will be expressed or used.uniquely in each agency. Intelligence consumers need to be aware of the Third Agency Rule's regional applicability. Case intelligence and intelligence products are the two categories of intelligence. While intelligence products provide generic knowledge about risks and signs, case intelligence identifies specific individuals. The Third Agency Rule should be seen as intact for case intelligence, but for intelligence products,

The Third Agency Rule may be deemed to be waived. Fundamentally, civil rights do not apply when people or organizations are not identifiable in intelligence products. The precise local applicability of the regulation will once again be determined by a review of agency policy.It should be emphasized that the Third Agency Rule, the right-to-know clauses, and both serve two goals in law enforcement intelligence: 1. to safeguard people's civil rights, and 2. to guarantee the safety of intelligence queries during operations.

Secret Information

There has been a lot of in-depth writing regarding sensitive material. These rules primarily apply to federal law enforcement and the intelligence sector. Most state, local, and tribal law enforcement officers won't have security clearances or access to classified information unless they're part of a fusion center or assigned to a Joint Terrorism Task Force, but having a basic understanding of information classification gives perspective for the discussion that follows. Information that is designated as classified is information that is essential to the security of the United States.

If the procedures for categorizing, storing, granting access, and generally managing this information are not followed, penalties may result, including federal criminal charges.The need of security clearances for SLTLE employees has been hotly contested. Executives and managers in law enforcement contend that access to information concerning risks in their area requires a security clearance. In a report on the same topic, the Congressional Research Service noted that in order to effectively plan, coordinate, and carry out homeland security operations, these officials may require some access to classified information, such as "real time" intelligence information regarding terrorist threats.

Some doubt is expressed in response to the federal authorities' claim that they will provide SLTLE officers all the information they need on risks inside a community.Federal security clearances are not universal, so it's important to be aware of this as well. For instance, a law enforcement official may have a clearance from the Department of Defense due to his or her status as a military reserve, or a DEA officer may have a clearance after a federal investigation. These clearances are often disregarded by the FBI since they provide access to material for

which the FBI is the custodian and was obtained from the Office of Personnel Management as part of an Organized Crime Drug Enforcement Task Force. The reader has to be aware of these problems since they have not yet been addressed. a variety of concerns including security clearances and sensitive information. It is sufficient to state at this time that only those with the proper level of security clearance, which establishes the right to know, are permitted to disclose secret material. Even if the person has the proper level of clearance, the need to know must still be established before distribution.SBU material, sometimes known as "tear line"13 information, is not subject to the same formal limitations, clearances, or consequences as classified information. The SBU designation should be seen more as a professional duty that must be upheld in light of one's other commitments. Although the majority of SLTLE officers won't have security clearances, almost all will have access to SBU data.Despite the fact that SBU material may have previously been classified, its "sources" and "methods of collection" have often been eliminated, declassifying it and converting it to SBU. In some situations, the information's intrinsic sensitivity due to its nature, such as an examination of terrorists' techniques that yields signs of terrorist activity, may justify the SBU designation.Law Enforcement Sensitive and For Official Use Only are the two SBU labels that are most often used in law enforcement, especially at the federal level. In general, LES information may be disclosed to any member of the law enforcement community who has a need to know about it and the right to know. FOUO denotes that the data may be disclosed to anybody who has a need to know and a right to know. For instance, the corporate security director and plant management would be informed of a danger to a nuclear power facility. These are basic guidelines without any actual legal penalties for breaking them. Instead, they provide recommendations for sharing sensitive information and depend on the recipients' skillful judgment to maintain security.There is confusion and inconsistency in the dissemination procedures as a result of the absence of specific guidelines and the broad variety of SBU dissemination labels.

As a result, one of the requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 was to create the ISE, and one of the duties of the ISE program manager was to develop a labeling protocol for SBU information that had a uniform meaning and application throughout the ISE. Given the significance of sharing non-classified terrorism intelligence with state, local, and tribal law enforcement, this is especially true. Information must be shared with others in order to be disseminated, but this information sharing has to be managed in order to safeguard information and prevent accidental dissemination.In order to implement a new information control model dubbed Controlled Unclassified Information, the federal government is replacing the SBU label marks. Compared to SBU labeling, a number of new elements with CUI provide more precise and inclusive guidance. Even Chapter 10 discusses these specifics, it should be highlighted for the sake ofdistribution of the procedures for establishing the right to know for unclassified information that has to be protected in the intelligence process [8]–[10].

Reevaluation

The traditional definition of a "system" is a collection of linked component activities with related goals, where a modification to one component would have an impact on the other components. There is a mechanism behind the intelligence process. The body of knowledge in the other components as it relates to the intelligence inquiry will change as each component, or phase, processes information. Homeostasis, or a "steady state" of the system, must be maintained in this system, just as in any other system. Reevaluation serves the following purpose: To guarantee that all information is processed thoroughly, the intelligence process must be ongoing, with each new

piece of information added to the overall body of new knowledge to help create the most accurate intelligence possible. Reevaluation also acts as a yardstick to gauge the usefulness of the intelligence outputs produced by this procedure. Threats are they correctly identified? Are all parts of the intelligence process working as they should? Can intelligence-based operational interventions be created to be effective?

CONCLUSION

Collection is the act of obtaining unprocessed data in response to needs. Intelligence is gathered using procedures such liaison connections, technological and physical surveillances, human source operations, and searches. The large volume of acquired data must be transformed via processing and exploitation into a format that analysts can use. This is accomplished via a number of techniques, such as decryption, language translations, and data compression. Data entry into databases as part of processing allows for the use of raw data in analysis. The transformation of unprocessed information into intelligence is called analysis and production. It involves combining, assessing, and analyzing the data that is already accessible and creating intelligence products.

The accuracy, validity, and applicability of the data are assessed. The data is rationally combined, contextualized, and used to create intelligence. This covers both "finished" and "raw" intelligence. The term "the dots" is often used to describe individual bits of information that make up raw intelligence. Finished intelligence reports "connect the dots" by contextualizing information and determining its ramifications. The last phase, dissemination, involves providing the customers whose wants led to the need for intelligence with polished or raw information. The three basic forms used by the FBI for information dissemination are intelligence information reports, intelligence bulletins, and intelligence assessments. The Attorney General, the President, and consumers throughout the FBI and in other agencies receive FBI intelligence products every day. These FBI intelligence users use the data to operational, strategic, and policy judgments that might result in the imposition of additional requirements, thereby sustaining the FBI Intelligence Cycle.

REFERENCES

[1] M. Li, C. Lal, M. Conti, And D. Hu, “Lechain: A Blockchain-Based Lawful Evidence Management Scheme For Digital Forensics,” *Futur. Gener. Comput. Syst.*, 2021, Doi: 10.1016/J.Future.2020.09.038.

[2] H. S. N. Hidayati Hj Abas, H. N. H. H. Md Yussof, F. N. Yusra, And P. S. R. Pg Hj Idris, “Effects Of Training And Motivation Practices On Performance And Task Efficiency: The Case Of Brunei Meat Slaughterhouses,” *Int. J. Asian Bus. Inf. Manag.*, 2021, Doi: 10.4018/Ijabim.20211001.Oa5.

[3] Ahmad Perdana Kusuma, “Child Religious Protection For The Muallaf Family In Sibolangit District, Deli Serdang Regency (Analysis Of Child Protection Law No.35 Of 2014 And The Concept Of Hadhonah),” *Britain Int. Humanit. Soc. Sci. J.*, 2021, Doi: 10.33258/Biohs.V3i1.352.

[4] N. S. Sujianti, T. S. Baskara, Bella Ayu D, Nimas Noormala D, And Agus Machfud Fauzi, “Hubungan Agama Dan Pekerjaan Sebagai Psk Di Kembang Kuning Surabaya,” *Maj. Ilm. Tabuah Ta`Limat, Budaya, Agama Dan Hum.*, 2020, Doi: 10.37108/Tabuah.V24i2.347.

[5] L. Fatimatuzzahro And L. Santoso, "Pengaruh Penguasaan Mata Kuliah Etika Bisnis Islam Terhadap Perilaku Konsumsi Mahasiswa," *Serambi J. Ekon. Manaj. Dan Bisnis Islam*, 2019, Doi: 10.36407/Serambi.V1i2.67.

[6] H. S. N. H. H. Abas, H. N. H. H. M. Yussof, F. N. Yusra, And P. S. R. P. H. Idris, "Effects Of Training And Motivation Practices On Performance And Task Efficiency," *Int. J. Asian Bus. Inf. Manag.*, 2021, Doi: 10.4018/Ijabim.20211001.Oa5.

[7] A. Tajabadi, F. Ahmadi, A. Sadooghi Asl, And M. Vaismoradi, "Unsafe Nursing Documentation: A Qualitative Content Analysis," *Nurs. Ethics*, 2020, Doi: 10.1177/0969733019871682.

[8] S. Suhandi And D. Erlita, "Kemiskinan Dan Perilaku Keagamaan Dalam Mengungkap Simbol Keagamaan Pengemis," *Ijtimaiyya J. Pengemb. Masy. Islam*, 2021, Doi: 10.24042/Ijpmi.V14i1.7471.

[9] L. Noviani, N. Diana, And M. Cholid, "Pengaruh Karakteristik Eksekutif, Komite Audit, Ukuran Perusahan, Leverage Dan Sales Growth Pada Tax Avoidance (Studi Kasus Perusahaan Lq45 Yang Terdaftar Di Bursa Efek Indonesia)," *J. Ilm. Ris. Akunt.*, 2018.

[10] S. Alibhai, Z. Jewell, And J. Evans, "The Challenge Of Monitoring Elusive Large Carnivores: An Accurate And Cost-Effective Tool To Identify And Sex Pumas (Puma Concolor) From Footprints," *Plos One*, 2017, Doi: 10.1371/Journal.Pone.017206.

CHAPTER 7

CONCEPT OF INTELLIGENCE-LED POLICING

Pujari Sudharsana Reddy, Assistant Professor, Department of Finance, CMS Business School,
JAIN (Deemed to-be University), Bangalore, India,
Email id-pujarisudharsana_reddy@cms.ac.in

ABSTRACT:

The concept of Intelligence-Led Policing (ILP) is a law enforcement strategy that involves using intelligence analysis and information to guide and prioritize police operations, investigations, and resource allocation. This approach emphasizes the use of data and analysis to identify crime patterns and trends, as well as to anticipate potential criminal activity and threats. The ILP model is based on the idea that intelligence analysis can be used to support crime prevention and control efforts more effectively than traditional, reactive policing approaches. It involves the collection and analysis of data from various sources, including crime statistics, offender databases, community surveys, and other intelligence sources. This data is then used to develop intelligence products, such as crime maps and trend analyses, that inform decision-making at all levels of the organization.

KEYWORDS:

Law Enforcement Intelligence, Open-Source, Intelligence, Situational Awareness, Suspicious Activity, Tactical Response Alternatives, Threat Assessment.

INTRODUCTION

The adoption of intelligence-led policing by American state, local, and tribal law enforcement agencies in the post-9/11 period was proposed by participants in the 2002 intelligence summit sponsored by the International Association of Chiefs of Police and the Office of Community Oriented Policing Services. ILP was intended to be a mechanism for information exchange that would help law enforcement agencies recognize dangers and create countermeasures to stop such threats from materializing in American communities.1 This was supported by a suggestion to implement ILP in the National Criminal Intelligence Sharing Plan2, which has received widespread support from law enforcement officials and been reflected in new programs by the U.S. Departments of Justice and Homeland Security [1]–[3].

The problem, however, is that different people have different ideas about how to use the ILP notion. There is, in fact, a movement to embrace ILP without a widely acknowledged definition or a manual of practice. The purpose of this talk is to offer an understanding of ILP in the context of current advancements in law enforcement intelligence, combining the most widely used applications of ILP, and concentrating in particular on the procedures needed to put the idea into practice.To successfully implement ILP, it is essential to have a realistic awareness of the present intelligence capabilities throughout the whole spectrum of American law enforcement, as well as a flexible strategy that can be tailored to the requirements and capacities of both large cities and counties and small departments as well as rural towns.

Conceptual Underpinnings

According to the NCISP, the main goal of intelligence-led policing is to provide decision-makers in public safety the knowledge they need to save the lives of our residents.3 How does one do this? ILP does not have a handbook of practice since, like community policing, it must be customized to the specifics of each agency. ILP may be defined as an underlying ideology that guides how intelligence functions within the framework of a law enforcement agency. ILP offers strategic integration of intelligence into the overarching objective of the business, as opposed to just being an information clearinghouse that has been added to it.

To guarantee that the ILP idea is integrated with an agency's aims and functions, as well as its capabilities and the characteristics of both the agency and the jurisdiction it serves, an inclusive development process must be used to construct it. It is not an additional duty for the agency, but rather a modification to better manage cross-jurisdictional risks and severe crime that affects communities. There are no quick cuts in the process; it calls for innovation, organizational reflection, and a readiness to change the structure of the company. The explanations that follow provide a framework for comprehending the many facets of the ILP idea. Building on this knowledge, the following explores the organizational dynamics and policy requirements for successfully implementing ILP [4]–[6].

DISCUSSION

Defining ILP

Although the elements of the majority of definitions are the same or at least comparable, there is no one definition of ILP that is widely acknowledged. Two definitions of ILP were produced by the Bureau of Justice Assistance in 2009 in collaboration with the Global Justice Information Sharing Institute. The conceptual foundation of these definitions was stated as building on the lessons of Problem-Oriented Policing and CompStat and applying these principles to a threat-based environment of multijurisdictional complex criminality. The conceptual framework includes current law enforcement intelligence projects, such as the National Information Exchange Model, the Global Justice Information Sharing Initiative, and the functioning of the Regional Information Sharing System.

According to the BJA, ILP is as follows:

a. ILP may be characterized as a collaborative strategy to law enforcement that combines increased intelligence operations, information sharing, and problem-solving policing.
b. However, BJA constrained the concept to the following for the purposes of their document:
c. ILP is the executive application of the intelligence cycle to support proactive decision-making for resource allocation and crime prevention.5 Police executives must have clearly defined priorities as part of their policing policies in order to properly execute this business process.
d. On top of these pillars, the author offers the following operational definition of ILP:
e. gathering and analyzing data on crime and factors that contribute to it to produce an actionable intelligence product that will help law enforcement create tactical responses to threats and/or long-term plans for dealing with new or evolving threats.
f. A greater comprehension will result by breaking the term down into its essential parts.

Collection

The gathering of raw data that may be utilized for analysis is a crucial step in the intelligence process. Focused data collection is necessary to recognize and comprehend emerging dangers in a jurisdiction. Based on information obtained from police, secret sources, and people in the form of tips, leads, and Suspicious Activity Reports, this emphasis is often chosen by an analyst who will establish the intelligence needs. The important thing to remember is that collection looks for unprocessed data within certain bounds, which is necessary for efficient analysis.

Analysis

The scientific method of issue resolution is analysis. To specify needs and foresee dangers, it uses deductive and inductive reasoning. Although analysis is typically qualitative for both tactical and strategic analysis, it may be quantitative in certain cases, particularly for strategic analysis. Analysis, according to the Office of the Director of National Intelligence (ODNI), is "a process in the production of intelligence in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions."6 The ODNI goes on to make the following distinctions between raw information and analyzed information:

a. Unprocessed data:
b. Offers suggestions
c. Increases awareness
d. Analysis of the data
e. Enables comprehension
f. Reduces ambiguity
g. Better choices are possible

The analytical process is synergistic, generating knowledge from a variety of unprocessed data and giving it a unified meaning. Analysis is also used to define "intelligence gaps" and "requirements."

Crime and the Prerequisites for Crime

ILP focuses on threats, making it crucial to identify local and regional factors that contribute to the emergence and development of crime. The emergence of extremist groups that advocate violence or hatred; conflict within a region that may be a breeding ground for violence between racial, ethnic, or religious groups; and a variety of other distinctive qualities that are particular to a given community, such as proximity to an international border, are just a few examples of these variables. It is crucial that the data gathered shed light on the presence of the circumstances, the causes of their escalation, and the people who could play a key role in exploiting them for criminal or terrorist activity.

Effective Intelligence

As former FBI Executive Assistant Director for Intelligence Maureen Baginski put it, intelligence influences the choices made by law enforcement officials. Fundamentally, for intelligence to be helpful, it must provide guidance for creating and carrying out plans. An intelligence report must allow a law enforcement organization to execute some kind of operation that will either reduce or prevent crime. This implies that operational reactions to threats and strategic planning for them will be driven by the information that an analyst produces.

A law enforcement agency has the necessary knowledge to create preventative actions to threats when it possesses actionable intelligence. A neighborhood or area may be the subject of immediate threats in the report, as well as threats from wanted individuals or threat tactics that law enforcement officials should be aware of. The agency must be able to utilize the information in some capacity is the fundamental tenet. Additionally, actionable intelligence should make sure that the proper information is given to those who can take action to counter the danger.

Threats: Tactical Responses

Actionable intelligence is a subset of tactical and strategic intelligence. Numerous tactical actions, ranging from stepping up mass transportation security measures to keeping an eye out for suspicious activity at a prospective intelligence target, may be judged acceptable depending on the situation at hand. The main focus of tactical intelligence is prevention: developing methods to remove or lessen short-term and immediate dangers by using information on terrorist and criminal threats. What kind of operational reaction can be produced utilizing this information? is the quintessential question of tactical intelligence."

Threats in a society often evolve over time, which is why strategic planning in relation to emerging or changing threats is important. Strategic analysis is largely utilized for planning and resource allocation to comprehend how the threat landscape is evolving. Decision-makers are informed about the evolving nature, traits, and tactics of threats as well as newly emerging threat peculiarities so they may create reaction plans and reallocate resources. A strategic study may reveal if a new clinic that performs abortion operations may be threatened by extremist organizations in the event that, for instance, the neighborhood has never had issues with right-to-life extremists [7], [8].

Plans may be created utilizing strategic analysis to either stop a danger from emerging or minimize it if it does. The query, "What future plans and resources must be cond, and how must they be cond, to meet threats defined in the strategic analysis?" serves as an apt exemplification."The British Experience: Fundamental Perspectives on the History of ILPContext is necessary to improve our understanding of ILP. One has to be aware of the constraints placed on the adoption of the British National Intelligence Model for U.S. law enforcement as well as the dynamics inside the American law enforcement environment that will affect the deployment of ILP.

The Current State of American Law Enforcement Intelligence,

Perspective 1:

According to some data, ILP may contribute significantly to community security by preventing terrorism, violence, criminal extremism, and complex crime. The author concurs. The implementation of ILP, however, is the issue. The issue is that American law enforcement is not structurally nor substantively prepared to support the ILP infrastructure. At one conference, a powerful ILP enthusiast pushed law enforcement authorities to "just do it." Like a structure, the foundation must first be established; the majority of American law enforcement organizations have collected some bricks, but the foundation is still far from being finished.

This author has trained literally thousands of law enforcement officers from hundreds of agencies on intelligence over the last 20 years. At all governmental levels from every state and the majority of the territories.7 However, this only makes up a minor percentage of American law

enforcement. What has been discovered is that intelligence-capable agencies are the exception, not the norm. Additionally, what is often referred to as an intelligence unit or capability in most agencies is really more of a hybrid organizational entity that may be doing criminal analysis and/or supporting investigations. Despite the fact that they are distinct, crime analysis and intelligence analysis are frequently combined.8 In other situations, there may be a number of intelligence capacities that are purpose-specific, such as gang intelligence, drug intelligence, and/or organized crime intelligence. Once again, a lot of these tasks resemble investigative support more than intelligence.

Historically, the great majority of law enforcement organizations in the United States have not been equipped with intelligence capabilities or training in the function and procedures of intelligence; instead, it has been assumed that only the larger organizations need such capabilities.The legacy of the agencies with an intelligence capability has proven a little difficult. Early law enforcement efforts often lacked analysis. Instead, they maintained dossiers on people who were "suspicious" or who were considered to be dangers of some kind, sometimes based on subjective rather than objective threat assessments. As a result of federal civil rights laws, numerous agencies faced legal action in the 1960s and 1970s for keeping intelligence files on individuals who had not yet committed a crime but were associated with practices and philosophies that were judged unusual or un-American. The legacy of these methods continues even though they are largely no longer used, as seen by the widespread mistrust that the public still has for modern law enforcement intelligence operations.

In addition to civil rights concerns, the intelligence role was sometimes ill-defined and usually kept to itself when it came to state and local law enforcement actions. There were few analysts and many of them lacked proper training; they often acquired the designation of "analyst" by tenure rather than competence. It was sometimes impossible to identify what the intelligence unit, as an organizational entity, added to the overall purpose of law enforcement. Although there were undoubtedly some exceptions to this description, it was the norm for the majority of American law enforcement intelligence programs. Although a lot has changed, history is still a challenging barrier to overcome.

In particular, this was the result of the IACP/COPS Office intelligence summit, the efforts of the Global Intelligence Working Group, the release of the NCISP, the creation of the Criminal Intelligence Coordinating Council, the growth of intelligence fusion centers, and the wide variety of new law enforcement intelligence training programs. This change started in the post-9/11 era, leading to an increased awareness of intelligence and growing intelligence capacities. However, this is far from being all-inclusive. For the majority of SLTLE agencies, the next step of becoming active participants in the Information Sharing Environment is really still very far.

Although more organizations are developing some kind of intelligence capability, the numbers are still rather modest. Additionally, a lot of agencies, including Crime Analysis, evaluate the interaction effects and covariance of explicit factors of crimes that have already happened in an effort to identify a perpetrator's methods in an effort to clear the crimes and stop similar ones in the future by catching the offender. Threats from terrorism, criminal extremism, or organized crime are dealt with through intelligence analysis, which examines information that suggests a threat, identifies intelligence needs, and employs target and vulnerability assessments with the aim of averting the threat's realization.

Major organized crime is handled by SOCA, an organization with a strong intelligence component. Threats against the United Kingdom are handled by the United Kingdom Security Service. The main focus of national security is terrorism, but it also includes espionage and domestic intelligence. Outside of the UK, intelligence is gathered by the Secret Intelligence Service. Because of conflicting demands, including rising violent crime rates and controlling call volume, moderate-sized departments either do not recognize the need for an intelligence capability or believe they cannot justify allocating resources to establish one. The chief executive and others in the chain of command for the great majority of these organizations sometimes rely on historically based notions about intelligence and are unaware of the quick development and importance of the current law enforcement intelligence role. These characteristics make it difficult for these organizations to embrace ILP. The problem isn't that agencies don't want to take part in fusion centers and the ISE; rather, they often fail to see the benefits in light of other obligations. Due to these problems, it's important to reiterate that the majority of American law enforcement agencies lack the infrastructure necessary to deploy ILP. First, a foundation of intellect must be built.

Perspective 2: Issues in Applying the British National Intelligence Model to the U.S. Legal Action

We often go to other models when attempting to apply a new idea in an effort to figure out what works and embrace that strategy. In terms of law enforcement intelligence, British law enforcement has a longer and more advanced history than American law enforcement. To cope with organized crime, narcotics, and other complicated crimes specific to their jurisdictions, all provincial British constabularies have maintained some kind of intelligence section for a good amount of time. To combat hooliganism during soccer games, for instance, several British constabularies maintain a Football Intelligence Unit. In order to combat the sharp rise in international drug trafficking and related crimes like money laundering, the National Drugs Intelligence Unit was established at the national level in the 1980s. The service was dependent on employees who were delegated from police forces throughout England and Wales. To combat all facets of organized crime, the agency was enlarged and given the name National Criminal Intelligence Service in 1992. The European Union's shifting political landscape, which included, among other things, the elimination of immigration and customs inspections for people traveling between EU member nations, had a special impact on how the NCIS developed. A new organization, the Serious Organized Crime

Crime Agency, which combined the NCIS with the nationwide Crime Squad, a nationwide investigative organization, and the drug enforcement operations of Her Majesty's Revenue and Customs Service.The British government started applying a business plan mentality for all aspects of public service in the 1990s. It had two basic goals: either "privatise" certain government services, or use a corporate model for the remaining services. The decision had a broad impact; for instance, BritRail, the British National Rail Service, was split up and sold to several private businesses. Similar to this, municipal governments "privatised" services including cleaning and car maintenance. In April 2007, CENTREX developed into a division of the National Police Improvement Agency, taking over responsibility for England and Wales' national police training program. The key fact is that practically every component of British government, including the police, was mandated to follow business procedures.

The British National Intelligence Model12 was created by NCIS as part of this movement in the late 1990s with guidance from Her Majesty's Inspectorate of Constabulary11. It was initially released in 2000 and formally adopted as accepted policy by the British Association of Chief Police Officers in 2002. The NIM adopted the government's strategy of dealing with crime control via the use of a business process model.When the NIM was adopted by ACPO, it meant that the chief constables of the 43 provincial police forces in England and Wales had also decided to accept it and modify it to fit their policing requirements.13 The intelligence division of the constabularies primarily deals with significant organized crime, football hooliganism, violent crime, and unusual locally recurrent criminal issues.

It has not been simple for the British police to transition to ILP in compliance with the NIM. Because it called for a reallocation of resources and included a sizable analytical component to each police force, the idea was not well understood by many. Many people criticized the NIM for being an obscure model that generated a lot of data and new procedures while being expensive and not offering excellent value for the money. As one would expect, some police agencies have embraced the idea considerably more openly than others, who, in certain instances, are utilizing the NIM primarily in name only. As a result, its complete implementation has been much longer than planned.

Despite these issues, the NIM has also contributed to significant accomplishments. The United States may use many of the NIM's lessons, and the HMIC14 has a special collection of model practices that includes analytical models. With certain exceptions in the mostly bigger U.S. major cities and counties, American law enforcement agencies lack the expertise in law enforcement intelligence necessary to use British ILP on a widespread scale. A different viewpoint will aid in better comprehension. As was previously indicated, the consolidation of several smaller police agencies in the 1960s led to the creation of 43 police forces in England and Wales. One of these constabularies, which is the smallest, has around 900 sworn cons who patrol vast geographic regions with both urban and rural aspects. Most agencies have between 1,200 and 1,600 sworn employees. Despite not being a national police force, all agencies must adhere to national standards for operations, remuneration, promotion, and training. It is true that employees may move lateral between the constabularies.

These police forces all have the capacity to employ analysts and the flexibility to transfer staff to fulfill the requirements of a completely new effort like ILP, given their size and their appropriate operating budgets. This is not intended to imply that the constabularies have an abundance of resources or personnel; rather, one finds that huge agencies have a lot more flexibility, resources, and broad experience than the tiny departments that are more common in the United States. The British police service was also better equipped to embrace the NIM and ILP since it has a long history of conducting sophisticated law enforcement intelligence analysis.

Comparing Law Enforcement Intelligence in the U.S. with the U.K.

The over 18,000 law enforcement units in America, the most of which have 10 or less sworn officers, have different policing requirements from state to state as compared to the British police system. With a few exceptions in the form of short-term government subsidies, they often operate on tight budgets, with all of their funding generally coming from local sources. Federal guidelines and suggestions are often not enforceable unless they are expressly linked to unique grant requirements.

When comparing U.S. and U.K. policing, it is unreasonable to assume that the fundamental principles of the NIM, as found in the United Kingdom, and, by extension, the ILP, can be successfully implemented in the United States on a short-term wholesale basis due to these stark differences and the vastly different histories of law enforcement intelligence. In America, we must begin much more fundamentally. It is necessary to create an effective ILP model that is adaptable to the structure of American law enforcement.

ILP should first be seen as a concept rather than a procedure. In fact, American law enforcement organizations should adopt this mindset in order to create fresh, intelligence-based procedures that properly balance the responsibilities, traits, and assets of each organization. The knowledge gained by community policing might be a useful manual.Creating the framework for information gathering to manage risks within a jurisdiction and creating the organizational infrastructure to support the ILP program are the two developmental tasks needed to establish ILP in a law enforcement agency. We shall talk about them.

Problem-solving, ILP, and Community Policing, and CompStat

Police executives often express worry that the move toward ILP, which is mostly due to heightened terrorist obligations, may necessitate a shift in resources away from community policing. The issue then becomes how community policing and ILP are combined. It will be clear that the two have more similarities than one may anticipate. Strong community ties are necessary for new ILP aspects. The police will still have a crucial role to play in combating crime and obtaining community support. It is also more important than ever to keep law enforcement and the community in constant communication given the rise in social unrest brought on by the homeland security environment.

Many law enforcement professionals have acquired abilities via community policing that directly complement new ILP responsibilities: One of the key contributions community policing makes to this difficulty is the scientific approach to problem solutions, environmental scanning, effective public communications, fear reduction, and community mobilization to address issues. The following were the factors that the NCISP observed:Over the last ten years, hundreds of community-policing officers have developed strong and fruitful bonds with the people they serve in parallel with federally sponsored measures to strengthen intelligence collection.

Information and intelligence sharing is closely tied to the advantages of these relationships: Officers of the COP have quick and unrestricted access to neighborhood and local information as it arises. Citizens are aware of COP officers and actively seek them out to get fresh information that might aid in preventing crime or finding long-term solutions to problems. Positive ties between COPs and citizens encourage a constant and dependable flow of information between the two. It is time to make the most of community policing initiatives' capacity to act as a conduit for information originating locally in order to stop terrorism and all other crimes.

The functions that community policing plays in the intelligence process are also described in the Office of Domestic Preparedness Guidelines for Homeland Security. They consist of the following:

1. Supplying community policing contacts with examples and information that might help in the identification of terrorism in order to raise community awareness of the actions, behaviors, and occurrences that qualify as "suspicious."

2. Organizing community gatherings to highlight public awareness, alertness, and preventative techniques.
3. As they are, or should be, aware of ways to communicate information to community policing officers, it is important to make sure that community people are aware of the ways and procedures for conveying observed data to police officers and police organizations.
4. Promoting proactive policing, prevention, and strong collaboration between the police and the community.

These elements prompted the creation of ILP as the guiding principle for how intelligence functions within the framework of a law enforcement agency. ILP offers strategic integration of intelligence into the overarching objective of the business, as opposed to just being an information clearinghouse that has been added to it. ILP expands community policing in many ways by using techniques and methods that have been refined through years of testing. This notion is shown by a few analogies. Community policing and ILP both depend on these actions:

I. Information Control
II. Community policing: Information obtained from the populace aids in defining the specifics of neighborhood issues.
III. ILP—Input of information is a necessary component of intelligence analysis.
IV. Two-way Information Sharing with the Public
V. Community policing: Information regarding criminals is gathered from the general population. Public awareness of important facts promotes crime prevention and fear reduction.
VI. ILP – Information from public communications may be useful for the intelligence cycle. Communicating vital information to individuals may assist avert a terrorist attack and, like community policing, will lessen anxiety when dangers are specified with precise facts.

Research Data Analysis

Community policing: A crucial component of the CompStat18 process is crime analysis.The key component of threat management is intelligence analysis, or ILP.Community policing and problem-solving techniques are utilized to resolve issues in the community that are antecedents to crime and disturbance.ILP The same procedure is used to intelligence to balance elements relating to the trafficking of illicit goods and susceptible targets.

The remarks made by FBI Director Robert Mueller in reporting a rise in fear about terrorism at significant national events during the summer of 2004 serve as an example of the significance of these elements. Director Mueller said, alluding to images of seven terrorist suspects allegedly present in the country: "We need the American people's support." must assist when requested, since agents will be contacting numerous people around the country to obtain data and intelligence... for those seen above, to be mindful of your surroundings and report anything unusual to "BOLO". Have you seen them in your local areas? Have you heard rumors that someone may be aiding their evasion? Do you have any notion of their possible location? If so, please step forward for us.

These terms capture the functional core of the interaction between community policing and law enforcement intelligence. ILP necessitates an effort investment by the community and all

organization-related parts, much as community policing. The days of intelligence agencies working covertly are long gone. According to the tenets of the ILP philosophy and the NCISP standards, law enforcement intelligence is an organizational duty that depends on a mutually beneficial connection with locals [9]–[11].

CONCLUSION

In general, the idea of "Intelligence-Led Policing" signifies a substantial change in how law enforcement organizations approach crime prevention and control. These organizations may more successfully target criminal activities and prevent crime by employing intelligence analysis to direct their operations, while also fostering closer bonds with the communities they serve. In order to prevent and discourage crime, the ILP strategy also uses proactive police techniques including targeted enforcement and community involvement. ILP may aid in preventing criminal behavior from happening by concentrating on high-risk regions and people, as well as lowering the overall incidence of crime. In recent years, the idea of ILP has been widely accepted, and many law enforcement organizations have started using this strategy to enhance their efforts at crime prevention and control. However, well-trained staff, efficient data collecting and analytic methods, and a strong commitment to community participation and partnerships are necessary for the successful implementation of ILP.

REFERENCES

[1] J. W. Coyne and P. Bell, “Strategic intelligence in law enforcement: A review,” *J. Policing, Intell. Count. Terror.*, 2011, doi: 10.1080/18335330.2011.553179.

[2] J. W. Coyne and P. Bell, “The role of strategic intelligence in anticipating transnational organised crime: A literary review,” *Int. J. Law, Crime Justice*, 2011, doi: 10.1016/j.ijlcj.2011.02.003.

[3] M. Maguire and T. John, “Intelligence led policing, managerialism and community engagement: Competing priorities and the role of the national intelligence model in the UK,” *Polic. Soc.*, 2006, doi: 10.1080/10439460500399791.

[4] N. Keane and M. E. Kleiven, “Risky Intelligence,” *Int. J. Police Sci. Manag.*, 2009, doi: 10.1350/ijps.2009.11.3.134.

[5] Z. Alach, “The Emperor is Still Naked: How Intelligence-Led Policing Has Repackaged Common Sense as Transcendental Truth,” *Police J.*, 2011, doi: 10.1350/pojo.2011.84.1.523.

[6] J. H. Ratcliffe, *Intelligence-led policing*. 2012. doi: 10.4324/9780203118245.

[7] B. Rider, “Intelligent investigations: The use and misuse of intelligence - A personal perspective,” *J. Financ. Crime*, 2013, doi: 10.1108/JFC-04-2013-0027.

[8] T. E. Engells and W. H. Adcox, “Conversations with commanders: a tool for organizational learning.,” *J. Healthc. Prot. Manage.*, 2010.

[9] J. G. Carter and S. W. Phillips, “Intelligence-led policing and forces of organisational change in the USA,” *Polic. Soc.*, 2015, doi: 10.1080/10439463.2013.865738.

[10] H. Gu, Y. Guo, H. Yang, P. Chen, M. Yao, and J. Hou, "Detecting Pickpocketing Offenders by Analyzing Beijing Metro Subway Data," in *2019 4th IEEE International Conference on Big Data Analytics, ICBDA 2019*, 2019. doi: 10.1109/ICBDA.2019.8712833.

[11] O. Guéniat, "In Vestige @ and Police Management?," *Polic.*, 2019, doi: 10.1093/police/pax044.

CHAPTER 8

COMPARING ILP AND COMPSTAT

Dr. V Y John, Assistant Professor, Department of Finance,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email id-dr.vy_john@cms.ac.in

ABSTRACT:

Intelligence-Led Policing (ILP) and CompStat are two popular law enforcement strategies used to prevent and control crime. While both approaches are data-driven and focused on proactive policing, they differ in their emphasis and implementation. ILP is based on the collection and analysis of intelligence data to identify criminal patterns and trends. This information is then used to guide police operations, investigations, and resource allocation. ILP emphasizes the use of intelligence to prevent crime and to disrupt criminal organizations and networks. CompStat, on the other hand, is a management model that uses data to identify crime hotspots and to hold police commanders accountable for crime reduction in their jurisdictions. CompStat meetings are held regularly to review crime data, identify trends, and develop strategies to reduce crime.

KEYWORDS:

Ilp, Compstat, Policing, Crime Reduction, Data-Driven, Community Policing, Crime Analysis, Performance Measurement.

INTRODUCTION

The CompStat procedure, which has its roots in the New York Police Department, has been a crucial tool for law enforcement organizations to quickly and efficiently address crime patterns. Numerous major and medium-sized law enforcement organizations across the United States and in numerous other countries have implemented the procedure in a variety of ways with continuous effectiveness. CompStat is a crime-management tool that highlights the benefits of creative solutions to law enforcement issues, and it is supported by a strong body of research. Many have said that ILP and CompStat are interchangeable as law enforcement officials struggle to comprehend ILP. There are undoubtedly many parallels that will aid in the acceptance of ILP, but there are also significant fundamental distinctions that must be acknowledged. The main issue is that a variety of functional variables account for the differences between CompStat and ILP.

ILP is concerned with "all crimes and all threats," as is evident; yet, the kind of crime that ILP concentrates on is often multijurisdictional and frequently complicated criminality, such as criminal enterprises [1]–[3].The benefit of CompStat is its timely analysis of event records that identifies emergent, substantial crime series or severe crime within a jurisdiction. The analysis of crime reporting data can yield crucial data, such as geographic parameters and modus operandi, that can be used to forecast future criminal incidents, assist in problem-solving, and provide descriptive data, such as behaviors, targets, and criminal instruments, that operational units may use to catch offenders, stop criminal activity, or change environments that encourage crime.

ILP, on the other hand, concentrates more on potential crimes than actual ones. The threat data may come from Suspicious Activity Reports submitted by officers, tips and leads provided by the local community, significant changes in the suicide myographic of a region, or other indicators that ostensibly point to the existence or emergence of a serious multijurisdictional crime problem. The intelligence analyst must specify intelligence requirements, which include the data the analyst needs to more precisely identify the danger and the elements contributing to the threat's progression, rather than analyzing information and evidence gathered from incident reports. Similar to how ILP need feedback on information analysis whether it be crime analysis or intelligence analysis to be continually aware of any issues or dangers that may be faced during a shift, both community policing and ILP are ineffective without it.

On a similar issue, the FBI created a set of interview questions for those who may know anything about terrorism in the wake of the terrorist events of September 11, 2001. Some people who were in the country on visas were questioned with the help of state and municipal law enforcement. Based mostly on the viewpoint of local government officials, there was a variety of reactions. Despite this, the questions were also meant to provide police knowledge and information. The protocol questions and more details are available in General Accounting Office. Homeland Defense. Interviewing Foreigners Project of the Justice Department after September 11, 2001. Prepare a report for congressional committees. GAO-03-459 report, April 2003.

CompStat and ILP are both focused on prevention and are powered by an information flow that rises from the line level. Street cops get intelligence awareness training since it is very likely that they may come across situations and individuals that might indicate a danger or point to the existence of a criminal organization.

To consistently relay such information to the intelligence unit for inclusion in the Intelligence Cycle for analysis, the patrol officer has to get the necessary training. Similar to community policing, this calls for additional duties for patrol officers and organizational flexibility to allow police to investigate previously unrecognized aspects of crimes and community issues. Although there are some essential similarities, ILP's methods and emphasis are much different from CompStat's and more challenging due to the variances in the raw data. The basis for the topics that follow is understanding these distinctions and, more importantly, the function that ILP serves [4]–[6].

DISCUSSION

Ethical Issues

The focus on ethical decision-making is another significant aspect that both community policing and ILP have in common. The necessity for ethical decision-making in community policing was driven, among other things, by the need to build community and police trust. The public would not contribute the vital information required for crime control without this confidence. Similar but more extreme ethical decision-making is required in ILP.

Because of worries about the kinds of data that law enforcement is gathering and how Concerns have been raised that law enforcement could breach people' rights in their search for terrorists due to the retention of information in records.

Due to these worries, the law enforcement intelligence function must maintain an unwavering sense of moral judgment and appropriateness.

ILP and civil rights

Maintaining confidentiality and defending people's civil rights provide a special problem while dealing with ILP. Crime analysis and CompStat both have their own unique set of legal guidelines. CompStat often deals with aggregate information on criminal occurrences and their characteristics. Since no specific persons are identified in such analyses, the data does not have any civil rights attached to it. If the crime analysis is primarily concerned with identifying specific people, the identification is the consequence of information gathered during the criminal investigation that provided probable cause for an arrest. Further evidence gathering is governed by the law of criminal evidence and process, and the information is kept in the law enforcement agency's records management system, which provides flexible regulations for preserving records of suspects, witnesses, and victims.

On the other hand, as was already said, ILP deals with threats and circumstances that could enable the threats. There are no significant civil rights problems at the moment. However, the information is classified as "criminal intelligence information" and may only be entered into a separate "criminal intelligence records system," not the RMS, as the intelligence process identifies individuals and organizations for which there is only a reasonable suspicion that they may exploit the circumstances to commit criminal acts in the future. Therefore, it is essential that the requirements of 28 CFR Part 23 be followed.23 If not, the law enforcement agency risked civil penalties [7]–[9].

The point to note for the current discussion of ILP is simply that there are significantly different rules for the collection, retention, and dissemination of "criminal intelligence information" compared to "criminal investigation information."

Beyond the information management differences, there are conceivably different methods of analysis when individuals are identified as either intelligence targets or witnesses. As a result, an exclusive records system, supporting rules, and training on the right way to handle information for ILP must be created.

Technically, 28 CFR Part 23 only applies to multijurisdictional criminal intelligence records systems run by state, municipal, and tribal law enforcement agencies and supported by the federal government. However, in reality, it must be taken as given that all state, municipal, and tribal agencies must comply with 28 CFR Part 23 for the following two reasons:

1. The NCISP advises that these recommendations be adopted by all organizations as a national standard of good practice and
2. If a civil rights lawsuit is filed against an agency for the kinds of information being kept in a criminal intelligence data system, precedent in federal civil rights cases implies that adherence to the federal rules may be an affirmative defense.

Targets may not always be obvious to a community. Does it seem like East Lansing, Michigan, is a terrorist target? The Michigan State University's mink research facility was damaged by a fire staged by the Animal Liberation Front in 1992, costing more than $2 million. A fire at MSU's Agricultural Hall on December 31, 1999, cost $700,000 to repair and ruined years of study. The Earth Liberation Front took ownership and declared war on genetic research.

The danger assessment and the need for intelligence will be covered later.

Community Education

Public education is essential for successful ILP, as was previously mentioned. The knowledge gained by community policing offers significant insights. distinct public education projects must be offered to each of the many distinct groups that make up the public. For instance, what does the organization want to achieve through a campaign of public education: lessening fear? building up volunteers for the police force? easing tensions within the community, such as the seeming hostility against the Muslim community? Is the only objective to enlighten the public about signs of terrorism to help in prevention? The crucial thing to remember is that the public education program needs a particular purpose.

A similar approach may divide the populace into distinct target audiences by stratifying the community. Who in the neighborhood should be the focus of an education program: the corporate sector? church and civic organizations? Citizens' Police Academy graduates? government workers who are not law enforcement? educators and learners? the general public?demographically distinct communities' segments?

The demands of various community sectors may vary. For instance, because the private sector owns around 85% of America's vital infrastructure, a unique public education campaign may concentrate on threat-related concerns for this specific group. The CPA grads, on the other hand, may get entirely different public education since they might be prepared to serve as volunteers in times of emergency or high alert. However, a distinct public education program would be targeted at a certain racial or religious group inside a city. The objectives of the community's many groups vary. The commercial sector in this instance hardened prospective targets, the

To help the police meet the growing demand for their services and the ethnic community to learn more about shady characters and their activities, CPA graduates.These groups might be further subdivided, especially if the community has specific goals. Different threats may target a nuclear plant, a telecommunication switching station, a meat processing plant, or a university genetic research laboratory, for example.

The business community, for example, may be divided into different segments. The law enforcement agency will need to conduct a threat assessment to fully understand the nature of the threat within the community as well as to understand the agency's intelligence requirements. Programs for community education should also have a clear goal in mind. All public education campaigns should include five elements linked to the intelligence function, whether the goal is to lessen anxiety or mobilize support for volunteer work:

1. Be able to observe.
2. Identify suspicious behavior.
3. Be able to report.
4. Understand what has to be reported.
5. Understand what comes next.

Law enforcement must provide a framework of information in order to optimize the quality and quantity of information offered by the community. In this respect, §§ 5-1 and 5-2 indicate a variety of issues that may be integrated into a public education program from both a subject and an outcome standpoint. The more that law enforcement can educate the community, the more robust the input from the community.

Volunteers from the community who work with law enforcement

Community people often inquire as to what they can do to support anti-terrorism efforts. Being a volunteer for the police force is an essential component. Experience has shown that neighborhood volunteers often bring specialized knowledge and may help the organization save money. When citizens can do jobs that would otherwise need to be done by others, money may be savedconducted by a law enforcement officer; as an example, the Civil Defense Battalion of the Austin Police Department deploys volunteers to carry out these objectives.

Naturally, when volunteers are working on behalf of a law enforcement agency, an organization has to design a method of screening them as well as a framework for their work agreement and administrative controls. In this sense, Volunteers in Police Service (VIPS) is a valuable resource.27 The VIPS website offers a wealth of materials, guidelines, and other information that may help a law enforcement volunteer program run smoothly.Volunteers with distinctive professional backgrounds may be especially beneficial to the intelligence function. Lawyers, accountants, those with knowledge of tracing land titles, academic researchers, and academics are a few examples of professionals that might provide valuable support to the intelligence function. Of course, all such volunteers must be subject to background checks and nondisclosure agreements. In a perfect world, the law enforcement organization would be able to tell the citizen about the information they reported. In the intelligence environment, this is often not possible; yet, when feedback is given to the citizen, it functions as positive reinforcement.

CONCLUSION

According to information found in a current report from the Office of Community Oriented Policing Services: In order to proactively detect possible threats and foster an atmosphere of safety, law enforcement has been urged to work with the community as a partner in community policing over the last 20 years. Its focus on problem-solving has produced more efficient ways to solve issues with crime and social disorder. The community policing ideology is well-positioned to play a crucial part in the 21st century's efforts to prevent and react to terrorism as well as to lessen public anxiety. The wise executive will investigate these possibilities as part of a comprehensive, neighborhood-wide homeland security plan. The necessity to welcome all members of the community takes on even more importance in light of worries about terrorism and Islamic extremism. According to the Muslim Public Affairs Council, a collaboration between politicians and the American Muslim community will ultimately be necessary for U.S. counterterrorism operations.

Establishing and Using Intelligence-Led Policing

outlined the idea of and problems with intelligence-led policing. This will outline the procedures and components necessary to establish ILP in a state, municipal, or tribal law enforcement agency, building on those notions. Because ILP is conceptual in nature, it must be created to specifically address the demands of a certain agency. The fact that a broad variety of resource and environmental factors will also affect implementation complicates things. It's crucial to keep in mind that there isn't a single ILP model that can be integrated into an organization. Instead, as will be shown, there are methods that may be used to pinpoint an agency's intelligence requirements before creating the procedures and guidelines needed to make ILP work for each department.

In essence, intelligence is the management of information more particularly, the information required to detect dangers to a community and to have enough knowledge of the threat to build operational countermeasures to avoid or lessen the harm. Regarding the integration of ILP within a law enforcement agency, there are three phases to the process. The creation of the information management strategy is the first step in the first phase, which evaluates the components required for the information management process to be successful. The development of the organizational framework necessary to implement the information management strategy is the second step. The implementation phase is the third. These three stages are discussed in the conversations that follow.

Creating a Framework for the Processing of Information and Strategic Priorities: The Information Management Plan. The intelligence function is guided by a targeted set of procedures that are outlined in the information management framework, which serves as a business strategy. Through the use of seven crucial components, this strategy identifies priority issues and institutionalizes a mechanism for keeping tabs on them. A simple explanation of each component is provided by identifying the kind of questions it is meant to address and the organizational roles that are most likely to be in charge of providing the answers.

The intelligence process is included in the information management strategy. The gathering and handling of information required for the intelligence function are operationalized via the six stages of the intelligence cycle. The Intelligence Cycle is the method for ensuring that information is gathered, evaluated, and processed in a way that is scientific and compatible with established practice. The information management components together build the information management strategy.

Information Management Strategy

The management plan's seven essential elements combine the intelligence function with all other agency duties. The fact that they are managerial components rather than just functional ones should be stressed. For instance, the management plan's "analysis" section emphasizes the function that analysis serves in information management. In contrast, the intelligence process' analysis phase is concerned with extracting intelligence from unprocessed data. The components of the strategy are briefly described in the talks that follow.

Setting Priorities for Strategic Intelligence-Led Policing

In view of the effect that criminal and terrorist threats have on public safety and security, law enforcement agencies must monitor and manage these risks as part of their intelligence strategic goals. It is necessary to describe a strategic priority in terms of the local community and the intention of the managing law enforcement agency. Because law enforcement agencies have a broad variety of possible tasks, from traffic control to counterterrorism, defining intelligence priorities may become a complicated procedure. Practically speaking, these many roles cannot be performed equally due to resource constraints. Each duty has to be assigned a priority that will determine how much organizational effort and resources will be spent to it. There will be further prioritizing even within each duty. For instance, it is certain that almost every SLTLE agency would have a strategic objective pertaining to traffic management. There will be subpriorities such as the following within the strategic priority of traffic control:

i. Examination of traffic accidents

ii. Enforcement of the drunk driving laws
iii. Enforcement of speed
iv. Registration of vehicles and enforcement of regulations
v. Parking regulations.

This does not imply that there won't be any parking enforcement, but generally speaking, complaints are the only time that parking enforcement takes place. Priorities might alter depending on the situation. For instance, when cars need to be relocated off an emergency snow route or a hurricane evacuation route when the weather warrants it, parking enforcement may be given a high priority. A law enforcement organization must consequently establish priorities within a flexible framework that specifies the circumstances under which priorities may change and the manner in which they will be handled.

The systemic effect of many environmental elements affects strategic priorities. They consist of the following:

i. Known dangers to public safety
ii. The gravity of every danger
iii. Priorities in a community's politics
iv. The agency's resources for law enforcement
v. Knowledge of the police enforcement organization
vi. Additional financial commitments

Obligations under cooperation contracts with other law enforcement, public safety, or business sector organizationsThe law enforcement executive's top goals are both personal and professional. These are valid considerations since they have an impact on organizational priority as a result of an interacting equilibrium between the considerations. The whole law enforcement agency, including intelligence, must follow this procedure.In light of the "all-crimes, all-threats, all-hazards" approach to intelligence, it is clear that ILP may focus on a wide range of issues. Executives must gather crucial data, both factual and ideological, that will aid concentrate the prioritizing process. The law enforcement executive may look for answers to a number of issues while establishing strategic goals for ILP, such as the following: The framework within which the strategic goals for ILP may be stated and prioritized will be provided by the responses to these and additional questions specific to the jurisdiction. Operationalizing the priorities is the next stage. Let's say a law enforcement organization determined the following four ILP strategic goals, in no particular order of importance:

1. Terrorism.
2. federal protection.
3. Armed conflict.
4. Gangs.

There will be a subset of priorities within each of these that must be operationally defined as they relate to the agency. For instance, the following are the FBI's definitions of both domestic and international terrorism:International terrorism refers to violent or life-threatening activities that violate U.S. or state criminal laws, or that would do so if they were conducted inside such countries' or states' territorial jurisdictions.

In order to intimidate or coerce a government, the civilian population, or any segment thereof, for the advancement of political or social goals, a group or individual operating entirely within the United States or Puerto Rico may use unlawful force or threaten to use unlawful force or violence against persons or property.While meeting the goals of the FBI, a state, municipal, or tribal law enforcement agency setting its strategic objectives is not likely to find these categories to be as helpful. Instead, an organization can utilize a more condensed formulation to suit its purposes. For instance, the strategic priority of terrorism might be stated as follows:

i. Terrorism
ii. Terrorist organizations with ties to other countries
iii. Radicals who support the ideologies of terrorist organizations with a worldwide presence.
iv. Extremist right-wing criminal
v. Extremist environmental criminals
vi. Extremist criminals who support life.

A state, municipal, or tribal law enforcement agency should establish the strategic priority of homeland security in the context of the particular features of a jurisdiction. As an example, the homeland security. A community with a high concentration of cattle raised for beef processing may prioritize hoof-and-mouth disease or mad cow disease, and an agency located close to the U.S.-Mexico border may prioritize strategic awareness of tuberculosis. A farming community that raises crops may also prioritize the accidental or deliberate introduction of communicable crop diseases like soybean rust. The crucial thing to remember is that the present all-hazards approach to homeland security intelligence takes into account elements beyond the realm of legal competence. When evaluating risks and establishing strategic goals for homeland security, enforcement has to be considered.The strategic goals for intelligence will often be larger than in the past due to the "all-crimes, all-threats, all-hazards" approach utilized in modern intelligence efforts.

The organization-wide definition of the law enforcement agency's strategic goals will take many distinct shapes. An example of a strategic priority, specifically for ILP, may be written like. An evaluation of the information that is already known about the characteristics of each priority must be done within the context of strategic priorities. Then, intelligence needs are stated for information gaps. contains the conditional modifier "terrorist" or "criminal." This is significant because state, municipal, and tribal law enforcement entities may only gather and hold data that identifies people and groups with a criminal connection, not only those with radical ideologies.Readers should keep in mind that homeland security intelligence addresses all threats that might affect the duties of law enforcement, public safety, and order maintenance.

Required Intelligence

While the intelligence community has historically used intelligence requirements, law enforcement has only recently begun to adopt this strategy. Once again, requirements have somewhat varied applicability for the law enforcement community due to jurisdictional variances.An "intelligence gap" is a lack of knowledge that is required to comprehend a danger, target, or suspect. An "intelligence requirement" is a piece of information that has been determined to close this gap. Administrators use requirements to guide their judgments, and those decisions might take many different forms. The important thing to remember is that requirements specify the categories of data that must be gathered in order to satisfy the strategic goals. A pro-active allocation of resources is needed to gather the data needed to meet the

intelligence need. Open sources, information systems used by law enforcement and intelligence agencies, human sources, undercover agents, patrol agents, informants, community collaborations, public-private partnerships, or the use of technological surveillance tools are a few examples of what may be considered. The collecting plan explains this in detail.

Plan of Collection

The collection strategy is a methodical process for obtaining pertinent information from all legitimate sources in order to develop an intelligence product that satisfies the needs of intelligence. The collection strategy often contains a time range, however it can be continuing in the event of a standing intelligence demand. By gathering focused information regarding threats from both strategic and tactical viewpoints, the collection strategy is connected to the strategic goals via the intelligence needs.

The elements of the intelligence cycle are used to process the information that has been gathered. Intelligence products are created to monitor the strategic priorities and identify what, if any, operational actions are required to manage risks in each priority area as long as there is enough accurate and trustworthy information received and processed.

Analysis

Prior to analysis, raw data obtained in line with the collection strategy is of little use. The analytical process delivers a unified meaning to several disparate individual bits of information by relying on the scientific method of problem solving, logical reasoning, and objective interpretation of facts. Cause and effect relationships, correlations of actions and behaviors, and linkages between the various data are established via analysis. The new information gleaned via analysis might provide perceptions into risks that are present and developing, as well as prospective action strategies. Ascertaining that the findings of the analysis are "actionable" i.e., that there is enough detail in the information provided to operational units in the law enforcement organization to enable them to develop specific plans to prevent and/or mitigate threat is undoubtedly one of the goals of effective analysis. The intelligence products, which are written documents that contain this useful information, are distributed.

Intelligence-Related Goods

The reports and delivery methods used to share the results of the analytical process are known as intelligence products. An intelligence unit or fusion center should ideally develop a menu of goods that cater to the distinct requirements of its numerous customers. The items should have a uniform format and look that will make it easier for customers to choose the ones that are most suited to their needs. Managers will require different kinds of information than line officers would need, for instance, when a danger is recognized and reported.

The intelligence products known as situational awareness, a strategic assessment, and tactical indications each have a unique emphasis on the same danger.

The kinds of intelligence products that each fusion center and intelligence unit will create will be decided individually. Importantly, the intelligence function will interact with its consumers primarily via its goods. The intelligence products that the intelligence unit disseminates will be used to assess its overall usefulness. The deliverables must be of sufficient caliber, substance, and usefulness to enable the agency's operational elements to devise tactics and plans for

thwarting threats. The value of any intelligence product will be maximized if these qualities are present, which will ultimately increase public safety and security.

Operations Reactions

A key component of ensuring public safety is the intelligence process' ability to identify dangers. But intelligence only accounts for a portion of the security puzzle; operational commanders must also design intervention strategies that will either neutralize or halt the danger. Some of the operational measures will be quite straightforward, including giving police warning signs of the danger so they can be aware of them as they go about their everyday duties. Other, more advanced approaches, such as the employment of suppression tactics, proactive intervention, target hardening, community education, task force establishment, and aggressive use of conventional investigative techniques, may help to locate and capture perpetrators. It is crucial to remember that while establishing intervention tactics, operational units should turn to the intelligence function as a resource. The analyst has the most thorough understanding of the danger and might provide useful input to operational planning. Resources must be spent in order to implement operational responses. The operational commander's role in establishing intervention tactics includes allocating resources, but the intelligence function may help concentrate and prioritize plans. This may result in a better utilization of resources [10]–[12].

CONCLUSION

ILP and CompStat are essentially two separate strategies for deterring and combating crime, despite some general similarities. Law enforcement organizations must carefully assess these tactics to choose the one that best fits their unique requirements and situation. ILP and CompStat are both founded on the gathering and analysis of data, but the main distinction between these two methodologies is their emphasis.

While CompStat focuses on lowering crime overall, ILP is focused on utilizing information to prevent crime and interrupt criminal behavior. ILP encompasses a larger variety of actions than CompStat does, such as information collecting and analysis, targeted enforcement, and community participation. Comparatively, CompStat's main objective is to reduce crime via resource allocation and targeted enforcement.

REFERENCES

[1] L. Sevilla-Ortega *et al.*, “Role of isolated limb perfusion in the era of targeted therapies and immunotherapy in melanoma. A systematic review of the literature,” *Cancers*. 2021. doi: 10.3390/cancers13215485.

[2] H. Døssing, F. N. Bennedbæk, S. J. Bonnema, P. Grupe, and L. Hegedüs, “Randomized prospective study comparing a single radioiodine dose and a single laser therapy session in autonomously functioning thyroid nodules,” *Eur. J. Endocrinol.*, 2007, doi: 10.1530/EJE-07-0094.

[3] R. C. Locsin and M. Purnell, “50 International Journal for Human Caring 50,” *Int. J. Hum. Caring*, 2015.

[4] M. Elsner and W. Schudy, “Bounding and comparing methods for correlation clustering beyond ILP,” 2009. doi: 10.3115/1611638.1611641.

[5] H. Døssing, F. N. Bennedbæk, and L. Hegedüs, "Effect of ultrasound-guided interstitial laser photocoagulation on benign solitary solid cold thyroid nodules - A randomised study," *Eur. J. Endocrinol.*, 2005, doi: 10.1530/eje.1.01865.

[6] X. Chen *et al.*, "Full coverage of optimal phasor measurement unit placement solutions in distribution systems using integer linear programming," *Energies*, 2019, doi: 10.3390/en12081552.

[7] S. Bonvalot *et al.*, "Limb salvage with isolated perfusion for soft tissue sarcoma: Could less TNF-α be better?," *Ann. Oncol.*, 2005, doi: 10.1093/annonc/mdi229.

[8] W. Liu, H. Cai, J. Zhang, J. Wang, and L. Sui, "Effects of immediate and delayed loading protocols on marginal bone loss around implants in unsplinted mandibular implant-retained overdentures: a systematic review and meta-analysis," *BMC Oral Health*, 2021, doi: 10.1186/s12903-021-01486-3.

[9] A. Lemos, F. S. Melo, P. T. Monteiro, and I. Lynce, "Room usage optimization in timetabling: A case study at Universidade de Lisboa," *Oper. Res. Perspect.*, 2019, doi: 10.1016/j.orp.2018.100092.

[10] F. Papadia *et al.*, "Isolated limb perfusion with the tumor-targeting human monoclonal antibody-cytokine fusion protein L19-TNF plus melphalan and mild hyperthermia in patients with locally advanced extremity melanoma," *J. Surg. Oncol.*, 2013, doi: 10.1002/jso.23168.

[11] J. P. Deroose, A. M. M. Eggermont, A. N. Van Geel, and C. Verhoef, "Isolated limb perfusion for melanoma in-transit metastases: Developments in recent years and the role of tumor necrosis factor alpha," *Curr. Opin. Oncol.*, 2011, doi: 10.1097/CCO.0b013e3283424dbc.

[12] M. V. M. França, G. Zaverucha, and A. S. D'Avila Garcez, "Fast relational learning using bottom clause propositionalization with artificial neural networks," *Mach. Learn.*, 2014, doi: 10.1007/s10994-013-5392-1.

CHAPTER 9

A BRIEF DISCUSSION ON LEADER COMMITMENT

Dr. Preetha Chandran, Associate Professor, Department of Finance,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email id- preetha.chandran@cms.ac.in

ABSTRACT:

Leader commitment refers to the level of dedication and investment that leaders demonstrate toward achieving organizational goals and objectives. In the context of business and management, leader commitment can have a significant impact on employee morale, job satisfaction, and overall organizational performance. Leaders who are committed to their organizations are more likely to set clear goals and priorities, communicate effectively with employees, and inspire and motivate their teams. They are also more likely to invest time and resources into training and development programs, as well as in building strong relationships with stakeholders and partners.

KEYWORDS:

Commitment, Communication, Ethics, Leadership, Organizational Culture, Performance Management.

INTRODUCTION

The chief executive must lead the move to ILP since it will never be effectively accepted if a law enforcement agency's leadership does not comprehend and support the idea. The law enforcement executive's dedication must be shown by the provision of people and funds for the concept's development and implementation. Implementation attempts will fail if agency employees do not think the leader is dedicated to the new program. The following experience is a great illustration of a leader demonstrating their commitment:In the late 1980s, Dr. Gerry Williams made the decision to put community policing into practice while serving as the police chief in Aurora, Colorado. He saw that there was a lot of opposition and that Aurora police officers needed to be educated on the idea. He requested that the National Center for Community Policing at Michigan State University put together a 4-hour awareness workshop on the shift in policing philosophy that would be required for attendance by all Aurora police staff.

In order for every staff to have the chance to attend the required training during their regularly scheduled duty time, he additionally requested that the team provide it at 12 various times throughout the day, one for each shift. Chief Williams began each of the 12 sessions, whether they were held in the middle of the day or the middle of the night, by resolutely declaring that the Aurora Police Department would use community policing as its unquestionable policing philosophy and that resources would be committed to ensuring the change would occur. Then, Chief Williams sat during each of the 12 sessions in the center of the front row where he could

be seen by everyone. Because he put other responsibilities on hold to attend the length of all the sessions, news quickly traveled around the department that "the chief is serious about this". This was a significant demonstration of dedication. Additionally, the chief demonstrated his dedication by responding to inquiries throughout the sessions and mingling with police during the breaks [1]–[3].

The chief executive's genuine knowledge of the idea is where commitment starts. This has sometimes happened after the CEO has participated in training designed only from the executive's point of view. The chief can interact with others who might not only provide reciprocal support but also might allow an exchange of ideas on how ILP may be used by showing how intelligence fits with the department's overall mission through a program like this, which offers fundamental concepts that demonstrate the value of intelligence. The top executive should also explicitly express in a policy statement that they support the idea. The policy statement outlines the ILP's organizational framework and provides all agency members with a concrete framework for understanding how ILP is to be utilized.The allocation of resources to ILP is maybe the finest representation of commitment. The executive's commitment is strongly conveyed to agency workers by training them, placing them in the intelligence function, and allocating resources for the creation and implementation of ILP.

Due to the fact that commanders and managers are in charge of carrying out ILP, it is crucial to win their support for the idea. Despite the chief executive's backing, full implementation will not happen if commanders and managers do not have a clear knowledge of how ILP may help the agency or of their ILP duties for managing the individuals under their command. There have been occasions in the management process of all sorts of businesses when middle managers have sabotaged new initiatives by failing to fully ensure that the employees under their supervision carry out the tasks required to make the initiative successful. An ancient management proverb goes, "Managers may not be able to turn the water on, but they can easily turn it off." This is reflected in this.

DISCUSSION

The chain of command must be fully committed. Partnerships A variety of partnerships must be formed for ILP to be effective. This is amply shown by the precedence set in community policing as well as the field of counterterrorism. The community, non-law enforcement government agencies, and the commercial sector are just a few of the collaborations that are available. Each may be a valuable information source for the intelligence gathering process. Public-private partnerships are fundamentally justified by the idea that the more individuals who are aware of what to look for and how to report it to law enforcement, the more likely it is that they will come across information that may be utilized to thwart a terrorist attack or criminal business [4].

The Turkish National Police, Israeli Police, and the London Metropolitan Police have all had success with initiatives that include community people in the information-gathering process. To help the police fight terrorism, each has created programs geared at encouraging the public to disclose certain sorts of information basically, "intelligence requirements" to them. Community collaborations may undoubtedly be successful in the United States if they are in these different cultures. Additionally, public-private partnerships are a straightforward extension of several existing crime-fighting initiatives employed throughout the United States, ranging from Neighborhood Watch to Volunteers in Police Service.

If the typical community member is interested in taking part in ILP programs is one issue that arises. Residents of Wichita, Manhattan, and Topeka, Kansas, were cordially invited to attend a public awareness workshop on citizen reporting of suspicious actions that may be connected to terrorism as part of a pilot program run by the Regional Community Policing Institute at Wichita State University. Because they were worried about the danger and wanted to help with counterterrorism efforts, more than 600 individuals attended the workshops in the heartland.

By including the community, the intelligence process's information-collection parameters may be greatly expanded. These collaborations are successful for ILP due to a number of crucial elements.Through local law enforcement agents, the law enforcement agency must develop relationships of trust with the public. A simple "meet and greet" is often insufficient. It could be necessary to convey information that is delicate, private, or even frightening. Community policing has taught us that the relationship of trust built through constant communication is essential.

A reliable two-way communication channel must be created with each person after confidence has been gained. This could sometimes be technical, like e-mail or the phone. In other situations, people may feel more at ease giving the information solely one-on-one with a dependable law enforcement partner.For the partner to be able to recognize crucial information that has to be reported, training or public awareness about the signs and symbols of terrorism and organized crime is vital, just like for cops. For instance, if a community partner is not taught to identify these symbols, the information will not be reported if they notice a sign, tattoo, or foreign phrase that is representative of a terrorist or criminal organization. Similar to this, in order to improve their particular awareness, community and private partners should be informed about actions that are uncommon and signal criminal activity.

The kind of information that should be recorded for reporting to law enforcement should also be included in partner training. For nonlaw enforcement professionals, recording behaviors, evidence, cars, and personal descriptions is not a common practice, despite the fact that it comes naturally to law enforcement officials. Partner training includes explaining the types of information that should be reported together with the date, time, and place.The organization has to create a procedure and policy to safeguard the security and privacy of community partners. There should be a privacy policy to safeguard business partners' confidential information that may need to be exposed throughout the course of business, as will be covered in more depth in a following method of exchanging information. To strengthen the relationship of trust, partners must be aware of these policies.

Examples of Partnerships in Other Nations

Israel. When the Al-Aqsa Intifada was at its worst, the Israeli Police looked for other ways to learn about impending terrorist assaults. In towns like Tel Aviv and Jerusalem, community partnership patrols that worked with the local Palestinian population were established as one tactic. In order to gather information or signs about potential terrorist acts, the Israeli community partnership officers formed close bonds with many Palestinian residents of these cities. These connections were typically private and based on trust. The Palestinians' motivations were rather straightforward: A large number of Palestinians who worked and lived in Israeli cities had also been victims of terrorist attacks, just like the Israeli victims.

Turkey. Following a string of terrorist assaults in Istanbul in November 2003, the Turkish National Police questioned terrorists who had been apprehended to find out how they had joined the PKK and Turkish al-Qaida. Many were recruited in high school, and they often joined the organization at first out of peer pressure rather than a genuine dedication to the cause. As a response, the TNP started outreach and education initiatives in high schools to both discourage kids from joining these organizations and to gather data that might be used in the intelligence gathering process [5]–[7].Numerous successful collaborations have developed, particularly in bigger law enforcement organizations. SHIELD6 is a comprehensive information-sharing and public information initiative run by the New York Police Department. The Delaware Information Analysis Center7 has legal agreements in place for the exchange of information across the safe Automated Trusted Information Exchange network with non-law enforcement government agencies and selected private-sector groups. The Security/Police Information Network was established by the Nassau County Police Department as a thorough public-private information-sharing network that is segmented by sectors and separated between vetted and nonvetted information-sharing partners via e-mail and sporadic meetings. The lesson is clear: Partnerships are essential, there are models to provide direction, and partnerships must be developed across America's communities, not only in big urban areas. There are undoubtedly further instances.The development process and anticipated results vary slightly between partners from the community and the commercial sector, as is to be expected.

Community Collaborations

It is crucial to seek the community's help, just like with any other criminal or neighborhood issue. Two considerations make community cooperation more difficult in the field of intelligence. The agency is worried about threats, and many members of the community are uncomfortable with the role that intelligence plays in law enforcement. It is inadequate to merely advise folks to be on the lookout for unusual activity when it comes to threats. More direction is required. Whether on purpose or not, residents often fall victim to stereotypes when they report anything to the effect of: "A man who looks like he's from a Middle-Eastern country is taking a picture of a bridge." Such information is essentially worthless without this element. People should be instructed on how to spot suspicious actions and how to record them so that they may report them to the appropriate law enforcement agency. This lessens the likelihood of categorizing individuals and gives the law enforcement agency more useful information.

Many individuals are worried that establishing community partnerships for intelligence is the same as turning residents into informants on their neighbors. This worry relates to the intelligence function. Many individuals assume that intelligence activities routinely violate citizens' civil and privacy rights. This assumption goes hand in hand with the belief that many people hold that law enforcement agencies are gathering as much information as possible on all citizens or at least on citizens who do not share "law enforcement beliefs." Because civilians are often in a position to notice suspicious actions more frequently than law enforcement agents, it may be difficult to convince doubters of the method and the value of public participation in ILP. The idea of citizen involvement may be traced back to one of Sir Robert Peel's core assertions while creating the London Metropolitan Police in 1829: "The police are the public and the public are the police."

As was previously said, citizen training workshops may be quite beneficial in this process. Programs for citizen training have had varying degrees of success in a variety of communities

both domestically and overseas. The populace should be informed of 1. What to watch out for 2. What information they ought to record, and 3. Giving such information improves efficiency and lessens the likelihood of stereotyping. How to disclose the information to a law enforcement officer or agency. Community partnerships are less organized than public-private collaborations. All companies are open to collaborations, but those that are vulnerable to threats should be given first consideration. A law enforcement agency may benefit greatly from the information sharing capabilities of the business sector, since many of them have extensive worldwide networks and communications infrastructure. The benefit of raw information shared with the private sector may be substantial, whether it is via the employment of delivery employees who can see suspect behaviors, security staff at corporate buildings, or salespeople who can spot odd or suspicious purchases.

In rare circumstances, a law enforcement agency may establish an intelligence liaison relationship with a business to operate as the main point of communication for both parties. The process of exchanging information will become more productive and efficient thanks to this relationship. Similar to community partnerships, the law enforcement agency will have to teach the proper business staff. In certain situations, specialized training that is specific to a particular corporate sector may be offered. The terrorist early warning group idea, which has been implemented in many areas throughout the United States, is theoretically similar to this. The intelligence liaison contact will be concerned with dangers other than terrorism since law enforcement intelligence concentrates on all crimes and threats.

Two concerns of special relevance must be addressed when law enforcement agencies collaborate more closely and share more specific information with the business community. Privacy protection for people comes first. There are times when an American citizen's or legal resident's identification may be given to the commercial sector, such as when law enforcement authorities and the airline industry interact. While there are legitimate reasons to share information on people, caution must be taken to guarantee the information is accurate and the people's privacy is protected. The second concern is guarding businesses' confidential information. In certain cases, a business may give details concerning. A law enforcement agency may use a company's goods or corporate procedures to find and eliminate dangers. The law enforcement organization is responsible for making sure that any such confidential information is safeguarded.

Processes for Sharing Information

The gathering and dissemination of vital raw information is the foundation of efficient intelligence. It follows that each law enforcement organization must create a reliable system for storing and managing this kind of data that is different from or separated from other records in the organization's records. Administration system. Depending on the size and resources of each law enforcement organization, this mechanism will have a very varied structure. Despite these distinctions, there are a few issues to be resolved when creating an intelligence or sensitive information records capability in a

US law enforcement organization. These include the following:

i. How and where will this data be kept? It should be emphasized that several law enforcement organizations in the United States still lack networking capabilities due to their small size and rural, often distant, locations.

ii. Exist data compatibility requirements for electronic systems? Are data standards compliant with the National Information Exchange Model and the Global Justice Extensible Markup Language Data Model10?
iii. Even while each point might be covered in depth, it is important to remember that for the sake of this discussion, all of these concerns must be taken into consideration when creating an ILP structure. These problems have often been overcome for big agencies, but for the vast majority of law enforcement organizations many of which have just a few police officers this is uncharted territory. However, the issues must be resolved if they are expected to gather unprocessed data for the fusion centers and the Information Sharing Environment.

Finally, any agency developing a criminal intelligence records system should make sure that it complies with approved regulatory and legal norms due to stated national standards and precedent in civil law.

Part 3: Important Takeaways

i. It is necessary to create explicit procedures and rules to make sure that the appropriate information is provided to the staff members who need it.
ii. Achieve two-way information sharing methods
iii. Policies need to cover both internal and external procedures.

Operating strategy

The majority of law enforcement organizations have an operational plan in place that outlines its purpose, aims, and objectives as well as a set of instructions. Many of these components are readily applicable to ILP without any modifications; for instance, standardized standards of staff behaviour or officer safety rules. However, a department's operational strategy would normally include elements focused on criminal investigation and apprehending. As a result, the operational aspects of controlling risks must be covered by the ILP operating plan. ILP should have well-defined goals and objectives. It is important to explain the operational distinctions between intelligence and investigations, as well as how ILP relates to the agency's goal of apprehending criminals. ILP differs from typical performance measurements in even such areas as personnel assessment.The road map for carrying out ILP as an agency strategy is the operational plan.

Part 4: Important Takeaways

"For intelligence-led policing to be effective, the process must be an integral part of an agency's philosophy, policies, and strategies and must also be integral in the organization's mission and goals," the National Criminal Intelligence Sharing Plan notes. The agency's operational strategy should be coordinated for the ILP mission to be included in each component.The agency should create an ILP operating strategy to direct its intelligence-related actions.

Ability to Analyze

Intelligence cannot exist without analysis, however the majority of American law enforcement organizations lack an analyst due to a lack of funding. If a chief executive considers employing an analyst, political and collective bargaining consequences often need to be taken into account as well. On the political front, it might be difficult for the general public to comprehend the need for an analyst in a small law enforcement agency when crime is on the rise, including city

council members. Unfortunately, adding a non-sworn analyst to the police force would be more challenging in many areas than adding a new sworn officer. Moreover, in states with mandatory collective bargaining, like Michigan, it can be challenging to add positions related to law enforcement without getting concessions from the CBU or renegotiating the CBA.13 As a result, many agencies must look into options for establishing an analytical capability. Among the options available to an agency to build an analysis capacity are an agreement with the fusion center, a shared analyst across agencies, the use of volunteer analysts, or the employment of college interns as analysts.

Though imperfect, innovative solutions could be the only choice; one such solution might include police doing a basic analysis. Officers that use issue analysis as part of problem-oriented policing have done this in the past. A model is available for download from the Center for Problem-Oriented Policing14.

curriculum for problem-solving policing that teaches analysis. Despite not being intended for ILP, it may help officers acquire the analytical abilities they require for threat analysis [8].

To offer a firmer basis for ILP, agencies should apply an objective examination of the facts rather than depending only on intuition, it should be noted.

Part 5: Important Takeaways

The secret to successful intelligence is analysis:Due to need, agencies' analytical capabilities range significantly, from sophisticated to basic.The analytical approach may sometimes resemble the fundamental analysis that individual police officers do in problem-oriented policing.It's crucial to have an analytical attitude.

CONCLUSION

Overall, each organization's success depends heavily on the dedication of its leaders. An organization's culture may be fostered, workers can be inspired and motivated, and teams can be led through times of transition and uncertainty by leaders who are dedicated to their businesses. These leaders may contribute to the development of a sense of shared direction and purpose that can boost organizational performance and success by devoting time and resources to cultivating good connections with workers and stakeholders. High-commitment leaders are also more likely to promote an encouraging workplace culture. They may encourage staff to take responsibility for their work and collaborate with one another to accomplish common objectives by setting an example of conduct that reflects the organization's values and purpose.

REFERENCES

[1] Z. Yuan, Z. Ye, and M. Zhong, “Plug back into work, safely: Job reattachment, leader safety commitment, and job engagement in the COVID-19 pandemic.,” *J. Appl. Psychol.*, 2021, doi: 10.1037/apl0000860.

[2] C. Abrell-Vogel and J. Rowold, “Leaders’ commitment to change and their effectiveness in change – A multilevel investigation,” *J. Organ. Chang. Manag.*, 2014, doi: 10.1108/JOCM-07-2012-0111.

[3] Z. Tarigan and H. Siagian, “Leader Commitment on the ERP Performance Through Information Technology Capability and Inventory Management,” *Sci. Int.*, 2020.

[4] B. K. (Brian) Joo, S. Byun, S. Jang, and I. Lee, "Servant leadership, commitment, and participatory behaviors in Korean Catholic church," *J. Manag. Spiritual. Relig.*, 2018, doi: 10.1080/14766086.2018.1479654.

[5] E. Ekawati and Y. M. Sari, "An Analysis of the Internal Control Department Role in Achieving Good University Governance with Leader Commitment as a Mediating Variable in State Islamic Universities in Indonesia," *Test Eng. Manag.*, 2020.

[6] R. Puspitasari, W. Yadiati, S. Winarningsih, and Iriyadi, "The influence of leader commitment on the quality of financial statements and its impact on the performance accountability of blud hospitals in West Java province," *Int. J. Pharm. Res.*, 2020, doi: 10.31838/ijpr/2020.12.04.491.

[7] D. Hariyanti, J. La Masidonda, S. J. Hehanussa, T. R. Hariyati, and W. Asrida, "The effect of leader commitment and internal factors on internal audit performance at state and private universities in Maluku," *Int. J. Civ. Eng. Technol.*, 2018.

[8] T. Gonçalves, M. S. Teixeira, J. G. Dias, S. Gouveia, and R. J. Correia, "Commitment to exporting as an antecedent of organizational skills and firm performance," *J. Bus. Econ.*, 2021, doi: 10.1007/s11573-021-01028-x.

CHAPTER 10

TACTICAL AND STRATEGIC RESPONSE ALTERNATIVES

Dr. Vinoth. S, Professor, Department of Finance, CMS Business School,
JAIN (Deemed to-be University), Bangalore, India,
Email Id- dr.vinoth@cms.ac.in

ABSTRACT:

Tactical and strategic response alternatives are two approaches used in the context of emergency management and response. These approaches are designed to help organizations effectively respond to crises, disasters, and other emergency situations. Tactical response alternatives are focused on immediate, short-term actions that are taken in response to an emergency. These actions are often designed to contain and mitigate the immediate impact of the emergency, and may include measures such as evacuation, first aid, and search and rescue operations. Tactical response alternatives are typically led by emergency responders and are focused on ensuring the safety and security of those affected by the emergency.

KEYWORDS:

Crisis Management, Emergency Response, Incident Command System, Incident Management, Mitigation.

INTRODUCTION

We already spoke about the difference between tactical and strategic analysis. Creating alternatives to criminal threats as a reaction shows a different perspective on crime. For instance, the FBI Counterterrorism Division traditionally investigated cases with the goal of making an arrest as soon as probable cause was established. Instead of making quick arrests, the FBI's counterterrorism strategy now emphasizes gathering as much information as possible on all investigative targets.

One strategy may be to "turn" a target into an informant, allowing the informant to go on with their activities. In other situations, a target may continue to be under surveillance despite the existence of probable cause so that the agency can locate as many associates as possible and gain insight into how the targets communicate, obtain funding, and run their business in general in order to dismantle the criminal organization.

Arrest is not the main objective, even if many of these targets will ultimately be taken into custody as is often the case with ILP. Instead, breaking up the illegal enterprise is a crucial objective to get rid of the danger. Ratcliffe and Guidetti point out that intelligence-led policing is a theoretical foundation for carrying out police operations. It is neither a technique like saturation patrols nor a method of reducing crime like situational crime prevention. Instead, it is a business strategy and an information organization process that enables police agencies to better comprehend their crime issues and gauge the resources at their disposal in order to choose the enforcement or preventive plan that is most effective in reducing crime [1]–[3].

Part 6: Important Takeaways

In contrast to operational actions used to deter crime or capture criminals, dealing with threats requires unique strategies.The agency may choose to observe the conduct of criminal suspects rather than promptly detaining them in order to gather further information.

Creative new activities must be established to avert threats, depending on the kind of danger; often, this may not require arrests.

i. Lack of intelligence
ii. Basic Intelligence for Sharing Information
iii. Capacity for Advanced Intelligence Including Mature Records Systems Capacity for full-service intelligence.

Despite recent growth in connection and information exchange, the majority of American law enforcement organizations only have rudimentary intelligence capabilities. To allow the agency to establish a viable intelligence operation, the infrastructure and knowledge must be developed internally over time and with resources, including specialized personnel. Resources and outside help may be used to design policies, provide training, provide access to vital information systems, and build other infrastructure pieces.

The categories used to describe cognitive capability are not binary but rather range along a continuum. That is to say, the intelligence capability will be somewhere along a continuum within that category depending on the operational features of the agency's intelligence function. As might be predicted, the lower on the continuum, the greater the need for outside help and resources to build the capability to the level the agency needs. A law enforcement agency must do a self-assessment of key factors to ascertain the amount of intelligence capability and the location to start for building or reengineering the intelligence function. operational traits that characterize the four tiers. Each operational feature calls for a certain course of action that should be followed in order to either maintain the present state or advance.

The "operational characteristics" and the "action steps" are unquestionably not a law enforcement agency's intelligence capability's defining trait. Instead, they stand for significant benchmarks that may be recognized and evaluated throughout the implementation process.For instance, it may be necessary for certain organizations that are subject to binding collective bargaining to address training and changes to duties in a new CBA. Another instance is when the municipal council in certain areas has prohibited a law enforcement agency from building an intelligence capability due to privacy and civil rights concerns. Before creating and implementing ILP, it may be necessary to make revisions to court orders or consent decrees governing intelligence in other agencies [4].

DISCUSSION

The Implementation Starting Point

Every new endeavor has to get off to a strong start with a clear understanding of the organization's present level of knowledge and skills. United StatesKingdom, the National Intelligence Model's starting point was mostly consistent throughout all police forces with a solid base, given their history, when it was presented to the provincial constabularies. The starting

point is substantially more basic in the United States. In any law enforcement agency, the following questions must be addressed in order to establish this point of departure:

The goal of these inquiries is to build a comprehensive profile of the agency's intelligence capabilities, if any, so that the law enforcement agency may understand where it stands. The results of this evaluation will assist the agency decide what to do next in the implementation phase.As was previously said, educating staff on core concepts is an essential socializing technique. The need of training cannot be overstated, especially for line employees who require awareness training. If staff members don't grasp the ideas, new rules and procedures won't mean anything. Because of our pre-9/11 intelligence system, the great majority of America's uniformed law enforcement personnel are simply oblivious of the intelligence process and their participation in it.

The Global Intelligence Working Group and ISE standards and guidelines are sufficiently new that most agencies have not fully addressed them, if at all, the philosophy that intelligence was to have very limited information sharing for operational security purposes. This assumption applies to all four categories. The paradigm has drastically changed, and local American law enforcement still has a long way to go in terms of mastering it. Providing training at two cognitive levels is one of the top priorities once an ILP implementation commitment has been made.19 The first level is awareness, which is actually more like education than training because the goal is to comprehend the concept of intelligence, how it functions, and how it will contribute to the implementation.

purpose of law enforcement. The development of intelligence-related abilities and applications, such as data collecting, reporting procedures, and correct use of intelligence reports, constitute the second level. Training that is specifically targeted at the various organizational levels and responsibilities within an agency that call for the knowledge and abilities is necessary in addition to cognitive-level trainingto successfully complete the ISE. The Minimum Standards include the essential underlying information required for all of these training programs. Additionally, the adaptability built into the Minimum Standards enables each agency to customize the training program to suit its unique requirements.Since most individuals first oppose change, overcoming this opposition or dogmatism is a crucial first stage in the process of introducing ILP. The best method to do this is through gaining a knowledge of ILP and showcasing the advantages the change will bring both to the person and the company. In a word, everyone in the company has to be convinced of the new idea in this instance, ILP. individuals need to be resocialized, which is a challenging process that calls for proactive measures, alertness, patience, and the understanding that some individuals will never accept the change.

Demonstrating dedication and allocating resources to ILP is one of the most important ways to aid the socialization process.An operational plan that specifies the goals and procedures of the agency's intelligence capability must be created while the resocialization process is ongoing in a law enforcement organization. The National Criminal Intelligence Sharing strategy's first suggestion, which addresses the need for an intelligence infrastructure for all American law enforcement agencies, regardless of size,20 reiterates that each agency would have its own operational strategy. The capacity to employ a real model operational plan is limited by the enormous variances across agencies, even if certain components can be modeled. Instead, help should be given to create an operational strategy that takes into account the requirements and resources of each SLTLE agency.

The operational strategy should be created, created and distributed within the agency, and then executed by official notice to all staff members. No matter how much preparation is done, certain parts of the plan will always fail. To find out what works and what doesn't, it is critical to get feedback from the staff. Plans that don't work should not be seen as failures but rather as a necessary step in refining the plan to make it as successful as possible. Last but not least, a performance evaluation system that rewards and acknowledges ILP practitioners as well as a performance review of the overall ILP project are crucial but sometimes underappreciated tools for successful ILP.The largely qualitative nature of an officer's activities will not be taken into account in the performance evaluation system if a conventional evaluation system is in place that is based solely on quantitative variables number of citations issued, number of reports written, number of arrests made, number of calls answered, etc. Employees are aware of how closely the evaluation process is related to organizational performance; as a result, if ILP is to be successful, there has to be a people assessment system that values the practice. The agency's overall effectiveness in successfully adopting ILP must also be evaluated. The operational plan's objectives should be expressed in quantifiable terms so that continuous evaluations may change implementation and amend the component parts as required to guarantee that ILP is practiced effectively and efficiently.The introduction of ILP is an exercise in organizational transformation, which is a process that is always challenging, has been a recurring subject in this debate. While

Although the British National Intelligence Model and other nations that have experimented with ILP, like Australia, offer valuable lessons, American law enforcement agencies currently lack the necessary structural and experiential characteristics to fully adopt the model. The implementation of ILP must begin at the most basic level since the majority of law enforcement agencies in the United States are only starting to join the intelligence field. Several crucial insights from the organizational change process may assist direct this transition when agencies start using ILP: There must be a stimulus for change. A change agent, or visionary leader, must be ready to challenge the status quo by making the initial move. It's crucial that this stimulus continue and be widely used.

Diverse areas of concentration

Administrative commitment is required. A new project or program needs constant support from the administration in order to maintain consistency between words and deeds. There is little reason to trust managers are sincere if they are unwilling to do things like reallocating resources, changing rules and processes, or experimenting with new ideas. The likelihood of success is considerably decreased if commitment is not made to either politicians or workers. Utilizing the ILP Self-Assessment Tool created as part of the Michigan State University "Sustaining Intelligence" training program, which is supported by U.S. funding, is one way to assess the status and effectiveness of implementation. Homeland Security Department.Any change must be supported by reasoned and convincing grounds. Although it may seem cliche, it is important to remember that just shaking up the company would not be a positive change. Politicians and workers must be provided with solid facts to back the change if they are to bind their professional futures to it. Additionally, because change requires resources, it is inefficient to pursue it unless it is well supported by reason and evidence.

All levels of individuals must be able to contribute. The value of team development for a new project cannot be overstated. Every endeavor has to include as many individuals as possible. Along with fresh insights from the variety of input, team building fosters ownership and, as a

result, a feeling of commitment and accountability among team members.Any new program or concept needs enough time for trial, review, and fine-tuning. When a new venture is launched, it will inevitably have bugs since not every illness or issue can be foreseen and some concepts won't function as intended. The mere fact that there are operational issues does not imply that the concept was flawed. Administrators, elected officials, and staff must be adaptable, modifying their actions until enough time has passed to properly assess the initiative's genuine consequences.

The plan must be explained to everyone before implementation and their support must be obtained. Politicians, residents, and workers all need to be aware of what is happening and why. One has a propensity to believe that everyone is as knowledgeable about and as familiar with a new project's problems as those who are actively involved in its preparation. A new activity may be destroyed by a lack of communication, but thankfully it is quite simple to prevent. It's important to keep in mind that communication entails more than just delivering messages; it also requires receiving response on those messages. Be aware of the situation and keep in mind the warning, "Don't leave people in the dark." It might take a while for a substantial shift to take place; it could even take a generation. American society tends to be impatient and short-term. Resocializing workers, citizens, and political leaders is a crucial component of big organizational and behavioral transformation initiatives like ILP. This is by nature a long-term project, therefore perseverance and patience are needed before success can be seen. To reduce irritation and frustration, everyone involved must be taught to respect time.

Be aware that not everyone will embrace novel ideas. Given the nature of the human mentality, we must acknowledge that perfect support for almost any activity is unlikely. But one must be careful not to dismiss those who reject new efforts as obstructionists or "lost causes". Pay attention to their worries; they can bring up some important points that should be addressed. People who are opposed to a new venture could end up joining the team if their recommendations are favorably implemented. But reality demands that there will always be people who disagree with the new order. An administrator's choices under these circumstances are:

1. Keep attempting to persuade them to change;
2. Avoid or ignore them;
3. Employees should be assigned to tasks where they won't do much harm;
4. Improve the relationship's quality with the politicians and staff who support the idea; or
5. Till they leave, retire, or lose power, tolerate workers or politicians.

Regarding organizational, philosophical, and programmatic change, be adaptable and receptive. We must acknowledge that many ideas are a waste of time, no matter how much thinking is put into a new endeavor and how much time is spent preparing. Frequently, we won't be aware of this until the concept has been tested and assessed. Failure may teach us something, too. Unfortunately, there is a propensity to dictate achievement given the ethos of our political environment—a technique that is equivalent to looking for mediocrity. We must preserve the ability to fail, both inside the police organization and within the larger political system. Without it, original fresh ideas will be hard to come by.

There is always a danger that one may find himself in a political hot seat. No effort at change can be made without danger; the bigger the change, the bigger the risk. Organizations, especially bureaucratic organizations often found in government, do not readily tolerate challenging

conventional dogma. The backers of new initiatives must realize that their political careers are on the line when they are in the forefront of change. Administrators must thus show sympathy and support for the politicians and staff members who are in favor of the reform.

Confronting conventional ideas or at the very least, traditions, is necessary for change. It has not historically been politically expedient for individuals to debate the merits of traditions, yet doing so is essential if new endeavors are to be launched. When conventional knowledge is questioned, skeptics, dogmatists, and traditionalists will object, criticize, and sometimes mock it. The wise leader must be ready to handle these responses on both a personal and professional level. Importantly, the leader has a responsibility to affirm the importance and contributions of people who support the leader's ideas of change when they are challenged [5]–[7].

Effective participation in change must be measured and rewarded through the organization's people assessment system. Since personal involvement or commitment is necessary for change, there must be some personal gains that may result from participation. Benefits might include things like constructive criticism, employment perks, creative freedom, recognition, and accolades or awards; they don't always have to be monetary. Those who significantly aid in bringing about change must also be given honors and other forms of gratitude. In essence, failure is certain in the absence of incentives. ILP has a lot of promise for US law enforcement. The change process to adopt ILP, however, must start at the most basic level, be intentional, and be adapted to the requirements and resources of the agency if it is to be successful.

The Law Enforcement Intelligence Process and Civil Rights

The defense of individuals' civil rights is a fundamental obligation of all law enforcement organizations engaged in maintaining public safety, and intelligence operations are no exception. The liberties granted to every person by civil rights protections are one of the most significant and essential components of American society. Law enforcement professionals embrace this obligation, despite what others may think. They are aware that defending civil freedoms is just as crucial as keeping the neighborhood safe from crime and terrorism. Although this is a basic reality, there is disagreement on where to draw the line in terms of how much government should be permitted to intrude on people's privacy and freedoms in order to safeguard American residents and the nation's sovereignty from foreign dangers like terrorism.

Whether certain civil freedoms should be curtailed in order to defend America against terrorism is one issue that has been up for discussion. This problem is expressed in the philosophical debate about what is more crucial: defending Americans from terrorist attacks that might result in the death of thousands of people, or defending individual civil freedoms that are the foundation of America's most cherished ideals. Since this subject is philosophical in nature and relies on each person's particular philosophy and life experiences, there isn't really a clear-cut right or incorrect response when it comes to it.Fortunately, this philosophical argument is irrelevant to the functioning law enforcement officer. Instead, the officer must concentrate on reasonably clear guidelines that guarantee the preservation of people' fundamental rights. They consist of the following:

In order to conduct intelligence operations, law enforcement must have a criminal basis before gathering personal information about a person. To fairly conclude that a specific intelligence subject has committed, is committing, or is going to commit a crime, the law enforcement officer must have trustworthy, fact-based information.It is required to follow the rules of criminal

process while gathering any information on a person for intelligence purposes.Information gathered cannot be kept forever. Instead, material may only be kept if there is trustworthy information that offers consistent proof of a criminal predicate.

It is the duty of the law enforcement agency to safeguard the confidentiality of any personal data it gathers during intelligence operations. Only authorities with a right to know and a need to know the information in order to further a criminal investigation may get information under this protection of privacy.All intelligence files on a person must be deleted if there is no proof of a proven criminal predicate. The following pages will address each topic. In order to make sure that information is being gathered, utilized, kept, and distributed in an appropriate way, there has been a considerable rise in the examination of law enforcement intelligence operations due to the significance and emotions on both sides of the argument. Many law enforcement organizations have been condemned for their intelligence operations, not only due to actual or prospective abuses but also due to perceived abuses. This last element needs further consideration.

The phrase "potential for abuse" does not imply that abuse will happen, but rather that it is possible if there are no controls in place to stop it. These are the three key elements:

1. Policy.
2. Training.
3. Accountability and Supervision.

The agency's ideology, standards, expectations, and decision-making parameters are established by policy for every job and duty inside the company.Training equips people with the information, talents, and skills necessary to carry out any specific vocational activity. It outlines the process for carrying out the required actions, as well as what must be done, how it should be done, and what cannot be done. It serves as an example of how policy is applied and often notifies staff members of consequences and punishments if the assignment is not completed properly. Organizational measures such as supervision and accountability help to guarantee that policies are followed and tasks are carried out according to the manner outlined in the training.A supervisor keeps an eye on the actions and conduct of their subordinates to ensure that they are carrying out their duties solely in ways that have been approved by the organization.

Abuse is far less likely with properly established policy, efficient training, and competent monitoring. Systemic to the organization are two more elements that may potentially influence the possibility for abuse. The first is the kind of personnel the agency hires. What are the specifications? What qualities are looked for in new hires? What selection criteria influence the sort of employee hired? The kind of clay used to create a law enforcement officer will have a big impact on how well training, supervision, and policy work.

The agency leadership is the second component. Employee actions will reflect the tone that the department head sets for the team as well as the expectations of the leader. The likelihood of abuse happening will also be considerably reduced by a leader who sets clear expectations for employee performance and supports those standards with appropriate incentives and penalties. All law enforcement tasks, not simply intelligence ones, have the potential for misuse. The goal of modern law enforcement is to carry out all of its duties in an ethical and legal way. It is a faulty reasoning to draw the conclusion that a law enforcement intelligence unit or an intelligence fusion center is necessarily problematic only because there is a risk of misuse [8]–[10].

CONCLUSION

To best suit their unique requirements and situation, organizations must carefully assess their emergency management and response plans and choose the right combination of tactical and strategic response options. Organizations may lessen the effects of calamities and protect the safety and security of their staff, stakeholders, and communities by adopting a comprehensive strategy to emergency management and response. Although the emphasis and breadth of tactical and strategic response options vary, both are essential to efficient emergency management and response. While strategic response options are vital to assist companies in anticipating and responding to crises in a timely and efficient way, tactical response alternatives are necessary to protect the safety and security of persons who are impacted by a disaster.

REFERENCES

[1] J. R. Howlett, K. M. Harlé, and M. P. Paulus, "Inhibitory failures in cocaine use disorder: Not paying attention when there is a need to be cautious," *Drug Alcohol Depend.*, 2021, doi: 10.1016/j.drugalcdep.2021.108833.

[2] J. D. Becker, "Strategy in the New Era of Tactical Nuclear Weapons," *Strateg. Stud. Q.*, 2020.

[3] K. Kim and L. Bui, "Learning from Hurricane Maria: Island ports and supply chain resilience," *Int. J. Disaster Risk Reduct.*, 2019, doi: 10.1016/j.ijdrr.2019.101244.

[4] R. Sara, M. Jones, and L. Rice, "Austerity urbanism: connecting strategies and tactics for participatory placemaking," *CoDesign*, 2021, doi: 10.1080/15710882.2020.1761985.

[5] A. A. Fleischmann, B. H. Spitzberg, P. A. Andersen, and S. C. Roesch, "Tickling the monster: Jealousy induction in relationships," *Journal of Social and Personal Relationships*. 2005. doi: 10.1177/0265407505049321.

[6] R. Verleger, N. Grauhan, and K. Śmigasiewicz, "Is P3 a strategic or a tactical component? Relationships of P3 sub-components to response times in oddball tasks with go, no-go and choice responses," *Neuroimage*, 2016, doi: 10.1016/j.neuroimage.2016.08.049.

[7] N. F. Piercy, D. W. Cravens, and N. Lane, "Thinking strategically about pricing decisions," *J. Bus. Strategy*, 2010, doi: 10.1108/02756661011076309.

[8] M. Santangelo, I. Botha, and N. Strydom, "Long- And short-run dynamics between South African hedge funds and the equity market," *J. Wealth Manag.*, 2021, doi: 10.3905/JWM.2021.1.138.

[9] S. Gavaris, "Fisheries management planning and support for strategic and tactical decisions in an ecosystem approach context," *Fish. Res.*, 2009, doi: 10.1016/j.fishres.2008.12.001.

[10] O. Bugrov and O. Bugrova, "Formalization of selection of contract-organizational project delivery strategy," *Eastern-European J. Enterp. Technol.*, 2018, doi: 10.15587/1729-4061.2018.151863.

CHAPTER 11

PRIVACY AND CIVIL RIGHTS: A FOUNDATION

Dr. Gopalakrishnan Chinnasamy, Associate Professor, Department of Finance,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email id- dr.gopalakrishnan_c@cms.ac.in

ABSTRACT:

Privacy and civil rights are fundamental principles that are essential to protecting individual freedoms and promoting a just and democratic society. Privacy refers to the right of individuals to control their personal information and to maintain their personal autonomy, while civil rights refer to the legal protections and guarantees that are afforded to individuals to ensure that they are treated fairly and equally. In order to ensure that privacy and civil rights are protected, it is essential to establish a strong foundation of laws and policies that reflect these principles. This foundation should include legal frameworks that protect personal privacy and prevent the unlawful use of personal information by government and private entities.

KEYWORDS:

Data Protection, Ethics, Fourth Amendment, Information Privacy, Privacy, Privacy Law.

INTRODUCTION

Some fundamental definitions should be given first. The concept of privacy relates to people's interests in avoiding the erroneous gathering, use, and disclosure of personally identifiable information. Private conversations, private actions, and private data are all examples of privacy interests.Although the term privacy is not used specifically in the U.S. Constitution, numerous of its clauses guarantee various facets of this basic right. Although there is no clear federal constitutional right to an individual's privacy, the U.S. Supreme Court has defined privacy rights in several instances.2 Numerous privacy safeguards exist, including protection against pointless or unlawful acquisition of personal data, public revelation of private information, and embarrassment or humiliation brought on by the publication of personal data [1]–[3].

National Criminal Intelligence Sharing Plan recommendations

Recommendation 1: All parties engaged in putting the National Criminal Intelligence Sharing Plan into action and promoting it should take efforts to guarantee that the law enforcement community respects people's constitutional rights and privacy throughout the gathering of intelligence.

Recommendation 2: Regardless of whether an intelligence system is funded by the federal government, law enforcement agencies must adopt, at a minimum, the requirements outlined in the Criminal Intelligence Systems Operating Policies federal regulation in order to ensure that the collection or submission, access, storage, and dissemination of criminal intelligence information complies with the rights to privacy and the constitution of individuals, groups, and organizations.

The phrase "civil rights" implies that the state has a responsibility to ensure that all citizens get equal legal protection and opportunities to enjoy their citizenship rights, regardless of their race, religion, sex, or other traits unrelated to their value as a person. Therefore, civil rights are demands made on the government to advance equality. The Thirteenth and Fourteenth Amendments, as well as legislation passed by Congress, give all citizens of the United States the right to personal liberty. Typically, the terms civil rights and civil liberties refer to constraints on government whereas civil rights generally refer to positive government activity.4 In this sense, the term "civil liberties" refers to basic personal freedoms derived from the Bill of Rights, such as the right to free speech, the freedom of the press, and the right to practice one's religion; the right to a fair trial; and other restrictions on the ability of the state to impose its will on people. Individuals are protected by civil liberties against impermissible government action and arbitrary government intrusion.

Particularly in light of prior abuses, privacy, civil rights, and civil liberties have significant consequences for the law enforcement intelligence process. Law enforcement's intelligence procedures, according to critics, have not altered, and counterterrorism programs implemented after September 11 have increased law enforcement's invasiveness. Understanding this issue and how individuals worried about civil rights violations scrutinize law enforcement intelligence efforts as a result offers significant insight [4]–[6].

DISCUSSION

Increased Scrutiny of Law Enforcement Intelligence: The Challenge of Balancing Civil Liberties and Community Safety. Why are law enforcement intelligence efforts receiving more attention and criticism when there is a clear danger of terrorism that may have devastating implications, as seen by the personal, societal, and economic fallout from 9/11? There seem to be a number of elements. Abuse from the past may be at the top of the list. Sadly, there is a history of law enforcement unlawfully gathering, holding onto, and/or sharing information and acts concerning people whose public remarks and behaviors were contentious but not illegal. Even while law enforcement authorities in many of those cases thought the intelligence target was damaging American sovereignty,5 the fact remains that the organizations lacked the legal right to gather or hold onto the material since it was being used for non-criminal expressive purposes. It must be underlined that the only legal basis for law enforcement's ability to conduct any kind of intelligence action is the power to enforce the criminal code; as a result, they are required to adhere to the rules of criminal process. As a result, it is inappropriate to gather data on civilians without a clear criminal connection. Law enforcement organizations are still being investigated and penalized for prior violations.

The Supreme Court decisions made during the Earl Warren era, which expanded the application of civil rights and liberties, are an example of a second reason.6 The 1960s saw citizens for the first time overtly exercising and testing their rights in the form of large-scale public demonstrations and civil disobedience as part of the civil rights movement and Vietnam War protests. A new generation of activist civil rights lawyers filed cases against police departments and correctional facilities as a result of this environment. A long-standing law, USC 1983—Civil Action for Deprivation of Civil Rights, was essentially revived by these lawsuits. Together, these incidents gave Americans' rights a new focus and gave the concept of citizenship in the United States a fresh vocabulary.

The fact that many people do not recognize the line between national security intelligence and law enforcement intelligence is a third reason. Therefore, they presumptively believe that the intelligence community's behaviors may likewise be reflective of those of a local police enforcement organization. One example of information gathering that a state, local, or tribal law enforcement agency won't undertake or ordinarily have access to is the National Security Agency's recording of international telephone conversations or the FBI observing a suspicious person entering the United States identified by the CIA as a potential threat. However, there is often the presumption that law enforcement organizations are complicit in such actions and as a result, must be closely scrutinized in order to uphold civil rights.

Fourth, the heightened scrutiny of law enforcement activities, including intelligence, is partly a result of the 24-hour news cycle and developing news channels. Despite certain changes in the print media, the development of the electronic media, including broadcast and Internet, has substantially aided in the public scrutiny of governmental actions. With more electronic venues, news companies are under fiercer competition to find news items that will stimulate customers' interests and satisfy their 24/7/365 need for material. These elements have increased competition for contentious tales with distinctive consumer resonance. As a result of the requirement to fill every hour with material, stories also get more in-depth treatment and are often replayed throughout the day. The result is a deluge of news on a certain subject that creates the sense that the problem is considerably exaggerated.

The growing partisanship among elected officials and the electorate seems to be a fifth factor influencing the examination of law enforcement intelligence. This has led to a dichotomous atmosphere where attitudes and actions tend to be drawn primarily along party lines with harsh criticism and no conciliation for opposing viewpoints on almost every social, political, and economic topic. Almost any relevant component, including law enforcement intelligence, may get embroiled in a politicized debate.

The expansion of civil rights advocacy organizations7 has also unmistakably altered how the general public views police enforcement. These organizations track patterns and situations that make them more worried about privacy protections. These organizations make the public aware of government actions they believe to be inappropriate via news releases, white papers, public presentations, and legal actions. Even though they are not usually well-liked by the general public, these organizations bring up the subject to start a discussion in society and often work to alter public policy via legal action or political sway.

The "open government" trend also welcomes public scrutiny. Slowly but surely, a grassroots movement known as "open government" started, mostly with Watergate in the 1970s. The main issue was that public officials were misusing the power granted to them by their positions, and they were required to show that their acts were both legal and in the best interests of all residents. Government authorities only gradually reacted as the movement continued to acquire significant support. The number of open records and open meetings laws approved was rising, as were the federal and state freedom of information laws and the scope of court interpretations of the FOIA. Due to public pressure, elected politicians were compelled to provide financial disclosure statements, and monitoring organizations started publishing reports on the varied acts of representatives from all levels of government. In essence, the movement calls for governmental responsibility.

Collectively, these elements have influenced the public's expectation of having the right to know what is happening with government operations and their increased use of legal action to demand justifications and responsibility. Accountability has increased to the point that many choices made by the government are now being questioned, thanks to the development of the Internet and of 24-hour news stations. One artifact for Democracy and Technology, www., is the recent publishing of certain secret papers by the media. cdt.org. Every individual has specific areas of concern about civil liberties, civil rights, and privacy in relation to all forms of governmental policy and activity, not only law enforcement. Each group plays a crucial watchdog function, even if there is often controversy.

Of course, a significant watchdog or advocacy group that stirs up controversy is unlikely to be actively involved in this movement. In general, prominent proponents of open government acknowledge the necessity to preserve the confidentiality of "content," but also anticipate transparency with regard to procedures. The general public understands the need to safeguard the privacy of explicit information, but they also want reassurances that information is being gathered, stored, utilized, and shared in a way that respects their rights. These ideas influence law enforcement intelligence operations at all levels of government and call for the establishment of transparent procedures and privacy laws [7], [8].

The concept that government should be "of the people, by the people, and for the people" is becoming more and more important, and decision-makers ought to take it seriously. No one is exempt from intelligence. In fact, further scrutiny is encouraged by the intelligence process' intrinsic threat-based confidentiality. The American Civil Liberties Union has made the following claims as proof of this: No one in America is unprotected by the law. And no one is above the bounds of the law. If American democracy is to be sustained, our system of checks and balances must be maintained.

Similar to this, the Bill of Rights Defense Committee has declared that its goal is to support, organize, and promote a broad, powerful, and nonpartisan national grassroots movement to restore and defend the civil rights and freedoms that the Bill of Rights guarantees to every American citizen.

Our mission is to raise awareness of the importance of those rights in daily life, to promote active participation, and to develop and disseminate the organizing tactics and tools necessary for people to transform their worry, outrage, and fear into discussion and action to reinstate Bill of Rights protections. It is crucial to understand the need of accountability and the effects it will have on a law enforcement organization if it is rejected or neglected. Together, these elements signal a substantial sociopolitical shift in American society, which has led to the development of new law enforcement intelligence projects.

Defined Consent Decree

A court order including a settlement is known as a consent decree. In order to make sure that the settlement is implemented, the court grants the defendant injunctive relief and consents to continuing to have jurisdiction over the matter. Consent decrees are often preferred by litigation plaintiffs because they have the support of the court behind the agreements. Such agreements are often preferred by defendants who desire to remain anonymous because they prevent the disclosure of potentially damaging information. The agreement's conditions will be carried out under the authority and control of the court.

Court Cases and Decisions Concerning Law Enforcement Intelligence Activities

Perhaps the most contentious aspect of law enforcement organizations' information collecting is situations when people engage in "expressive activity" that is often severe or contentious. Even if their exact activities are not illegal, those who hold radical ideas about white supremacy, animal and environmental preservation, anti-government emotions, anarchy, and other belief systems are often seen as threats. There is, in fact, evidence of a dynamic and often ill-defined behavior range between "extreme" and "criminal" conduct. It might be difficult to tell the difference between a solid declaration of conviction and a threat. We as a nation have developed heightened danger awareness after September 11, which seems to be encouraging us to be less tolerant of opposing, even radical, viewpoints.

It is difficult for law enforcement to distinguish between the two. The goal of the intelligence gathering process is to learn more about people who are a danger to society, yet what a law enforcement official may interpret as having a connection to crime may be what a civil libertarian refers to as exercising one's right to freedom of speech. To guarantee that law enforcement officials are carrying out their duties legally and safeguarding the community at the same time, it is crucial to comprehend the complexities of these discrepancies. Unfortunately, as previously mentioned, there is a history of law enforcement abuses in which organizations have gathered data on people solely because of their political beliefs.10 Although law enforcement organizations have undergone significant change over the past several decades, this legacy is challenging to overcome.

A group engaging in First Amendment activity can be shielded from unwarranted political or religious surveillance that causes them cognizable harm thanks to the Supreme Court's expansive interpretation of the right of association based on the First Amendment, as first established in NAACP v. Alabama11 and most recently in Boy Scouts of America v. Dale12. As a consequence, in many cases, the safeguards may exceed the state's interest in keeping the community safe. A sui balance between the interests of public safety and associational rights can be achieved by requiring a reasonable suspicion of criminal activity before conducting First Amendment activity investigations, even though restrictions on surveillance cannot unduly restrict the government's ability to conduct necessary information gathering. This proof of illegal behavior, which serves as the basis for further investigation by law enforcement, demonstrates the strong state interest that underpins such efforts. There are two notable court decisions that deal with expressive behavior and the role of police enforcement intelligence. Understanding the takeaways from these examples might help decision-makers make informed choices about the acquisition and storage of information.

"Special Services Division"

The FBI Guidelines outline three progressively higher degrees of investigation work:

1. Pursuing preliminary leads, information is acquired that warrants further investigation into the probability of criminal behavior;
2. A preliminary investigation that is permitted when there is evidence or an accusation that suggests the potential of criminal action and that, in order to be handled responsibly, needs more investigation than just following up on first leads;
3. A thorough inquiry is permitted where evidence or circumstances ostensibly point to the commission, ongoing commission, or impending commission of a federal offense.

Both the NYPD and civil libertarians considered the amendment that the court approved to be a "mixed bag," thus one would infer that it was a fair compromise. The updated consent decree kept the Handschu Authority for supervision. Another motion concerning the consent decree argued that the New York City Police Department Interim Order 47, which established policies and guidelines for the use of photographic and video equipment by the police department, was incompatible with NYPD guidelines, infringed upon the plaintiff's First Amendment rights, and contravened earlier Handschu judgments. The court was asked to enjoin enforcement of the order.

The applications were denied by the court in February 2007 on the basis that the investigations in issue are not political in nature. The court also declared that it would not grant the plaintiffs' request for injunctive relief since Order 47 did not violate the First Amendment. Later on in the year, the court changed its February ruling on the enforcement of the consent decree once again, stating that before the court may enjoin any police department policy, the plaintiffs must demonstrate a systematic pattern of breaches.

The takeaways from Handschu include that, regardless of the danger environment a community is exposed to, a criminal connection is still necessary for law enforcement to monitor people, including taking photos, videos, and gathering IDs. Even while there may be some wiggle room in the post-9/11 world, law enforcement organizations nevertheless have a duty to uphold the constitutional right to free speech and the right to express oneself.

Denver:

City and County of Denver v. American Friends Service Committee, et al., 2004 U.S. Dist. LEXIS 18474. The Denver Police Department's Intelligence Bureau was found to have been keeping files on the expressive activities of advocacy groups about which there was no evidence of criminal activity, as well as monitoring and recording the peaceful protests of local residents in the Denver area, according to documents made public by the ACLU of Colorado on March 11, 2002. The ACLU requested four more moves from the Denver mayor in a letter dated March 11, 2002, in addition to urgent action to end the DPD's practice of maintaining data on nonviolent protest activities.

1. Make it illegal for the police to share with other law enforcement organizations any information they may have on criminal activity.
2. Ordering a thorough public accounting of the criminal intelligence data would provide answers to many problems.
3. Notify the people included in the criminal intelligence information and provide them access to the files containing information about them.
4. Save the criminal intelligence data since it may be used as evidence in future legal proceedings.

The Denver mayor said the following during a press conference on March 13, 2002:

After conducting a preliminary analysis of the policy and looking through a selection of the files that have been kept on people and organizations, we have come to the conclusion that the policy was interpreted too broadly, leading to situations where it might not have been appropriate to include specific people or organizations in our intelligence-gathering efforts. The DPD was accused of violating the U.S. and Colorado constitutions by failing to follow the police

department's policy on intelligence records and failing to manage its criminal intelligence records system in accordance with the requirements of 28 CFR Part 23.

The plaintiffs brought a class action civil rights lawsuit against the DPD for these violations. The Denver Police Department's practice of keeping track of residents' peaceful protests even when there was no proof of criminal activity was criticized in the Plaintiffs' class action complaint for declaratory and injunctive relief31, which was initially filed on March 28, 2002. the advocacy work done by law-abiding people and groups, many of whom the Department has wrongly classified as "criminal extremists," as well as giving copies of certain spy files to outsiders.

Additionally, it was claimed in the lawsuit that the DPD had chosen and singled out the plaintiffs and the plaintiff class for surveillance and monitoring due to their support for divisive or unpopular political viewpoints and beliefs. The plaintiffs also voiced worry that people would be less willing to engage in protests or other forms of expression if they felt intimidated that they would be identified in police criminal intelligence files or that they would be photographed by the police. The criminal intelligence records on the plaintiffs, according to the complaint, only contain identifying information and facts that demonstrate that the individuals who were the targets of the surveillance are involved in legal and peaceful educational activities, political expression, petitioning the government, and political association. No information on the sites points to any of the identified plaintiffs engaging in illegal behavior. The Plaintiffs are the subject of incorrect and damaging information that the Department maintains on file. It has tarnished the Plaintiffs' reputations on all fronts and misrepresented the aims and objectives of their expressive activities.

The Department has made the data in the Spy Files available to other parties.

The plaintiffs provided evidence to support their allegations, including memos to officers from supervisors and departmental procedures that directly ran counter to the DPD's criminal intelligence records policy, 28 CFR Part 23, and/or constitutional requirements. In one communication to subordinates, the Intelligence Bureau chief said, in part:

The City of Denver and the plaintiffs came into a Settlement Agreement after considering the facts in the case, despite the City of Denver denying "...any fault or liability to Plaintiffs, nor any violation of law"37. The Department formed an oversight board, bought a new computerized intelligence records system, committed to semi-annual audits of compliance with the Settlement Agreement for 5 years, and adopted a new, more stringent intelligence records policy as part of the Settlement Agreement38.

The takeaways from this case strengthen the need for a criminal predicate. In addition, the Denver example exemplifies 1. The significance of monitoring in enforcing the present policy, 2. use of the right-to-know and need-to-know principles for information transmission, and 3. the significance of following the regulations in 28 CFR Part 23.

Consequences of Hands Chu and American Friends

The gathering, preservation, and distribution of information that identifies people and groups whose utterances and expressive actions represent a danger to public safety and security are at the core of civil rights problems relating to law enforcement intelligence. The obvious conclusion from these two decisions is that any collection, retention, and distribution of this information may take place where there is a connection between the conduct and an offense.

Simply using unpopular, strange, or harsh language and establishing the notion that those using them could one day commit a crime do not enough to pass the test. A crime must be proven by tangible evidence. Law enforcement personnel need to get training on the problems connected to expressive action and a criminal predicate.

These examples also demonstrate the need for more than just a policy on criminal intelligence records, even one that complies with 28 CFR Part 23. In order to make sure that the policy is implemented, oversight is also necessary. Information-gathering procedures by law enforcement employees must be explicitly directed, and such direction must be in accordance with norms that are representative of both professional good practice and the defense of civil rights and freedoms.Reiterating that any such criminal intelligence material must adhere to the right-to-know and need-to-know principles is also crucial. We'll talk in more depth about these elements later. The crucial thing to remember is the part these criteria played in these two significant incidents and the consequences that followed when the requirements weren't satisfied.First Amendment Free Expression Two Views: Civil Rights

Example

Actions connected to free speech by participants in protests or demonstrations are a frequent source of civil rights disputes. Advocates for civil rights contend that their protests qualify as expressive action covered by the First Amendment. It is thus inappropriate for law enforcement authorities to gather and hold data on those who are active in organizing and taking part in protests, as well as about those who support such people.Law enforcement organizations say that the only data they gather and hold on to is information on those who commit crimes or represent dangers to public safety. Civil rights activists counter that minor offenses like trespassing

Law enforcement exploits small offenses as a justification to gather information on people it disagrees with, and minor crimes, such as vandalism of minor property, are of such low size that they do not balance the violation of the wider First Amendment rights. According to law enforcement, any protest that allows property damage may swiftly spiral out of control and lead to even bigger risks. Law enforcement asserts that it is their duty to defend the property of all victims. The discussion goes on, often with conflicting viewpoints,

1. No matter how offensive the behavior, the government should not try to control it as long as it is carried out lawfully.1. Frequently, it is difficult to tell whether a crime is being done or is about to be committed when a protest or gathering is in progress. For instance, during protests, anarchists regularly break windows or spray paint on private property. Spray painting someone else's property is "destruction of property," not an act of expression.
2. The fabric of American society depends on the basic freedom to engage in expressive action. Therefore, law

1. Enforcement should refrain from interfering with free speech.2. All Americans' rights must be upheld by law enforcement, not only those participating in expressive activities. As a result, law enforcement organizations have a duty to implement appropriate restrictions in order to maintain community safety and security as well as other people's legal rights.
2. There shouldn't be any "protest zones" that are specifically designated to favor one group over another. More often than not, certain organizations have a history of committing crimes during demonstrations. Protest Zones are only utilized where there is a history of

criminal activity or when there is evidence that makes a solid case that criminal activity will take place during a demonstration.
3. Pens and barriers may be employed in certain instances to keep demonstrators safe or to stop clashes between them and others opposed to the group's expressive activity.
4. Law enforcement shouldn't monitor or infiltrate political or social organizations that engage in expressive activities.
5. The use of surveillance and infiltration is a recognized and legal approach to collect evidence for building a criminal case for prosecution if there is a plausible suspicion that a crime will be committed.

On the same problem, they are effectively diametrically opposing stances. Which postures are accurate? Truth lies somewhere in the center of the spectrum, like most topics with distinct, opposing viewpoints. The onus of proving that the information gathered and actions taken by the law enforcement agency were done so as to preserve both civil rights and community safety often rests with that organization. Several efforts might be taken to reduce claims of carelessness and improper behavior as well as to show the law enforcement agency acted in good faith [9]–[11].

CONCLUSION

Overall, the protection of individual liberties and the advancement of a fair and democratic society depend on the fundamental concepts of privacy and civil rights. We can guarantee that people are safeguarded from harm and that our society continues to be just and equitable for everyone by developing a solid foundation of laws and policies that represent these ideals. In addition, this base must contain safeguards for civil rights, such as the right to equality before the law and the absence of discrimination. This calls for a steadfast dedication to upholding anti-discrimination legislation and making sure that people have access to legal counsel and remedy in situations when their civil rights have been infringed. Promoting innovation and progress in the digital era also requires a solid foundation of civil rights and privacy protections. It is crucial to set precise rules and laws that safeguard human rights, privacy, and creativity while simultaneously encouraging economic development as technology develops.

REFERENCES

[1] M. J. Kelly and D. Satola, “The right to be forgotten,” *University of Illinois Law Review*. 2017. doi: 10.1093/oso/9780198868422.003.0006.

[2] S. Gilman, “Proliferating predation: Reverse redlining, the digital proliferation of inferior social welfare products, and how to stop it,” *Harvard Civil Rights-Civil Liberties Law Review*. 2021. doi: 10.2139/ssrn.3511892.

[3] Albert Jones, “EFF urges Biden to reverse Trump’s support for facial ID,” *Biometric Technol. Today*, 2021, doi: 10.1016/s0969-4765(21)00017-5.

[4] A. A. Lytvynenko, “Data Privacy and Banking Secrecy: Topical Issues in Commonwealth, Continental Europe and International Jurisprudence,” *ATHENS J. LAW*, 2019, doi: 10.30958/ajl.5-3-5.

[5] S. Braman and S. Roberts, “Advantage ISP: Terms of service as media law,” *New Media and Society*. 2003. doi: 10.1177/14614448030053007.

[6] James Hunt, "Electronic Frontier Foundation," *Choice Rev. Online*, 2010, doi: 10.5860/choice.48-1189.

[7] M. E. Whitman, J. Perez, and C. Beise, "A study of user attitudes toward persistent cookies," *J. Comput. Inf. Syst.*, 2001.

[8] A. Mattlage, "Responsibilities of information professionals vis-à-vis information rights," *J. Infor. Ethics*, 2015.

[9] J. Roman, "A proteção de dados pessoais na Lei nº 13.709/2018: Uma análise sobre consentimento e o direito à autodeterminação informativa na Lei Geral de Proteção de Dados," *An. dos Congr. Estaduais Magistr. - RS*, 2020.

[10] A. Laje, "Privacy right, the family and entertainment," *J. Int. Commer. Law Technol.*, 2014.

[11] C. Geiger and E. Izyumenko, "Designing a Freedom of Expression-Compliant Framework for Moral Rights in the EU: Challenges and Proposals," *SSRN Electron. J.*, 2021, doi: 10.2139/ssrn.3868008.

CHAPTER 12

NEED FOR MORE CONTROLS OF INTELLIGENCE INQUIRIES THAN CRIMINAL INVESTIGATIONS

Amit Verma, Associate Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-amitverma2@gmail.com

ABSTRACT:

Intelligence inquiries and criminal investigations are two different types of activities that involve gathering information for different purposes. Intelligence inquiries are typically carried out by government agencies and are designed to gather information on potential threats to national security, while criminal investigations are conducted by law enforcement agencies and are aimed at gathering evidence of criminal activity. Given the sensitive nature of intelligence inquiries and their potential impact on civil liberties, there is a need for more controls and oversight of these activities than criminal investigations. This is because intelligence inquiries often involve the collection and analysis of large amounts of data and may include activities such as surveillance and monitoring of individuals who are not suspected of criminal activity.

KEYWORDS:

Confidentiality, Congressional Oversight, Intelligence Collection, Judicial Oversight, Law, Privacy Protection.

INTRODUCTION

Many people hold the opinion that intelligence inquiries pose a greater threat to liberty than criminal investigations, which is at the core of the many reasons why material gathered by law enforcement authorities for the intelligence process is viewed with suspicion and mistrust. Unlike a criminal investigation, which takes place after a crime has been committed, an intelligence inquiry aims to determine if a danger is there and whether it is genuine. Additionally, intelligence investigations often include First Amendment speech, are more covert, and are less open to review after the fact. Therefore, civil rights groups contend that intelligence gathering should be subject to more compensatory safeguards and redress mechanisms for infractions. These ideas are supported by three main elements [1].

Inquiries into intelligence are first wider. Although they are constrained by the criminal law, their scope stretches beyond already-committed crimes and into the realm of threats. Civil rights groups specifically object when law enforcement gathers information regarding First Amendment activity. There is often dispute about how words and actions should be interpreted and whether a certain action constitutes the exercise of free speech or the threat of violence.

Second, intelligence investigations are done with even more secrecy than criminal investigations. Normal public remarks regarding one's innocence and public denials of the criminal allegations in open court processes are permitted when one is charged with a crime. Furthermore, throughout

a criminal investigation, the suspect is often aware of what is going on. In a similar vein, the majority of searches in criminal cases are conducted while simultaneously notifying the target. Contrarily, in intelligence cases, the target and those being investigated because of their relationships with the target are seldom ever informed that the government is gathering data on them. While there is no question that the presumption of evidence in a criminal investigation is respected, it is sometimes maintained that there is a presumption of guilt in an intelligence probe. This viewpoint needs to alter.

Third, practically everything the government conducts during a criminal investigation is eventually made public. A prosecutor is aware that the results of the criminal investigation will be made public. If the prosecutor goes too far or is out on a fishing expedition, it will be made public, putting them in the spotlight and maybe leading to their disbarment.41 That restriction is strong. Similar to this, the public will eventually demand an explanation from a police agency on crime and disorder in a neighborhood. The majority of intelligence investigations don't end in a court case or other public action. It is possible to exploit the evidence covertly. The sheer awareness that the government is looking might sometimes be the intended outcome.

Protections must be implemented from the start since intelligence probes are larger, more covert, and less amenable to post-factum review. A federal rule concerning criminal intelligence records kept by state, municipal, and tribal law enforcement organizations is one significant safeguard [2], [3].

DISCUSSION

Maintaining Privacy in the Intelligence Process

The idea of privacy is wide and takes into account a variety of individual beliefs and interests. In the present law enforcement intelligence environment, a variety of privacy-related considerations become important and are meant to handle "all crime and all threats. A wide range of concerns, including the privacy of a person's ideas, personal conduct, personal communications, personal traits, and personal data, may be defined as privacy interests. Information that a law enforcement agency may be gathering regarding a person's potential participation in a crime also falls under the category of private information.

Regardless of whether the individual is an intelligence target, witness, informant, or information source, the law enforcement agency must respect the privacy of any personal information it gathers during an intelligence investigation.When, how, and to what degree you reveal personal information about yourself are all considered aspects of personal data privacy. The right to manage one's personal information includes the power to choose if and how such information should be collected and utilized. It imposes limitations on a variety of procedures including the gathering, using, keeping, and disclosing of personal information.

The law enforcement agency is responsible for safeguarding the privacy of any individual whose personal information it includes individuals who are thought to have committed crimes. Security and secrecy are employed as the two main techniques.When personal information is considered to be secure, it implies that safeguards and procedures have been put in place to guarantee that no one else has access to it. There must be a sufficient mechanism in place to guarantee that the private information is not accessed by those who do not have legitimate access to them, whether the private information is in a computer system or in paper records.

When it comes to exchanging information, confidentiality refers to the actions and procedures used to avoid unauthorized exposure of the information to outside parties. Unless there is a legitimate purpose for a third party to acquire the information, the custodian of the information has a duty to preserve private information once it has been collected. Once again, the threshold for disclosing private information to third parties is based on their need and/or right to know the information. This serves as an example of how confidentiality is ensured. Furthermore, it is expected of those who receive private information to protect the privacy of the data given to them. The goal of confidentiality is to restrict access to personal data.

1. To those with particular authorization to view the records, 44 and
2. preventing unauthorized third parties from learning about it.

Law enforcement organizations should make sure that privacy measures are in place to enhance privacy protection. This was highlighted by the National Strategy for Information Sharing, which established fundamental privacy standards that all agencies must follow. Which are:

1. Share only the portions of protected material pertaining to terrorism, homeland security, or law enforcement that are relevant to terrorism.
2. The protected information that has to be shared inside the information sharing environment should be identified and reviewed.
3. Give ISE participants the ability to decide the kind of protected information to be disclosed and any legal limitations on it.
4. All relevant laws and regulations must be evaluated, documented, and followed.
5. Establish protocols for data quality, accuracy, and preservation.
6. Put in place sufficient security measures to secure confidential information.
7. Adequate accountability, enforcement, and audit measures should be put in place to ensure compliance.
8. Create a grievance procedure that complies with legal standards and mission needs.
9. Implement the recommendations by making the necessary adjustments to corporate procedures, systems, and training, as well as technology.
10. As necessary, inform the general public about the agency's policies and practices.
11. Make sure that agencies only divulge protected information to nonfederal organizations—including state, local, tribal, and foreign governments—if those organizations provide equivalent security measures.
12. A senior individual accountable for implementation must be designated by state, municipal, and tribal governments.
13. Implementing a privacy policy46, combined with efficient training and monitoring, is how privacy is protected.

An organization's policy stance about how it manages personally identifiable information that it collects and uses in the regular course of business is expressed in a written, public statement known as a privacy policy. Information on the procedures for data collection, analysis, maintenance, dissemination, access, expungement, and dispose should be included in the policy.

A privacy policy's goal is to publicly state that the agency will abide by the laws and agency policies that permit information to be collected and shared in a way that respects individual privacy rights. A well-designed and put into practice privacy policy makes prudent and effective use of the resources of the justice organization, safeguards the agency, the person, and the public, and fosters public confidence.

In order to participate in the ISE as well as the NCISP, state, municipal, and tribal law enforcement organizations must create a privacy policy. It is obvious that there are clear requirements for law enforcement organizations to adhere to national professional standards for the protection of civil rights and privacy. As a result, the duty is to guarantee that the policy is successfully implemented by not only implementing it but also by providing training and monitoring [4].

Criminal Intelligence Operating Policies, CFR Part 23

The primary question about civil rights concerns is whether law enforcement authorities are gathering and keeping personal identifying information on people who are engaged in expressive behavior, as is clear from the debate that came before it. It might be difficult to tell the difference between expressive behavior and behavior that is a sign of impending criminal action. It is the duty of the law enforcement agency to gather data to confirm any indications that a crime is being planned and to take proper action if necessary. Criminal intelligence data are kept until the threat's legitimacy is confirmed or rejected since it is not always evident if a crime is in the planning stages. This thin line necessitates the establishment of standards as a matter of policy to guarantee that the data is balanced and properly maintained or deleted, depending on what further gathered data implies about criminal responsibility.

The federal regulation titled Criminal Intelligence Systems Operating Policies, which is codified in the Code of Federal Regulations at 28 CFR Part 23.48, is the governing regulation for managing a criminal intelligence records system for SLTLE agencies. The regulation was created largely as a response to past practices of law enforcement agencies collecting and retaining information about people based on their activities and/or expressed nontraditional beliefs that were frequently extreme. In accordance with constitutional protections, the rule aims to give procedural direction for the administration of criminal intelligence records systems. To autonomously controlled state and local governments, the federal government cannot impose this legislation. However, SLTLE agencies must consent to the regulation's adoption in order to be eligible for certain federal grant money. Adoption of 28 CFR Part 23 is a condition for obtaining the money if, for instance, a local police agency accepted federal monies to buy a computer system that would be used to manage a criminal intelligence records system.

Regardless of whether federal monies were used or not, most agencies embraced this law as the de facto norm for keeping criminal intelligence data since it was the only one with clear guidelines. The NCISP's recommendation that all law enforcement agencies implement 28 CFR Part 23 helped the rule become more widely adopted. As a consequence, the rule became a widely accepted professional norm at the national level. Although the regulatory language was understood by the agencies that adopted the rule, translating it into policy was difficult. The rule also has a few operational holes. In order to make the wording and intent of the legislation easier for a law enforcement agency to implement, the Law Enforcement Intelligence Unit created a model operational policy and procedures. The LEIU File Guidelines are a practical interpretation of 28 CFR Part 23.

The administration of criminal intelligence records systems represents a critical step in the LEIU File Guidelines' pursuit of constitutional integrity. The management of a criminal intelligence records system must take into account factors beyond this practical interpretation of 28 CFR Part 23, according to litigation, experience, and concerns raised by civil libertarians. As a result, the current best practice is an amalgamation of various sources relying on a conservative integration

of accepted practice and regulation. These sources include the LEIU File Guidelines, 28 CFR Part 23, the legislation governing criminal evidence and process, and precedent from civil rights cases involving the use of criminal intelligence data. The fact that this information represents general practice rather than particular state regulations with potential for varied consequences should be emphasized. The decision tree is a graphic illustration of the discussion below about the variables to be taken into account when adding information to a criminal intelligence database system. To provide the safest advice on information retention in a criminal intelligence records system, this is a conservative interpretation of these elements.

One of the first questions to be answered when information is gathered is whether it identifies a person or an entity. Identity is not only a name; it may also contain any descriptive information that enables someone to reasonably exclude others from identification of that person. For instance, giving an address and a physical description of someone residing there might be considered identity. Because 28 CFR Part 23 mentions organizations as protected criminal intelligence information but does not define organization, it might be difficult to discern whether the information identifies an organization. An organization is a recognisable entity with a defined goal, a recognizable organizational leadership structure, and a procedure or technique for members to connect with the organization, even if it is informal, based on precedent and experience. There are other organizations that individuals choose to associate with because they have a similar viewpoint, such as anarchist collectives, but they lack the above-mentioned stated qualities. In this example, the group is less of an organization and more of a movement. Even as a group, a movement that only has a discernible idea that supports it is not an organization. If information does not identify a person or organization, why may it still be kept in a criminal intelligence data system without establishing reasonable suspicion? Individuals, not aggregate data, philosophical movements, criminal tactics, or other material that is descriptive and helpful for intelligence research but does not directly identify a person, are the subjects of constitutional rights. Logic based on Katz v. U.S.50's assertion that the Fourth Amendment protects persons, not locations

asserts that only specific persons are given constitutional rights, not groups of people's actions or any data that isn't directly related to any one person. Organizations are expressly covered under 28 CFR Part 23 in addition to people.The next stage is to assess whether the material was gathered in a way compatible with legal criminal process if it may be used to identify a person or group. Although this is not a requirement of 28 CFR Part 23, precedent in both criminal and civil law implies that an agency should adopt this as a good practice when determining what data should be stored in a criminal intelligence records system. There are several causes. First of all, it is a constitutional safeguard that should be provided to people; it is a crucial component of the basic fairness that people in the American judicial system are guaranteed by the Fifth and Fourteenth Amendments' due process provisions. Second, the legislative authority to implement the criminal law serves as the only foundation for law enforcement's investigative and criminal intelligence powers. As a result, there is a chance that criminal intelligence and investigation efforts may result in prosecution. Evidence may be excluded from trial if there are breaches of criminal process. Third, it improves the intelligence or investigation inquiry's legal integrity, lowering the likelihood

civic responsibility. Processes that closely follow constitutional protections show good faith and, on the other hand, serve as an affirmative defense against agency negligence. Fourth, including this phase in the procedure lessens criticism of law enforcement actions given the attention given

to law enforcement intelligence and investigative procedures by many in the civil rights sector. Finally, the approach complies with the Information Sharing Environment's Privacy Guidelines, which include the following statements.

1. Only seek for or hold onto protected information that the agency is legally permitted to do so with respect to the laws, rules, regulations, policies, and executive orders that apply to the agency.
2. ii. Make that the protected information the agency makes accessible through the ISE was legally collected by the agency and is permitted to be made accessible via the ISE.

Information Sharing Environment program manager. Rules to Make Sure That Americans' Legal Rights and Information Privacy Are Protected During the Creation and Use of the Information Sharing Environment.

Submission of Intelligence Records Decision Tree

The agency must have a purpose for gathering information on a person if it is done so in a way that complies with constitutional requirements when used in the intelligence process. The goal of this rationale is to continue investigating potential community risks in an effort to stop them before they materialize. As a consequence, even if a person is not accused of committing a crime, information about them is gathered because they are either the subject of an intelligence investigation or have some kind of knowledge about the danger. In a criminal intelligence records system, both sorts of information must be legitimately retained.

"Non-Criminal Identifying Information" may be included to a criminal intelligence information file if it is pertinent to the identification of the subject or the subject's illegal behavior and comes from a source who is not the inquiry's target but contains crucial information, provided that: 1. The information is accompanied by the necessary disclaimers, stating that it is only identifying information without any implication of criminal activity; and 2. If the material relates to the criminal subject's political, religious, or social opinions, affiliations, or activities, it must be directly related to criminal behavior or action. The inclusion of a criminal subject's religious affiliation in the system as NCI Information, for instance, would only be allowed if it is directly tied to the criminal subject's attendance at a specific church, synagogue, or mosque to the illegal behavior or activity, like in cases when it is clear from the evidence that the crime was committed in a church, synagogue, or mosque. An person may also be added to the criminal intelligence records system with a clear NCI identity if they provide relevant information about an acquaintance that helps the intelligence investigation.

If the subject of the investigation is the person about whom the information has been gathered, the information may only be kept if a criminal predicate is proven. A criminal predicate is determined in two steps. First, there has to be a connection between a person's actions and a crime or between an organization's activities and criminal conduct. In accordance with 28 CFR Part 23, "Reasonable Suspicion," the standard of evidence for material to be submitted to a criminal intelligence records system as criminal intelligence information is "reasonable suspicion."

A skilled law enforcement or criminal investigative agency officer, investigator, or worker has grounds to suspect that a person or group is engaged in a certain illegal activity or operation. These particulars are referred to as "Criminal Predicate" or "Criminal Fact." A person's actions

may raise reasonable suspicion, which goes beyond "mere suspicion," but before such information is recorded in a criminal intelligence data system, it must meet the standards for criminal link and degree of proof.

The public tip or even a patrol officer's Suspicious Activity Report are common sources of information for intelligence personnel. Typically, such information is devoid of any proof of a crime. In actuality, the intelligence officer has a responsibility to evaluate the information's veracity in light of a possible criminal threat rather than just disregard it. How the data may be stored lawfully in the absence of a criminal foundation is the problem that has to be answered. The 28 CFR Part 23 recommendations do not address this circumstance, therefore the LEIU File Guidelines52 provide a practical interpretation of the rule that has been accepted by the courts. Temporary files and permanent intelligence files should be created, according to the criteria.

A temporary file is for information that does not rise to the level of reasonable suspicion but relates to an event or activity that suggests the possibility of criminal behavior, as opposed to a tip, lead, or SAR, none of which qualify as criminal intelligence material under 28 CFR Part 23. This material must be expressly labeled as transitory as it is not criminal intelligence information, regardless of whether it is stored in the same database, accessed, or transferred alongside criminal intelligence information. Policy must set limitations on how long data will be stored in the temporary file. The sole purpose of the temporary file is to give a place to store raw data while an investigation is carried out to see if a criminal predicate may be established. If the criminal basis is not proven within the allotted time, the item will be removed. After a criminal predicate has been established, the material is considered as criminal intelligence information and may be stored in a permanent file. Despite being often used, the term "permanent file" is somewhat misleading since, in accordance with 28 CFR Part 23, the information in this file has to be reviewed and deleted every five years.

It's crucial to remember that these policies and procedures only apply to criminal intelligence records systems that are managed by SLTLE agencies. A law enforcement agency's investigative file and records management program are both exempt from the requirements of 28 CFR Part 23. Although worries about the numerous records that law enforcement agencies retain are often kept outside of the RMS, they sometimes appear pertinent to intelligence. The most frequent inquiries relate to gang records and Field Interview records. Due to the vast variation in these data amongst law enforcement agencies, it is possible to properly ascertain whether the records qualify as criminal intelligence information for the purposes of 28 CFR Part 23 by asking a few generic questions[5]–[7].The goal of this debate was to disseminate broad knowledge concerning the handling and use of criminal intelligence data. There are often direct inquiries about certain systems of a particular agency. The 28 CFR Part 23 Training and Technical Assistance program, financed by the Bureau of Justice Assistance, is the greatest source of information for these queries.

CONCLUSION

There is a greater need for controls and oversight of intelligence investigations to ensure that they are conducted in a way that respects individual rights and liberties, even though both criminal investigations and intelligence inquiries play significant roles in preserving national security and ensuring public safety. We can contribute to ensuring that intelligence investigations are handled in a way that is compatible with our democratic ideals and principles by providing clear legal frameworks and strong oversight procedures. It is crucial to develop precise legal

frameworks that outline the scope of these operations and provide reliable supervision and accountability systems in order to guarantee that intelligence investigations are conducted in a way that respects individual rights and freedoms. This might include the creation of impartial monitoring organizations, the use of warrants and other legal protections, and stringent guidelines for the use and distribution of gathered information. The use of search warrants and the necessity for probable cause, on the other hand, are common examples of the stricter legal controls and supervision systems that are often applied to criminal investigations. These measures are intended to safeguard the rights of those who are being investigated for criminal conduct and to stop law enforcement authorities from abusing their authority.

REFERENCES

[1] BBC News Online, "Is privacy dead in an online world," *BBC News Online*, 2017.

[2] K. Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired*, 2013.

[3] A. H. Beare, "Prosthetic Memories in The Sopranos," *M/C J.*, 2019, doi: 10.5204/mcj.1586.

[4] A. Harrington *et al.*, "News and notes," *Procedia - Soc. Behav. Sci.*, 2015.

[5] M. Awais, W. Li, M. Ajmal, and M. Faheem, "Using IoT Innovation and Efficiency in Agriculture Monitoring System," *J. Bot. Res.*, 2020, doi: 10.30564/jrb.v2i2.1900.

[6] E. M. Backett and A. M. Johnston, "Social patterns of road accidents to children: Some characteristics of vulnerable families," *Inj. Prev.*, 1997, doi: 10.1136/ip.3.1.57.

[7] A. M. Younus, "Utilization Of Artificial Intelligence (Ann) In Project Management Services: A Proposed Model of Application," *Cent. ASIAN J. Theor. Appl. Sci.*, 2021.

CHAPTER 13

FEDERAL CIVIL RIGHTS LIABILITY AND INTELLIGENCE

Sourabh Batar, Assistant Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-battarsourabh@gmail.com

ABSTRACT:

Federal civil rights liability and intelligence are two important areas of concern for government agencies and law enforcement officials. Civil rights laws protect individuals from discrimination and ensure that they are treated equally under the law, while intelligence activities are designed to gather information and protect national security. However, intelligence activities can sometimes come into conflict with civil rights protections, leading to potential liability for government agencies and law enforcement officials. For example, the use of surveillance technologies or the monitoring of social media activity may raise questions about the potential infringement of individual rights to privacy and free speech.

KEYWORDS:

Equal Protection, Federal Civil Rights Liability, Intelligence-Led Policing, Law, Racial Profiling.

INTRODUCTION

Numerous lawsuits, like the ones from the previously mentioned New York and Denver instances, provide proof of intelligence abuses. Unfortunately, opponents often fail to acknowledge the significant adjustments made to law enforcement procedures as well as the more focused professional focus on law enforcement intelligence. Higher educational requirements, improved training, the acceptance of ethical norms, and the inculcation of law enforcement as a profession are signs that the culture of law enforcement has evolved and rejected previous methods that led to the aforementioned abuses [1]–[3]. Beyond this historical context, the general public has a misperception of the role of law enforcement intelligence, imagining it to include surveillance, covert operations, and stealth information gathering. It is important to reassure the public and the media that law enforcement intelligence procedures rigorously adhere to each individual's constitutional rights while gathering, storing, and sharing information.

Additionally, it is important for the general public to comprehend that intelligence analysis is just the scientific method of issue resolution, much as how analysis has been successfully used in community policing. The distinction is that whereas intelligence concentrates on dangers and potential ways to thwart them, community police is more concerned with crime and disruption in the community. The majority of opponents merely urge that information collecting and analysis be done in accordance with the legal guidelines that law enforcement officials are required to follow in order to prevent terrorism and solve crimes. A remedy is available to citizens when an employee of a state, local, and, in some cases, tribal law enforcement agency violates an

individual's civil rights under color of law because it is crucial to protect citizens' civil rights in all law enforcement activities, including intelligence operations. Title 42 of the United States Code, 1983 - Civil Action for Deprivation of Civil Rights, is the remedy, as was previously mentioned.

By 1983, civil actions were available for the violation of federal and constitutional rights by those acting in bad faith. This law was first enacted as a part of the Civil Rights Act of 1871, which sought to rein in repressive actions by the federal government and private citizens supporting vigilante organizations like the Ku Klux Klan. Before the historic Supreme Court decision Monroe v. Pape, 365 U.S. 167, which granted people access to federal court as a last option rather than just in the absence of state action, 1983 was dormant until 1961. Today's 1983 lawsuits against police enforcement organizations most often center on First Amendment concerns, such as freedom of expression, Fourth Amendment concerns, such as use of force or search and seizure, and Fourteenth Amendment concerns, such as allegations of due process violations.

The statute's essential components are:

a. Was the person's constitutionally guaranteed or nationally recognized right violated?
b. Did the law enforcement agent behave in accordance with state law?
c. Did the law enforcement agent fail to treat the person with the appropriate level of care?
d. Was the violation of the person's constitutional rights or federal statutory protection the result of the law enforcement officer's actions?
e. Did the law enforcement organization do all necessary to guarantee that its personnel policies and procedures uphold civil rights?

A successful civil rights action requires the plaintiffs to establish both the law enforcement agency's carelessness and a pattern of wrongdoing that went along with it. This is often accomplished by providing proof that the law enforcement body did not exercise due care in defending people's civil rights. In order to do this, the plaintiffs will often try to establish that the law enforcement agency intentionally ignored safeguarding people's civil rights and privacy. This willful apathy in intelligence-related situations may be the result of the following factors:

Failure to train: In accordance with the Global Advisory Committee's recommendations for the Minimum Criminal Intelligence Training Standards, the agency does not offer intelligence training to all members of the law enforcement community.

Failure to direct:the agency's policies and practices for the gathering, storing, reviewing, and disseminating of criminal intelligence material are unclear.

Failure to supervise: The organization either fails to enforce the intelligence policy or fails to appropriately oversee the personnel's actions relating to intelligence.

Lack of a privacy policy:the agency fails to provide a clear policy to safeguard people' civil liberties, civil rights, and privacy in relation to intelligence and records management operations.

Failure to follow recognized professional standards of good practicethe organization does not implement the National Criminal Intelligence Sharing Plan's guidelines or the Commission on Accreditation for Law Enforcement Agencies' intelligence standards.

DISCUSSION

Hypothetical Example: Federal Civil Rights Liability and Intelligence Records

If the regulations of the system are in accordance with 28 CFR Part 23, how might a state or local law enforcement agency be held accountable in a federal civil rights action for inappropriately keeping personal identifying information in a criminal intelligence data system?There is a possibility of negligence for failing to train if the police who were putting personal identifying information on suspects into the criminal intelligence records system were unaware that this information could not be submitted since there was no criminal link.There is a possibility of negligence for failing to train if a law enforcement agent failed to recognize that protesters were expressing their First Amendment rights to free speech.

There may also have been carelessness due to a lack of training if the officers' training was insufficient to educate them how to perform their duties correctly.There is a possibility of negligence for failing to oversee if a supervisor failed to keep an eye on the data being input into the system or failed to amend data that was entered incorrectly.There is a possibility of negligence for negligent retention if a law enforcement personnel plainly did not comprehend the policies of the intelligence unit, did not respect/follow the policies of the intelligence unit, or was unable to adequately implement the rules.

There may be negligence for failing to direct if command-level individuals become aware of inappropriate information being gathered and maintained but do nothing to fix the issue.The actions and procedures that come from the willful indifference are those that consistently fail to defend civil rights and freedoms. The following are some instances of actions or behaviors that show persistent neglect. Preserving data that identifies individuals or groups in cases where there is no convincing proof of a criminal connection. Profiling that is entirely focused on characteristics like race, religion, ethnicity, or country of origin rather than actions that have a connection to crime. Sharing information with other law enforcement organizations that names individuals or groups and suggests criminal activity when neither a criminal predicate nor the recipient's need for the information has been established.Losing a civil rights lawsuit may be expensive, humiliating, disruptive to operations, and result in major new limits on intelligence activity, as shown in the New York and Denver instances. As can be shown, with the right policy, training, and monitoring in place, this may be readily prevented.

Transparency in the Process

Making ensuring that the intelligence process is open and transparent is a crucial step in establishing public support for the intelligence function while also reducing claims of improper behavior. A news statement from the Massachusetts ACLU about the debut of the state's intelligence fusion center highlighted the need for openness. The statement particularly said the following in order to voice its concern over the function and operations of the center:We need a great deal more details on the specific tasks the fusion center will do, the data they will be gathering, who will have access to it, and the safeguards that will be put in place to avoid misuse.

These queries are logical and simple to respond to. Many conflicts, rebukes, and skepticism may be avoided by simply delivering this information to the community through a public information sheet or in town hall presentations. Uncertainty causes citizen anxiety, which leads to distrust and improper behavior accusations. These conflicts may be eased by educating the public about the

information gathering process.An imaginary example is a court's decision about a criminal intelligence records system.

A federal funding was used to create a SAR records system for a local law enforcement department. The SAR system is not a criminal intelligence records system, according to the agency's stated policy. Is it possible that the 28 CFR Part 23 regulations would apply to this SAR data system? This may happen as a consequence of a lawsuit, in theory. A plaintiff may, for instance, initiate a federal civil rights case against a law enforcement organization on the grounds that the latter is gathering, holding, and spreading criminal intelligence in the form of personally identifiable information. According to the lawsuit, the new records system is essentially a criminal intelligence records system that hides its true nature by claiming that the data is "only in SARs."

The government will undoubtedly claim that SAR records are not criminal intelligence records and that 28 CFR Part 23 only pertains to the criminal intelligence records system in its response to this complaint [4]–[6]. If the plaintiffs are successful in demonstrating that the employees assigned to the intelligence unit and intelligence analysts are the main users of the SAR system, this might be convincing. Additionally, if the law enforcement agency practices "Intelligence-Led Policing," in which intelligence analysis pervades law enforcement operations and operational decision-making, this might be additional proof that the SAR system is in fact criminal intelligence. The argument would go on to say that the way the system is utilized is the only factor that matters, not what the law enforcement agency labeled the system.If these defenses were successful, the court may decide that, regardless of what the law enforcement organization labeled the SAR system, it is in fact a criminal intelligence records system. Consequently, the rules of 28 CFR Part 23 may be applied to the SAR system as part of a settlement or injunctive relief.

The National Criminal Intelligence Sharing Plan, the Law Enforcement Intelligence Unit File Guidelines, and various intelligence training programs developed with funding from the Bureau of Justice Assistance56 and the Department of Homeland Security Training and Exercise Integration have all been instrumental in helping many SLTLE agencies reengineer their intelligence capacities in recent years. The constitutional safeguards for civil rights are covered in these intelligence operations, but new problems are arising that raise fresh concerns about misuse.

Concern is growing in especially about the ISE58, which is a result of the 2004 Intelligence Reform and Terrorism Prevention Action. The executive implementation of IRTPA is created to increase information sharing across all levels of government, including exchanging terrorist information between the Intelligence Community and SLTLE agencies. It is largely based on the recommendations of the 9/11 Commission Report. Of course, the motivation was to make sure that America would have the knowledge and capacity to make connections should a danger from terrorism materialized. Even though the measure was intended to safeguard America from terrorism, many detractors thought it went too far.

Three key areas where civil rights concerns are present develop in order to solve these various problems:

1. Make sure that information is gathered and stored in a criminal intelligence records system in a way that is appropriate, both legally and morally.

2. Ensure that any information that has been gathered and stored is secured in accordance with each individual's right to privacy.
3. Make sure data security and quality integrity are maintained.

Although there are other intelligence-related concerns with civil rights implications, these are among the most important and difficult. It should be emphasized that these concerns apply to data and records that include personal information. Make sure that data collection and storage in a system of criminal intelligence records are done properly, legally, and morally. As previously said, SLTLE agency' legislative competence to execute the law gives them the right to conduct any kind of intelligence activities. As a result, any data that is gathered and kept in a system of criminal intelligence records must be grounded in criminal predicate; more specifically, it must be shown that there is a connection between the individual named in such records and illegal action. The degree of that connection must go beyond simple suspicion; there must be stated, reasonable suspicion connecting the accused person to a particular criminal act.Make sure that the information that has been gathered and stored is safeguarded in terms of privacy. The protection of people' civil rights involves many different factors, one of which is making sure that information on individuals is gathered and held with appropriate legal justification.

A written, public statement that outlines an organization's perspective on how to handle personally identifiable information that it collects and uses in the regular course of business is known as a privacy and civil liberties policy.These include the State and Local Anti-Terrorism Training Program, the Criminal Intelligence Commanders Course, and the Criminal Intelligence for the Chief Executive courseas at the time of writing, is being prepared. Law enforcement organizations need to have safeguards in place to ensure that sensitive information is not disclosed to anyone who do not have a need or a right to know it, including appropriate training, rules, procedures, monitoring, and punishment. A privacy policy must be created and put into effect with the appropriate protections. This policy must have a precisely outlined disciplinary procedure that demonstrates harsh, prompt, and definite punishments for sworn members who violate the policy's rules.

Make sure data security and quality integrity are maintained. The term "data quality" describes the procedural controls that make sure that unprocessed data is gathered and recorded in a legitimate, dependable, and impartial way. Its goal is to increase the reliability of the raw data that will be included into the intelligence records system. Security involves procedures and controls that prevent access to and dissemination of information to those who do not legitimately need to know it. Without disclosing the content of the intelligence obtained, such security procedures strengthen the formal safeguards of personal privacy rights. Procedure above content is a general policy tenet that may be communicated to the public to reduce distrust while without jeopardizing an agency's efforts to safeguard data quality.

Actions to Ensure Civil Rights Protection for Citizens

There have been discussions on a broad variety of topics that reflect hot-button legal problems in relation to police enforcement intelligence efforts. A variety of methods might be quickly put in place to guarantee that civil rights safeguards are maintained while addressing opponents of intelligence's worries.

1. **Implementing Policy:**Every law enforcement organization needs to implement a privacy policy, a security policy, and a recognized records management policy, like the LEIU

criminal intelligence file guidelines.60 Relying on the policy models and policy development procedures advised by the Global Intelligence Working Group offers a strong foundation on which to show that the organization complies with recognized national standards. This provides two benefits: First, it serves as proof to the public that the law enforcement agency's intelligence strategy is in line with accepted national standards. Second, the fact that the agency's regulations are in line with generally accepted best practices may be utilized as an affirmative defense in court.

2. **Training:** Three essential stages exist in training. First and foremost, every agency should adhere to the NCISP's training guidelines and the Minimum Criminal Intelligence Training Standards, which include a program on intelligence awareness for all officers.61 Secondly, in addition to these training requirements, the agency's appropriate personnel should receive training on agency policy and fusion center policy pertaining to all facets of the intelligence function. Special consideration should be given to the collection, the distribution of intelligence as well as unique topics including SARs, adolescent intelligence, and other unusual types of information. Last but not least, as was already said, sworn professionals need to understand the seriousness of constitutional rights abuses as they relate to intelligence collecting. Similar to other pressing police concerns, these offenses must be treated with zero tolerance. This policy makes it clear to the community and to law enforcement officers that civil rights breaches will not be tolerated and that swift disciplinary action will be taken.
3. **Supervision:** An agency must make sure that rules and procedures are being followed as intended; having good regulations and training alone won't solve the problem. There is a lack of institutional accountability and consistency when it comes to meting out appropriate sanctions if staff are not adhering to policy or are misinterpreting it. Street-level managers are responsible for upholding the highest professional standards, particularly when it comes to intelligence collecting, and for being diligent in their agency's adherence to constitutional policing. Plaintiff lawyers just need to show jurors that lower-level supervisors and their superiors knew or should have known about the violations and purposefully decided not to take disciplinary action when patterns and practices of civil rights abuses are found over time. For law enforcement agencies that have chosen to turn a blind eye when people or other officers have reported potential civil rights abuses, deliberate indifference has proved to be extraordinarily expensive.
4. **Education in the public:**Informing the public on law enforcement intelligence programs is a crucial component of their effectiveness. Again, there are two very important causes for this. The first is to simply inform the public about the intelligence process, as was mentioned before in relation to the concerns of the ACLU. This gets rid of incorrect predictions and second-guessing. A large portion of the general population believes that law enforcement agencies engage in broad covert information gathering and function similarly to the intelligence community. The Intelligence Process may get a lot of support if this misunderstanding is cleared up. The second advantage of public education is that it helps the information-gathering process by educating civilians about the telltale symptoms and symbols of terrorism [7]–[9].For instance, the Regional Community Policing Institute at Wichita State University offered community training on terrorism and intelligence to enlighten the community on what to look for and how to report the information via a trial program in collaboration with multiple police agencies in Kansas. Participants in the training got instructions on how to submit their observations to law

enforcement, how to identify markers of conduct that were regarded suspicious, and how to use a document named Observe- Document- submit. This methodology also lessens residents' mistrust in their agency's attempts to fight crime and terrorism and gives them a sense of involvement in the security of their own neighborhood.

5. **Transparent Methods:**An American law enforcement agency's intelligence division should have open procedures that are easy to understand. Although some of the data utilized in the intelligence function must be protected, the process itself must be transparent. opponents ofAn agency that is open and transparent about how the Intelligence Process functions, including relationships of an agency with other organizations, such as a fusion center, can successfully counter this argument. Law enforcement intelligence argue that the Intelligence Process is secretive and that there is widespread spying on citizens. An agency's attempts to inform its residents about the measures used for information collecting and its data storage practices may go a long way toward getting buy-in from the populace policed without disclosing the content of intelligence records.
6. **Audits of Accountability:**The regular internal auditing of an agency's intelligence operations need to be a requirement. There can be a two-step procedure required. A manager or supervisor must first examine and record the intelligence procedures using a known checklist of variables65 that is presented in the form of an inspection report. A balanced, independent external auditor, such as a retired judge or other well-respected person, would then analyze the report and challenge both the auditor and chief executive. Another crucial point is that the audit should be seen as a constructive process intended to find problems or issues that may be fixed. A proactive measure like an audit may guarantee that all processes are carried out in accordance with the constitution's requirements. It may reveal unanticipated issues and provide as concrete proof that the agency is acting honestly and without malice.
7. **Always act with integrity:** Every action taken by the agency and its employees should be able to unequivocally show that the choices made during the gathering of intelligence are specifically designed to adhere to legal requirements. Good faith may be shown in a number of ways, such as by putting policies and procedures into practice, educating staff members, and making sure that the right kind of monitoring is being carried out. There are several gray areas in the intelligence process where clear legal advice is often lacking. The likelihood of negligence is decreased by these good faith actions if the framework is in place to assist staff in making the best discretionary judgment that upholds community safety while protecting individual rights.
8. **Aid from Legal Counsel:**When assessing an officer's actions in retrospect, the case law for police misconduct focuses on principles of best police practice such good faith, reasonableness, and judgment without malice. In most cases, juries will give the officers the benefit of the doubt since they generally do not want to find them responsible for the claimed wrongdoings or policy breaches. However, an agency's legal counsel may find it challenging to defend one of its own against a claim of civil rights breaches in a court of law without clearly written regulations, in-depth training scenarios, and proof of an organization's rigorous compliance with constitutional law concerns.

The greatest preventative strategy that agencies may take to be ready for litigation involving claims of civil rights violations may be to hire competent legal counsel. An attorney knowledgeable in municipal law, 1983 actions, and police misconduct cases can help draft an

agency's privacy and security policies as well as the procedure for gathering and analyzing intelligence data, whether they work as a sole practitioner or the legal counsel for an insurance carrier. With this strategy, an agency may be certain that every reasonable measure has been made to adhere to the most recent Supreme Court decisions about the best police tactics in light of society's growing need for vigilant police protection in the wake of 9/11. Police ethics instructors have previously utilized arbitration awards and case law cases to illustrate instances of wrongdoing by officers that led to suspensions or terminations. In order to engage police trainees in discussion on both best practices for police work and the necessity to properly adhere to constitutional requirements for police work, municipal legal experts may create street-level scenarios [10]–[12].

CONCLUSION

Law enforcement officials confront new hurdles in handling sensitive information and intelligence in the rapidly changing world of information sharing, which is increasingly being driven by intelligence fusion centers and the information-sharing environment. Professional law enforcement embraces the duty of defending the community and the civil rights of individuals. Additionally, this same environment will come under more scrutiny by civil rights advocates to make sure that the information that law enforcement agencies gather, keep, and distribute is done so in a legal way. We have the information and resources necessary to defend both the rights of the public and the community.

This conversation was intended to make sure that these tools are taken into consideration and put into context. Overall, the achievement of both goals depends on careful consideration of the relationship between federal civil rights responsibility and intelligence. We can guarantee that intelligence operations are carried out in a way that respects civil rights safeguards and promotes our democratic ideals and principles by creating clear regulations, standards, and supervision procedures.

REFERENCES

[1] S. French, “Genetic testing in the workplace: the employer’s coin toss.,” *Duke Law Technol. Rev.*, 2002.

[2] S. R. Klein and C. M. Flinn, “Social Media Compliance Programs and the War Against Terrorism,” *SSRN Electron. J.*, 2016, doi: 10.2139/ssrn.2833368.

[3] E. B. Bazan, “The foreign intelligence surveillance act: A brief overview of selected issues,” in *The Foreign Intelligence Surveillance Act and its Ramifications*, 2010.

[4] N. I. Kozak, “Fighting for the Internet: Online Blackout Protests and Internet Legislation in the United States, 1996-2018,” *M/C J.*, 2018, doi: 10.5204/mcj.1415.

[5] K. J. M. Baker, “How Colleges Flunk Mental Health,” *Newsweek*, 2014.

[6] J. A. Laub, “Assessing the servant organization; Development of the Organizational Leadership Assessment (OLA) model. Dissertation ABSTRACTs International,” *Procedia - Soc. Behav. Sci.*, 1999.

[7] J. A. Laub, “Assessing the servant organization; Development of the Organizational Leadership Assessment (OLA) model,” *Diss. Abstr. Int.*, 1999.

[8] C. C. Cantarelli, B. Flybjerg, E. J. E. Molin, and B. van Wee, "Cost Overruns in Large-Scale Transport Infrastructure Projects," *Autom. Constr.*, 2018.

[9] C. Doyle, "Privacy: An overview of the electronic communications privacy act," in *Privacy: Select Issues and Laws for the 21st Century*, 2013.

[10] E. B. Bazan, "The foreign intelligence surveillance act: An overview of selected issues*," in *The Foreign Intelligence Surveillance Act*, 2013.

[11] A. Bris *et al.*, "Knights, Raiders, And Targets - The Impact Of The Hostile Takeover - Coffee,Jc, Lowenstein,L, Roseackerman,S," *J. Bank. Financ.*, 2021.

[12] M. S. Khan and S. Dash, "A Study of Impact of Motivation on Productivity of Employee," *Int. J. Bus. Manag.*, 2014.

CHAPTER 14

INTELLIGENCE FUSION PROCESS

Bhirgu Raj Maurya, Assistant Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-brmourya.mourya321@gmail.com

ABSTRACT:

The intelligence fusion process involves the integration of information from multiple sources to produce a comprehensive and accurate picture of a particular situation or threat. This process is critical for ensuring that decision-makers have access to timely and relevant information that can inform their actions and help them to address potential threats to national security. The intelligence fusion process typically involves the collection of information from a variety of sources, including human intelligence, signals intelligence, open-source intelligence, and geospatial intelligence. This information is then analyzed and integrated to produce a comprehensive intelligence product that provides decision-makers with a clear understanding of the situation or threat.

KEYWORDS:

Fusion Center, Information Sharing, Intelligence Cycle, Situational Awareness, Threat Assessment, Unified Approach.

INTRODUCTION

The technique of intelligence fusion is a recent development in the development of law enforcement intelligence. For the majority of state, local, and tribal law enforcement agencies, fusion centers provide a new intelligence structure that they can engage with and comprehend. Contrary to popular belief, the fusion process and the establishment of fusion centers entail more than just restructuring an existing law enforcement intelligence unit's organizational structure. It often entails either completely reengineering the conceptual structure of an agency's intelligence function or forming a brand-new entity. The development of new agreements and functional relationships, the creation of new policies and procedures, the creation of new agreements and functional relationships, and the inculcation of the Intelligence Led-Policing1 philosophy are all necessary. It also requires engaging a wide range of individuals and organizations to be contributors and consumers of the intelligence function [1], [2]. The difficulties are many, but one of the biggest is exposing oneself and one's agency to organizational change. Most people are rigid and resistant to change, yet the possibility of success is reduced if outdated habits and false presumptions are not disregarded in the development of intelligence. The discussion that follows is meant to provide light on many aspects of the fusion process as well as on some of the voiced worries about it.

Historical Overview

Initially, Regional Intelligence Centers were the most common name for intelligence fusion centers. There was no one set model for what the intelligence center performed or how it should

be structured, therefore they took various shapes around the United States. The intention was to marshal the resources and expertise of various agencies within that region to deal with cross-jurisdictional crime problems, and they evolved largely through local initiatives as a response to perceived threats related to crime, drug trafficking, and/or terrorism within a geographic region. A region was sometimes described as a county, a significant metropolitan area, a section of a state, or an entire state.

In the 1980s, anti-drug activities gave rise to the first RICs. In fact, the intelligence centers in High Intensity Drug Trafficking Areas 6 provided as examples of effective programs and structures as well as ways to identify systemic problems that needed to be fixed for the intelligence center to operate.7 The Bureau of Alcohol, Tobacco, and Firearms created a variety of programmatic initiatives to lower gun violence in the late 1990s. ATF Regional Crime Gun Centers were created as a result of these activities. In other situations, the centers shared space with the HIDTA RIC and performed a variety of intelligence-related tasks, such as analyzing trace data to find gun traffickers, disseminating information about possible leads, and working together with the HIDTA RIC to track down gun and drug traffickers.8 The HIDTA and ATF intelligence centers interacted with SLTLE authorities often in almost all instances. The goal was to fuse, or integrate, data from various sources in order to better comprehend and address the issues associated with multijurisdictional crime.

This created the framework for intelligence centers, but apart from peculiar local crime problems, there wasn't much motivation to grow the centers. Obviously, after September 11, 2001, this changed.Additional state and municipal organizations adopted the idea and started creating their own centers as a result of their proven effectiveness and the information-sharing difficulties associated with counterterrorism. State and municipal governments first created these facilities. The federal government, first via the Department of Homeland Security, recognized the importance of these efforts and started to assist them financially. The function of fusion centers was going to change.

The Program Manager for the ISE, the Department of Homeland Security, and the Department of Justice are taking steps to partner with and leverage fusion centers as part of the overall information-sharing environment. They do this because they recognize that state and local fusion centers represent a crucial source of local information about potential threats as well as a mechanism for providing terrorism-related information and intelligence from federal sources.Taking this remark as a starting point, the Government Accountability Office's study detailed a variety of government initiatives that are being made to help fusion centers and resolve any problems or barriers that the directors of fusion centers have highlighted. They consist of the following:

Actions have been made by the DHS, FBI, and PM-ISE to help fusion centers manage and get access to a variety of government information systems, including classified systems.Both the DHS and the FBI have pledged to provide security clearances to employees at state, municipal, and tribal fusion centers and to speed up the clearance processing process. Through the placement of federal workers in state fusion centers and some budgetary assistance from the DHS, the FBI and DHS are helping fusion centers find and keep suitable staff.To facilitate quicker and simpler grant awards, federal monies supporting fusion centers have been more accessible and simplified in their administration.In order to encourage the growth and maturity of fusion centers, the DOJ and the DHS have both provided technical help and training.Although

there has been progress, many fusion centers and their governing officers seem to feel that there is still more work to be done before fusion centers can effortlessly play the function they are intended to play.

DISCUSSION

Refining the Fusion Center Concept

After the terrorist attacks of September 11, it became evident that there had been inadequate information sharing within and across all tiers of law enforcement. It became painfully clear that present information systems and procedures were simply unable to handle threats of this sort when additional details about the terrorists' minor run-ins with state and local law enforcement in the weeks and months before to the attacks emerged. It was also obvious that if a wide variety of raw data were gathered by various agencies, a system for data integration and analysis would be necessary to make its meaning useful to operational law enforcement officers [3], [4].

State and local law enforcement officials began to realize that the lessons learned from the RICs and HIDTAs may be used to combat terrorism. The FBI, the DHS, and the fusion centers communicated with one another to construct fusion centers more holistically since two-way information exchange with federal law enforcement and the intelligence community were required. "Federal departments and agencies, including DHS, FBI, and DOD, launched efforts to develop strategies to incorporate these fusion centers into their information and intelligence activities," it is true.

The claim that fusion centers are an essential component of our country's homeland security is supported by at least four suppositions:

1. Terrorist attacks may be prevented in large part via the use of intelligence and the intelligence process.
2. To build a more complete picture of the danger, it is crucial to combine a wider variety of data, including data from unconventional sources.
3. Public sector organizations and state, municipal, and tribal law enforcement are in a unique position to make observations and gather data that might be crucial to the danger assessment mentioned above.
4. State and local communities, as well as maybe the whole country, can gain by having fusion activities take place at the sub-federal level.

A handful of the new fusion centers, like the Georgia Information Sharing and Analysis Center, still have terrorism as their exclusive area of focus. The majority of the centers expanded their scope to include "all crime and all threats" due to two factors. First, it was acknowledged that concentrating just on terrorism may overlook certain crucial signs since the majority of terrorist attacks had a connection to other crimes. Second, it was acknowledged that the fusion process would be helpful in addressing a range of crimes, particularly criminal enterprises that were cross-jurisdictional and constituted sophisticated criminality.

The duties of fusion centers are now evolving to include an all-hazards perspective. Two factors led to the inclusion of the all-hazards approach: the first is a consequence of the all-hazards-specific special requirements on certain DHS funding to fusion centers. Mandates from the state or governing board of the fusion center are the second source. Complex criminality is the term used to describe criminal businesses that engage in a variety of illegal acts to sustain their main

business. For instance, a drug trafficking organization may engage in drug manufacture, drug trafficking, money laundering, smuggling, government corruption, fraud, and other crimes.The Homeland Security Advisory Council saw that fusion centers were progressively fusing the ideas of existing law enforcement intelligence operations with the "all-crimes, all-threats, all-hazards" model of intelligence.

For state, tribal, and municipal institutions, intelligence/information fusion will help continuing efforts to address non-terrorism-related challenges even if its main focus is to detect, prevent, and react to developing terrorism-related threats and dangersenabling state and local organizations to more accurately discover and predict new trends in crime, public health, and quality of lifesupporting proactive, interdisciplinary, risk-based, community-focused, problem-solving law enforcement and other activitiesenhancing both emergency and non-emergency service delivery. Due to the many requirements and external factors that would impact a center's structure, procedures, and outputs, there is no one model of a fusion center. The construction and operations of fusion centers will vary dramatically between states with a huge geographical mass, a large population, and international boundaries, like Texas and California, and those with a rural population that is mostly landlocked, like Wyoming or Nebraska.

In a study, the Congressional Research Service noted that concerns have been raised about the existing and/or future effectiveness of fusion centers. There does not seem to be a "one-size-fits-all" structural or operational model for fusion centers, according to the paper, given the expansion of fusion centers in state and local governments without a coordinated national framework. The CRS report reflects a centralized government viewpoint that assumes the absence of a unified model is a serious issue. Local and state perspectives are considerably different. In fact, it is preferable to be able to create a fusion center around local demands since this enables state and local agencies to shape the fusion center into a model that best matches the requirements and difficulties that are particular to each jurisdiction. In discussing the New York State Intelligence Center, Johnson and Dorn stated the following:

To avoid duplication of effort by many agencies, one center for intelligence and terrorist information should be established. This center should consolidate and transmit information to law enforcement authorities across the state. A complete image of criminal and terrorist networks is also provided by the one state fusion center that serves the whole New York law enforcement community. This assists in the prevention of future terrorist attacks and lowers crime. Fusion centers are also constructed differently as a result of governmental or administrative directives, following the same line of reasoning. For instance, the mandate for the fusion center in Montana is to focus on "all threats," while emergency operations and fusion are also included in the New Jersey Regional Operations Intelligence Center, all crimes are the focus of the Massachusetts Commonwealth Fusion Center, and the Oregon Terrorism Intelligence Threat Assessment.

The network focuses only on terrorism. Due to practical need, the intrinsic nature of local governance, and states' rights viewpoints, fusion center architectures vary widely.Regardless of the aim of the center, national professional standards have been set that describe good practice in crucial administrative areas, despite the fact that the structure and operating procedures of fusion centers may vary. The Fusion Center Guidelines are meant to achieve this. Contrary to certain complaints, the fact that fusion centers are organized differently is a strength rather than a drawback. It serves as an example of how each center is created to fit local and regional demands and to integrate the fusion center with current organizational components in the best way

possible.For instance, the Michigan State Police is in charge of enforcing criminal and traffic laws throughout the whole state. The Michigan Intelligence Operations Center is hence administratively assigned to the state police.

Florida, however, has two main state law enforcement agencies: the Florida Department of Law Enforcement, which is in charge of criminal law enforcement, and the Florida Highway Patrol, which is in charge of traffic law enforcement. As a consequence, the FDLE Office of Statewide Intelligence is established to include the Florida Counter Terrorism Intelligence Center. The two states designed their fusion center to meet organizational structures and functional tasks as effectively as possible. The important thing to remember is that there are several operational and functional models of law enforcement used throughout the country. Fusion centers will have difficulties in meeting the particular demands of the jurisdictions they serve since they are components of state or municipal governments. As shown in a study:

Fusion bases its decisions on the kind of analytical product it will generate and for whom on its goal and its clients. Not every fusion center will need the same level of tactical or strategic research, but in order to decide what to create, they must first understand the demands of their clients and take steps to ensure that they are informed about the differences between the two products. Fusion centers will also need to decide how to include the community of first responders. Because providing for the demands of the emergency responder community and gathering all-hazards information are not conventional duties for the law enforcement intelligence function, this final criterion will likely be the most difficult to describe. It is being established certain guidelines to help fusion centers in this area via the designation of "baseline capabilities."

Baseline Capabilities for Fusion Centers for Intelligence

Fusion centers will act as the connection between SLTLE and the federal Information Sharing Environment for the exchange of terrorist information as a consequence of national initiatives that aim to improve the efficiency and efficacy of information-sharing operations. In order to address the information demands of all users of the different intelligence centers, it was recognized that there was a need to identify core baseline operating capabilities that should be employed by fusion centers and large metropolitan area intelligence units. a collaborative undertaking of the Program Manager-Information Sharing Environment, the Global Intelligence Working Group, and the Departments of Justice and Homeland Security of the United States working on the project at the moment. In the end, a companion document to the Fusion Center Guidelines will be created, outlining the components needed to integrate state and significant metropolitan area fusion centers into the overall national information sharing environment. The project is based on the capabilities of the fusion process described in the 2007 Fusion Center Assessment.

Supplemental Resource for the Fusion Capability Planning Tool, 2007 and 2008 Homeland Security Grant Program. The National Criminal Justice Act, the Fusion Center Guidelines, and the 2007 Assessment are being used as a guide in developing the baseline operating requirements that will be defined in the project. Information Sharing Environment Implementation Plan, the Intelligence Sharing Plan, and the U.S. National Preparedness Guidelines and Target Capabilities List of the Department of Homeland Security. The requirements of the National Strategy for Information Sharing will serve as a framework for developing the basic capabilities for fusion centers based on the direction provided by these national standards. The baseline capabilities

constitute a thorough articulation of functional requirements and performance objectives and are structured in accordance with the Fusion Center Guidelines. Baseline capabilities for Critical Infrastructure and Key Resources have been created as an addition to the Baseline Capabilities for State and Major Urban Area Fusion Centers, albeit the capabilities had not yet been given the go-ahead for implementation at the time of writing. Additionally, the Fire Service Intelligence Enterprise and public health baseline capabilities have been built. The all-hazards duties of fusion centers are supported by these supplementary publications. The reader should keep an eye on the National Criminal Intelligence Resource Center 21 and/or the Global Justice Information Sharing Initiative website 20 for the latest version of the Baseline Capabilities for State and Major Urban Area Fusion Centers supplement, which has been officially authorized.

What Is Fusion Intelligence?

According to the GIWG national Fusion Center Guidelines, a fusion center is a joint effort between two or more agencies that offers resources, knowledge, and/or information to the center in order to maximize its capacity for criminal and terrorist activity detection, prevention, capture, and response. A fusion center's intelligence component focuses on the intelligence process, which involves gathering, integrating, assessing, analyzing, and disseminating information. Information from nontraditional sources of intelligence collection, such public safety agencies and private sector groups, may be "fused" with law enforcement data to provide valuable insight on threats and criminal behavior.

The fusion process, which relies on the active participation of state, local, tribal, and federal law enforcement agencies and occasionally nonlaw enforcement agencies to provide the raw data for intelligence analysis, is an overarching methodology for managing the flow of information and intelligence across levels and sectors of government. There will be more accurate and comprehensive analysis that can be shared as intelligence as the variety of information sources grows. The intelligence process24 is used by information fusion to handle and analyze information. The actual spot where the fusing process takes place is the fusion center.

Despite the fact that the term "fusion center" is often used, many people are misinformed about what it really does. Most people have the impression that the center is a big space filled with workstations where employees are always answering questions from cops, investigators, and agents. Not an intelligence fusion center, but rather a "watch center" or "investigative support center," is truer in this perspective. Another widespread misunderstanding is that the fusion center is understaffed until a crisis occurs, at which point personnel from various public safety organizations congregate to staff workstations to handle the emergency. An "emergency operations center," not a "intelligence fusion center," is what this is.

The fusion center is primarily a support center rather than an operating center. Analysis is what drives it. The fusion process actively strives to recognize and prevent risks to national security and law enforcement.The core of the intelligence process is prevention. However, the fusion center differs in that it is often set up by combining officials from several federal, state, local, and tribal law enforcement organizations into a single physical facility. Each representative should act as a conduit for raw data from his or her agency, incorporating agency-specific data into the overall body of data for analysis. In contrast, when the fusion center requires intelligence, the representative acts as a channel to the agency to relay, track, and process the new information requirements. The agency representative also makes certain that analytical outputs and threat data are provided back to

the parent organization for appropriate distribution. Although agency representatives often referred to as terrorism liaison officers or intelligence liaison officers may be physically assigned to the center, it is more typical for them to carry out their fusion center duties in addition to their other duties at their home agency.An intelligence fusion center must, in essence, be able to: 1. access and peruse any government databases, including those for law enforcement, regulation, and intelligence; 2. integrating the data from various databases; 3. Make your own decisions on that knowledge; 4. Give a warning.

Use of ATIX by the Delaware Information Analysis Center

The Delaware Information Analysis Center approaches information exchange and homeland security pro-actively. The Automated Trusted Information transmission portal is used by the DIAC to connect with all of its local law enforcement partners and private sector critical infrastructure partners through the Internet in order to optimize fast, secure, two-way information transmission. In addition to content and encrypted email, ATIX offers a broad range of different threat and homeland security information. RISS.net offers ATIX as a free service; all you need is an Internet connection and the safe ATIX/RISS.NET software to use it. In order to make sure that only DIAC and its partners have access to specific information, users, like DIAC, are also able to create secure information exchange "communities". The Delaware fusion center is

The employment of ATIX by DIAC in its proactive approach to local law enforcement has been a key component of its success.Of course, not every law enforcement organization can provide a worker for the fusion center. Instead, the center must create systems for two-way information exchange that gather data from unconventional sources and provide threat-based intelligence and information needs to people who need them. As a consequence, various technologies and tactics must be created for varied two-way information exchange. Electronic two-way information exchange using a number of secure electronic information systems, such the Regional Information exchange System Network, LEO, Homeland Security Information Network, National Law Enforcement Telecommunications System 32, or ATIX33, may be very efficient. In the case of ATIX, users from the commercial sector and other groups that have a legitimate need may also have access to the system and utilize it for safe two-way information exchange. Operation Nexus of the New York Police Department is another such.

Operation Nexus, run by the New York City Police Department, is a network of companies and organizations working together throughout the country to stop further terrorist attacks against our people. Our detective agencies have collaborated with us on this project. Operation Nexus participants are devoted to reporting dubious business interactions that they suspect may have ties to terrorism. The NYPD is concerned that terrorists may pose as genuine clients in order to buy or rent certain items of equipment or to get official training in order to gain valuable knowledge or credentials. The NYPD actively encourages business owners, operators, and their staff to use their specific business and industry knowledge and experience against each customer transaction or encounter to identify anything unusual or suspicious and to report such instances to authorities through Operation Nexus [5], [6].

In the United States, a new model has evolved and is being used more often. The Terrorism Early Warning organization, established in Los Angeles, has a variety of purposes, one of which is assisting the intelligence fusion center.In order to create a variety of intelligence products at all stages of reaction that are individually targeted to the user's operational function and needs, the Los Angeles TEW comprises analysts from local, state, and federal agencies. To assist strategic

and tactical users, the TEW connects operational and criminal information. Using input and analysis from a multidisciplinary, interagency team, the TEW aims to detect emerging dangers and give early warning as part of this process. To this end, the TEW has established partnerships with the private sector to comprehend threats to critical infrastructure, built local networks of terrorism liaison officers at law enforcement, fire, and health agencies, and developed and improved processes to analyze and synthesize threat data to support its client agencies. No of the manner of distributing information, these are the crucial elements: 1. Raw materials must be diversified; 2. It has to be examined; and 3. The proper consumers must be informed about actionable intelligence output.

Fusion Facilities

A wide variety of true and accurate raw data forms the basis of competent intelligence analysis. The quality of the analytical results increases with the robustness of the raw data. The typical law enforcement intelligence unit has a limited bandwidth, meaning that information is gathered from a relatively small number of sources, which restricts the quality of the analysis and the capacity to see the big picture of a criminal enterprise. Simply said, the bandwidth is considerably larger if the number of sources is increased to include a diverse variety of agencies reflecting far greater geographic and jurisdictional constraints. The more restricted the intake of raw information, the more limited the quality of intelligence. Wider bandwidth results in a more significant and varied information flow. The analysis improves in accuracy and utility as more information is exchanged. The capacity to stop or reduce a terrorist organization's or criminal organization's activities becomes exponentially more possible as analysis quality improves.

The stovepipe of information in agencies has been identified as a problem in recent analyses of both law enforcement and national security intelligence operations36. Each agency would accumulate a sizable body of information and analytic products that it would keep and infrequently share with other agencies. Analysis was often restricted to data from internal sources, and it was also widely disseminated inside. As a consequence, agencies simply piled and stored information in isolation, like a stovepipe, while it was being developed. Current thinking acknowledges that information that is broadly shared for analysis may provide far greater value.

There was a need to combine as much information as possible since information from one agency may be crucial to understanding a danger when combined with information from another agency.The Heritage Foundation said that rather than just duplicating the work of current agencies, the fusion center would strengthen and improve them by offering a service that does not now exist. Another viewpoint on their growth noticed the following:Fusion centers conceptually vary from since they aim to combine data from the public and commercial sectors in addition to criminal intelligence when it comes to sources of information for analysis and integration. Fusion centers can widen the focus of state and local analyses to include concerns related to homeland security and counterterrorism.

Fusion centers reflect a major shift in the approach to homeland security and law enforcement, while being an enlargement of current sub federal intelligence/information efforts. Fusion centers have grown in popularity as unconventional players, such as state and local law enforcement and public safety organizations, have come to understand their significance to homeland defense and security. Research by the Police Executive Research Forum that examined the need for and structure of fusion centers highlighted five crucial questions:

1. Why is a fusion center necessary? Fusion centers serve as an efficient tool to make the most of available resources and forge reliable partnerships when demands rise and resources become scarce. Fusion centers represent the fundamental purpose of cooperation. Fusion centers combine data from several sources and specialties, which sets them apart from intelligence units inside local law enforcement organizations.
2. What is the purpose of a fusion center? Although there are many different perspectives on the matter, many in the law enforcement community think it makes more sense to set up a fusion center with a wider objective and scope, i.e., adopt an all-crimes or all-hazards strategy, while still preserving the special capacity to monitor terrorist activities. The benefit of an all-crime center is that it improves law enforcement's capacity to identify conventional crimes that may eventually serve as indicators of terrorist activities. A fusion center's main objective is to provide law enforcement organizations analysis of local, state, and regional activity. However, local law enforcement organizations must contribute by providing the center with information.
3. Who is in charge of the fusion centers? According to the suggestions made in the Fusion Center Guidelines, the majority of fusion centers created memorandums of understanding with participating agencies and constituted a governing board of members from these agencies to offer oversight and guarantee adherence to rules.
4. What essential tasks and services are carried out by fusion centers? Fusion centers are designed to serve as analytical hubs for public safety organizations like police enforcement. A fusion center acts as a clearinghouse for all data collected by open-source and law enforcement organizations throughout the state or area. Together, fusion centers and the organizations they serve decide on the most effective way to share center research and output.
5. How does the link between law enforcement and fusion centers define value?
    i. Giving law enforcement agencies daily information
    ii. Interpreting various threat data from a regional standpoint
    iii. Offering timely, useful information.
    iv. Making connections between several jurisdictions that have an impact on a local region.
    v. Acting as a central location for threat data.
    vi. Managing various types of information for local law enforcement authorities in a coordinated manner [7]–[9].

CONCLUSION

To guarantee that decision-makers have access to the information they need to make informed choices, the intelligence fusion process, which is a crucial part of national security, calls on the cooperation and coordination of several stakeholders. Organizations may improve their capacity to combine intelligence and successfully counter possible threats to national security by creating clear regulations, using cutting-edge technology, and encouraging a culture of cooperation and information sharing.

Organizations must develop clear rules and procedures that specify the obligations of various stakeholders and guarantee that data is gathered and shared in a way that complies with moral and legal obligations in order to assist the intelligence fusion process. Additionally, the efficiency and efficacy of the fusion process may be increased by using cutting-edge analytical tools and technologies like machine learning and artificial intelligence.

REFERENCES

[1] R. McCann *et al.*, "In-situ sensing, process monitoring and machine control in Laser Powder Bed Fusion: A review," *Additive Manufacturing*. 2021. doi: 10.1016/j.addma.2021.102058.

[2] S. Jusoh and S. Almajali, "A Systematic Review on Fusion Techniques and Approaches Used in Applications," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2966400.

[3] X. Zhao, Y. Jia, A. Li, R. Jiang, and Y. Song, "Multi-source knowledge fusion: a survey," *World Wide Web*, 2020, doi: 10.1007/s11280-020-00811-0.

[4] T. Baltrusaitis, C. Ahuja, and L. P. Morency, "Multimodal Machine Learning: A Survey and Taxonomy," *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2019. doi: 10.1109/TPAMI.2018.2798607.

[5] Z. Liu, G. Shi, A. Zhang, and C. Huang, "Intelligent tensioning method for prestressed cables based on digital twins and artificial intelligence," *Sensors (Switzerland)*, 2020, doi: 10.3390/s20247006.

[6] Y. Pan and L. Zhang, "Roles of artificial intelligence in construction engineering and management: A critical review and future trends," *Automation in Construction*. 2021. doi: 10.1016/j.autcon.2020.103517.

[7] D. L. Hall and J. Llinas, "An introduction to multisensor data fusion," *Proc. IEEE*, 1997, doi: 10.1109/5.554205.

[8] S. Mao, B. Wang, Y. Tang, and F. Qian, "Opportunities and Challenges of Artificial Intelligence for Green Manufacturing in the Process Industry," *Engineering*. 2019. doi: 10.1016/j.eng.2019.08.013.

[9] M. R. Belgaum, S. Musa, Z. Alansari, M. M. Alam, and M. S. Mazliham, "Impact of Artificial Intelligence-enabled Software defined Networks in Infrastructure and Operations: Trends and Challenges," *Int. J. Adv. Comput. Sci. Appl.*, 2021, doi: 10.14569/IJACSA.2021.0120109.

CHAPTER 15

FUSION CENTERS AND THE CRIME LABORATORY: AN ANALOGY

Aruno Raj Singh, Assistant Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-arunorajsingh@gmail.com

ABSTRACT:

Fusion centers and crime laboratories are two important components of the criminal justice system that play a critical role in the collection, analysis, and dissemination of information that can help to support law enforcement efforts. While these two entities may seem very different at first glance, there are a number of similarities that make them useful for understanding one another. Both fusion centers and crime laboratories are designed to collect and analyze information from a variety of sources in order to provide law enforcement with actionable intelligence that can support their efforts. Fusion centers typically focus on the collection and analysis of information related to terrorism and other national security threats, while crime laboratories are primarily focused on the analysis of physical evidence in criminal investigations.

KEYWORDS:

Fusion center, Information sharing, Intelligence fusion, Law enforcement intelligence, Scientific analysis, Unified approach.

INTRODUCTION

A reasonably well-known comparison between the fusion center and a law enforcement organization is the crime laboratory. Although the great majority of law enforcement organizations do not have a crime lab or an intelligence division, they sometimes need forensic examination of evidence for a case. Each agency has to have some level of forensic expertise in order to appropriately gather physical evidence and use the crime lab. The agency must also be familiar with the procedures for submitting evidence for analysis, as well as having a working connection with the crime lab [1].

Most organizations employ a state crime lab. Even though a small agency may only seldom utilize the lab, forensic analysis is required when it is used. To use the crime lab's services quickly and efficiently, the local agency must have staff who have received the necessary training and access to the necessary materials. a comparison of a number of elements that apply to both fusion centers and crime labs.This comparison shows that many of the organizational procedures and standards needed for fusion centers have a history. Integrating the fusion center into law enforcement agency operations may be made considerably simpler by building on these experiences.

The development of fusion centers was accepted by the Information Sharing Environment Implementation Plan as a crucial component acting as information hubs for federal agencies,

nonfederal law enforcement, and the commercial sector.In the wake of 9/11, all states and municipalities made a strong effort to develop and finance fusion centers. These fusion centers currently have a significant impact on the gathering, analysis, and dissemination of information about terrorism. Each of these facilities is a crucial resource for gathering information on terrorism. Their collective work with one another, the Federal Government, and the business sector has significantly improved the nation's total analytical ability and the multidirectional flow of information. It is important to remember that these centers are not uniform; there are major differences in terms of how they operate and what their missions are focused on. A lot of work has gone into creating and establishing standards to make it simpler to access, share, and utilize information. As of now, more than 40 such centers exist around the United States.

A National Fusion Center Coordination Group has been formed by the PM-ISE to further this concept. It is headed by DHS and the DOJ, and its goal is to find federal funding sources to facilitate the growth of a nationwide, integrated network of fusion centers. The ISE also acknowledges the "all-crimes and all-hazards" aspect of State and local sharing, where SLT entities may combine and share numerous kinds of information to fulfill a range of requirements, including law enforcement, readiness, response, and recovery. In many cases, this information may not at first be identified as being related to terrorism, but it may still be knowledge that later proves essential in preventing, preparing for, or reacting to terrorism. These extra fusion center operations won't be hindered or interrupted by the ISE's emphasis on terrorist information [2].

DISCUSSION

Operationalizing the Fusion Process

The integrated information-sharing approach is functional thanks to three key focus points. While each element is important, the fusion core is especially vital. According to Recommendation 1 in the National Criminal Intelligence Sharing Plan, the first phase in the plan is to fundamentally build an intelligence capability in every SLTLE agency, regardless of size. A law enforcement agency's proactive involvement with the fusion center must be connected with the intelligence capability. The value of the center increases with the number of organizations who join as partners. The PM-ISE has stated that "state and major

The creation of the fusion center is simply one component; it is crucial to have mass involvement. "Urban area fusion centers will be central to implementation at the state and local levels..."The federal ISE, which includes both the Intelligence Community and federal law enforcement, is the outer ring of the 8-1 system. Both cover homeland security and national security broadly and usually at a classified level. Sharing pertinent danger information with local law enforcement is a hurdle. Similar to this, there has to be a way to properly communicate information when local law enforcement finds anything that is important to the ISE. These functions are supposed to be carried out by the main state fusion center.

The fusion center is intended to act as a communication hub for ISE and regional law enforcement. In general, the center will contain officials from all governmental levels, seasoned analysts, staff with federal security credentials, and access to a variety of information systems, sometimes including secret systems. With this foundation, the fusion center may send crucially important raw data that is gathered at the local, tribal, and private levels to the federal ISE as well as communicate key intelligence to local and tribal partners.

To achieve these goals, a streamlined fusion technique is used. Gaining support from all important state stakeholders, including law enforcement, federal partners operating inside the state, the Intelligence Community45 as appropriate for each state, and the business sector, is a crucial goal. Several agencies provide input to the fusion process. The analysts combine the many data sources and provide analytical output, which may include data forthreat assessment, target hardening, or prevention. The analysts may also specify other intelligence needs. The fusion center disseminates pertinent data and intelligence to its participants in the form of actionable intelligence after reviewing and clarifying intelligence needs.It is essential that as many law enforcement agencies as possible take part in the process for intelligence fusion to be effective. Each non-participating organization shows a gap in the capacity to recognize and stop threats.

The Fusion Method

Is the private sector playing a role?

The private sector, which is sometimes disregarded, may be a valuable source of data that gives information gathering a wider perspective. Many major organizations have highly developed security operations that keep an eye on the hazards that organized crime, criminal extremists, as well as rapacious criminals, pose to their facilities, goods, and staff on a worldwide scale. This kind of data is often distinct from that gathered by law enforcement agencies and may provide a unique, insightful element to the data set being examined by the fusion center.

Similar to this, the private sector often qualifies as a lawful recipient of information shared according to the principles of right-to-know and need-to-know. The private sector owns 85% of the country's essential infrastructure. Furthermore, the private sector employs a sizable workforce that, when given the right information, may dramatically expand the number of "eyes and ears on the street" to spot potential hazards in people and behaviors. A jurisdiction's analysis and synthesis institution should also set up procedures for exchanging information with the local business sector, according to a "Best Practices" study published by the DHS.

Of course, there are problems with information exchange that need to be addressed. For instance, it may not be permissible for law enforcement to provide certain categories of personally identifiable information to the private sector. On the other hand, the private sector will be hesitant to provide confidential information about company goods and procedures. The private sector has a genuine place in fusion centers notwithstanding these restrictions. Memoranda of Agreement must be in place with stipulations on information-sharing procedures and limitations, much as with law enforcement partners [3].

Fusion Centers: Concerns

Centralized intelligence fusion centers have increased concerns among some citizens, as might be expected. These citizens are worried that the centers will gather, store, and spread information that will further erode the privacy of law-abiding citizens who support unpopular or contentious causes. A discussion with the neighborhood will sometimes allay the worries; other times, it won't. Nevertheless, it is critical to comprehend these grounds of contention. The main frequent objections to fusion centers are discussed next, followed by the reaction from law enforcement. The goal is to facilitate dialogue and understanding between fusion centers and detractors.

There's a problem: "There is no underlying philosophy. Fusion center development and advancement may be hindered in the lack of a consensus on what constitutes intelligence.The goal of a philosophy is to define the fundamental goals, procedures, and constraints that guide an organization's operations. There has never been a time when the ideology of law enforcement intelligence, and hence intelligence fusion centers, was more apparent. The National Criminal Intelligence Sharing Plan's explicit definition of duties and responsibilities, together with the Information Sharing Environment Implementation Plan and the DHS Target Capabilities List's additional assistance, are helping to shape the concept rather well. In fact, Fusion Center Guideline 1 instructs employees to "Adhere to the National Criminal Intelligence Sharing Plan and perform all steps of the intelligence process."48 The Guidelines established the NCISP and the standards contained therein as an unmistakable guiding principle.

The various national criteria mentioned above must be taken into consideration while evaluating the Fusion Center Guidelines. The guidelines constitute agreed national professional standards that are approved for two reasons, despite the fact that they are optional and the federal government lacks the jurisdiction to order all state and local fusion centers to comply. First, maintaining continuous professional practice is the philosophical justification. The second, more practical justification is that adopting the Guidelines shows good faith and is a sign of diligence, both of which assist shield the fusion center from legal responsibility. The Fusion Center Guidelines are optional, but they serve as the de facto national standard for tribal, municipal, and state law enforcement.

Last but not least, it is perplexing that the Guidelines "are oriented toward the mechanics of fusion center establishment." According to the idea outlined above, national standards for the mechanics of fusion centers have been created in order to assist assure uniformity, efficiency, and effectiveness. This is a responsible, proactive, and effective reality. In fact, the Guidelines serve as crucial checkpoints for fusion centers to assist guarantee conformity to the law. The argument that fusion centers are effectively preemptive law enforcement that information obtained without a criminal motive is illegally gathered information is often the focus of criticism. This argument is false because it is based on incorrect or uninformed assumptions about the role of law enforcement intelligence. Information is gathered in the initial step; intelligence is the result of the analytical process. This difference is crucial.Intelligence is undoubtedly preventative. The goal of intelligence is to stop crime from happening. Programs designed to reduce crime are all examples of proactive law enforcement. The criticism's justification is flawed from the start. A preventive response to crime wherever feasible has been a tenet of law enforcement for decades. The National Crime Prevention Council was established due to this preventative concept. Simply said, law enforcement intelligence is another aspect of prevention.

Law enforcement officials at all levels of government are highly aware of the criminal predicate standard for intelligence with regard to the worry about "illegally gathering" information. In the course of conducting intelligence operations, they follow the same privacy and civil rights regulations that they do while conducting criminal investigations. Law enforcement agencies have privacy rules, procedures for intelligence records, and training that all adhere to legal and statutory standards. Law enforcement is aware of these duties and upholds them.

Fusion centers operate in a no-man's land between the federal government and the states, where policy and supervision are sometimes ambiguous and susceptible to manipulation. Concern: "Ambiguous lines of power allow for 'policy shopping.Since all state and regional fusion centers

are extensions of state or municipal governments, they are subject to the same chain of command and have the same level of responsibility. Every fusion center has a policy handbook that outlines duties and authority, among other things. Fusion centers sometimes share space with federal organizations, most notably the FBI, but there are still established lines of authority and accountability for the administration and reporting of the fusion center to the state or local government. Some have governing boards, while others have direct reporting lines to a state office of homeland security or a municipal or state law enforcement agency. Fusion centers may have various organizational arrangements, but the lines of power are clearly defined. Simply said, insurance shopping is not a practice. Privacy and security are at danger from private sector engagement in fusion centers. The development of a "Surveillance-Industrial Complex," in which security agencies and the business sector band together in a frenzy of mass information collection, monitoring, and regular surveillance, is a significant trend that has recently emerged in the United States. Fusion centers are positioned to be a part of this movement.

In fusion centers, involving public and private partners, every non-law enforcement employee must pass a background check in order to access information. The majority hold security clearances, making them subject to both state and local privacy protection laws as well as federal rules controlling the handling of secret and sensitive information. Additionally, representatives from the private sector speak for the whole industry, not just one particular business. For instance, the Washington Joint Analysis Center and The Boeing Company came to an arrangement for Boeing to provide a Boeing intelligence analyst to WAJAC. The analyst will represent aircraft manufacturers and their suppliers at the fusion center and has a security clearance from the Defense Department.

Information is not gathered in a frenzy for the intelligence process; rather, it is gathered via clear processes that are governed by law and the scientific method of problem resolution.In fact, bulk information collecting is discouraged since it complicates the intelligence gathering process by requiring a larger volume of data to be processed through in order to detect a danger. In fact, the goal of intelligence needs is to pinpoint and gather just the data that is necessary for analysis. The significance of private sector participation in law enforcement intelligence is discussed in the National Criminal Intelligence Sharing Plan, the Fusion Center Guidelines, the Information Sharing Environment Implementation Plan, and the DHS Target Capabilities List.Each fusion center includes a privacy policy that private-sector players are required to abide by since there is sensitivity to the sorts of information that the participants from the private sector have access to. In addition, private sector partners are required to sign a nondisclosure agreement and a memorandum of understanding, both of which contribute to the protection of individual privacy.

Military involvement in fusion centers is unconstitutional since it goes against basic liberties. Those in power who see American neighborhoods as front lines in a "war" may be tempted to do away with "inconvenient" checks and balances.Although the general public may not be aware of it, military personnel who work in the field of law enforcement intelligence are very sensitive to these problems. The military does not affect law enforcement, and neither does law enforcement have this war viewpoint. legal actionThe military is merely employed by agencies as a legal support resource in the fusion centers, just as it has done for years in legal drug enforcement programs. Agencies are fully aware of the differences. Military analysts, generally from the National Guard, are assigned to fusion centers rather than intelligence gatherers or operational staff.Data mining, which is detrimental to both security and privacy, is a concern.The two methods of inquiry and analysis are distinct from one another. Data fusion is the process of

combining information from various heterogeneous sources into a single composite picture of the environment. Data mining is defined as "the nontrivial extraction of implicit, previously unknown and potentially useful information from data." It uses machine learning, statistical, and visualization techniques to discover and present knowledge in a form that is easily comprehensible to humans. Data fusion is an integration and analytical technique that increases the accuracy of analysis by relying on a wide array of diverse information sources. Generally speaking, law enforcement agencies and fusion centers have neither the resources nor the expertise for data mining activities; however, the inclusion of different agencies from different sectors can help.

Unwanted secrecy: "Fusion centers' missions are undermined by excessive secrecy.

However, the content of much of their work must remain largely secret to protect both privacy and the integrity of investigations. In some cases, levels of secrecy increase when the fusion center is accredited as a Sensitive Compartmented Information Facility.60 In these situations, there will be more secrecy, as a matter of federal law, because the facility will contain classifiable information.The ongoing skepticism, while frustrating, serves as a reminder of the need to remain vigilant in the training, supervision, and management of the intelligence process. For many people, the past abuse of law enforcement intelligence will be the lens through which all law enforcement intelligence activities will be judged. Similarly, critics need to understand the radical changes that have occurred in law enforcement organizations over the past five decades: Officers are significantly more educated, training has increased dramatically, and professional leadership has embraced modern management techniques, values, and responsibilities.

Concerns about Civil Rights and Fusion Centers

As stated in a National Governors Association best practices paper, "The risks to individuals' privacy begin when personal information of any kind is entered into criminal justice information systems."61 Criminal intelligence records systems are unquestionably included in this description and warrant special attention due to the nature of the information they contain. This problem is complicated by the fact that many privacy activists worry that the centers may lead to centralized monitoring of residents in the future since they don't comprehend the fusion process.Certainly, when an SLTLE agency is the custodian of an intelligence records' system, care must be taken to exclude information from the fusion center that does not meet the standards of 28 CFR Part 23. However, the participation of federal law enforcement agencies whose jurisdiction for information collection and retention is different from SLTLE agencies may be the greatest concern of a fusion center in this regard.Fundamentally, the privacy and civil rights concerns of individuals linked to fusion centers are the same as any other component of the intelligence process, and the pertinent NCISP requirements should be completely implemented.

How to Support and Engage Your Fusion Center

Recognize the value of information sharing; promote the sharing of information with other law enforcement and public safety organizations; and build or improve your organization's intelligence function using the NCISP's standards and action procedures.Streamline the flow of information, make sure that there are channels of communication for effectively exchanging information and intelligence, including Suspicious Activity Reports, and collaborate with the fusion center to determine a common terminology and the most efficient ways to convey this

information. Provide training sessions for everyone and explain intelligence, why it is vital, and how it helps the department to support an information-sharing culture.Train new recruits on the function of fusion centers, the significance of the mission, the types of information to gather, and the transmission of information to the fusion center.Constantly communicate your information needs and requirements to the fusion center and provide definitions for actionable information. Ensure that your agency provides feedback on the value of products distributed and offers recommendations for improvement when necessary. Communicate your needs to the fusion center or governing board.

There are a variety of models for assignment; some agencies choose to assign personnel on a part-time basis, while others serve full-time for a 3- or 6-month rotation. Assign personnel to the fusion center. Depending on the center, officers, investigators, and analysts may all be assigned and have skills and knowledge to contribute. Establish or take part in a program for terrorism liaison officers (TLOs) or intelligence liaison officers (ILOs), whose job it is to ensure that all appropriate information gathered by each agency is effectively shared with the fusion center and to disseminate information from the center to the "boots on the ground" for departments that cannot afford to lend personnel to a center. Join the governing board of the fusion center, if one exists. Participating on an interagency governing board will show the value of collaboration with the fusion center and allow for a greater understanding of its needs. Educate political leaders. Educating political leaders about fusion centers, their value, and their needs may encourage them to demonstrate commitment to the fusion concept and, thus, support your agency and that commitment through appropriate funding.

Hire analysts, if possible. Both intelligence and crime analysts require different skill sets than those required for patrol officers and investigators. Analysts can make officers work smarter, providing for both increased efficiency and effectiveness adhered to. Further, Guideline 8 of the Fusion Center Guidelines states that the management of the fusion center should: “Develop, publish, and adhere to a privacy and civil rights policy.”62 Commentary on this guideline goes on to note the following: one of the critical issues that could quickly stop intelligence sharing is the real or perceived violation of individuals’ privacy and constitutional rights through the use of intelligence sharing systems. In order to balance law enforcement’s ability to share information while ensuring that the rights of citizens are upheld, appropriate privacy policies must be in place. As a consequence, civil rights issues for fusion centers have components related to policy, training, supervision, and public information that must be addressed in the development and implementation stages [4]–[6].

CONCLUSION

In conclusion, despite their seeming differences, fusion centers and crime labs have a lot of crucial parallels that help us comprehend one another. We can improve our capacity to gather, analyze, and distribute information that supports law enforcement initiatives and works to advance public safety by identifying these parallels and using the best practices from each institution. Despite these distinctions, in order to efficiently handle and interpret the data they acquire, fusion centers and crime labs both need highly qualified analysts and cutting-edge analytical technologies. To guarantee that the data they gather is shared correctly and utilized in a way that complies with legal and ethical norms, they also need clear rules and procedures. Additionally, fusion centers and crime labs both work in dynamic contexts that need ongoing innovation and adaptability. This might include the creation of novel analytical methods, the use

of cutting-edge technology, and the formation of fresh partnerships and collaborations with other criminal justice system participants.

REFERENCES

[1] D. Dampier and J. Cohoon, "Building an education program for engineers in digital forensics," 2008. doi: 10.18260/1-2--3132.

[2] D. L. Hall and J. Llinas, "An introduction to multisensor data fusion," *Proc. IEEE*, 1997, doi: 10.1109/5.554205.

[3] P. L. Morgan *et al.*, "News.," *Pediatrics*, 2019.

[4] S. Sotome *et al.*, "Naldebain for Control of Post-Cesarean Section Pain," *Pain Physician*, 2021.

[5] P. Zhang *et al.*, "IEEE Draft Standard for Spectrum Characterization and Occupancy Sensing," 2019.

[6] B. T. Abebe *et al.*, "Mindfulness virtual community," *Trials*, 2019.

CHAPTER 16

DEVELOPING THE FUSION CENTER

Yogesh Chandra Gupta, Assistant Professor
College Of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id-cognitor.yogesh@gmail.com

ABSTRACT:

Developing a fusion center requires a strategic and collaborative approach that involves multiple stakeholders and is guided by a clear understanding of the center's mission, objectives, and target audience. Fusion centers are designed to facilitate the sharing and analysis of information from a variety of sources, including law enforcement agencies, public safety organizations, and private sector partners, in order to support the identification, prevention, and response to criminal activity and other threats to public safety.

The development of a fusion center typically involves several key steps, including the establishment of a governance structure, the definition of the center's scope and mission, the identification of key partners and stakeholders, the development of operational procedures and protocols, and the deployment of advanced analytical tools and technologies to support information processing and analysis.

KEYWORDS:

Counterterrorism, Fusion Center, Homeland Security, Information Sharing, Interagency Cooperation, Law Enforcement Intelligence.

INTRODUCTION

As was previously said, the NCISP64 and the Fusion Center Guidelines65 of the Global Intelligence Working Group should both be followed while operating a fusion center. To promote best practices, efficient operations, and respect to civil rights, the NCISP offers standards for all facets of the intelligence function. The following is what the Fusion Center Guidelines are intended to make sure of: When each fusion center follows a uniform set of principles, information and intelligence sharing throughout states and authorities will become easy and effective. Fusion centers can only be successfully set up and run with the full backing of public safety authorities at all levels.The quality of information sharing between the participants in the fusion center, outside intelligence agencies, and the information sharing environment will improve if defined national criteria are followed.

Additionally, the standards will institutionalize a uniform method for gathering, retaining, analyzing, and disseminating information that reflects acknowledged and approved methods as determined by the agreement of intelligence subject matter experts who assisted in the standards' construction [1]. Beyond depending on national norms, it is necessary to take into account who the center's stakeholders are and what it will take to win their support for its activities. It is that easy. The success of the fusion center is directly correlated with the involvement of stakeholders in the center. In a similar vein, stakeholders won't engage with the center unless they find the

items, they get beneficial.From an operational standpoint, the North Central Texas Fusion Center's experience has led to the development of five guiding principles to enhance its performance:

The following elements are part of Phase 1 of the foundation phase:

Reeducation. Stakeholders need to be aware of the capabilities of the fusion center as well as the current function of law enforcement intelligence. Stakeholders must be aware of their part in ensuring that the intelligence function is successful in thwarting terrorist attacks, preventing the emergence of organized crime, and managing risks to homeland security that might endanger public safety. Employees at all organizational levels, from CEOs to line staff, should receive awareness training on how intelligence pertains to their position, as advised by the NCISP and the Minimum Criminal Intelligence Training Standards.

establishing a purpose, objectives, and goals. The fusion center should accomplish what? How will it function? Which offences will it deal with? What will be the result? What are its responsibilities to and relationships with customers? What are the fusion center's top priorities? The answers to these issues must be stated clearly in the purpose, goals, and objectives. It is a time-consuming procedure that calls for involvement from executives and stakeholders. However, until the training component is finished, it cannot be done properly since all staff members must be aware of the modern law enforcement intelligence function and make sure that their conception of the fusion center complies with modern requirements [2], [3].

something which the fusion power plant won't. A discussion of what the fusion center won't accomplish is just as significant as what it will achieve. The traditional intelligence operations of agencies that won't be continuing in the fusion center will probably alter; for instance, many of the state police intelligence units' activities tended to be more in line with investigative assistance than intelligence activities. These aspects need to be understood in order for the center to operate at its best. Similar to this, in order to prevent having unrealistic expectations, stakeholders and customers must be aware of what the fusion center will not accomplish.

Phase 2. The following proactive developmental actions need to be openly addressed at this phase:

establishing connections. The gathering of information and its distribution are two essential components of every intelligence operation.To make sure that everyone performs their duties with regard to intelligence operations, both must have certain components. The management support provided by cooperating organizations is necessary for the fusion center to function. It must also depend on staff to compile necessary data, record it, and send it to the fusion center. Similar to this, for the fusion center's information and products to be successful, they must be disseminated in a way that is efficient, readily accessible by customers, simple to use, and constantly contains important information. To do this, there must be overt efforts to forge connections between the fusion center's internal constituency of stakeholders and its exterior constituency through encouraging participation in the center's operations.

Outputs/products. Specific outputs and goods that will be generated on a regular basis must be identified by the fusion center. As the fusion center's development process progresses, among the questions that must be answered and stated are these ones: Reports that are both tactical and strategic will be produced? Are bulletins and advisories going to be published? Will there be

summaries produced? What is the outputs schedule? How will answers to certain questions be generated? How are standards for goods and outputs determined based on the right-to-know and need-to-know principles?

Phase 3. The third step entails putting all of the actions from Phases 1 and 2 into operational shape, from personnel and buildings to creating memoranda of understanding to actually implementing the fusion center's functions. This stage may take a significant amount of time and resources, especially if the intelligence function is being both changed and reengineered. Other tasks in this phase include combining agencies and their data, safeguarding each agency's data, standardizing data for integration into a single system, guaranteeing data quality control and security, and setting up auditing and accountability mechanisms.

DISCUSSION

Outputs of the Fusion Center

It is not the intention of the fusion center to react to on-going calls or enquiries concerning specific people or threats. This will undoubtedly happen from time to time, but if it occurs too often, the employees will get overburdened and unable to carry out their analytical duties. The intelligence provided by the center will guide operational reactions and a strategic knowledge of threats, making it the most crucial output of the intelligence fusion center [4]. When the analysis concludes that there is a danger against a certain kind of target, an operational reaction is triggered. Operationally, the law enforcement agency may then take the required steps to bolster the target or thwart the danger.Strategic awareness is a bigger body of knowledge that offers details on risks, techniques, and telltale signs of terrorists and criminals.

It is not always the case that fusion centers produce certain types of output. When designing output, it is important to take into account the different areas of the nation, the types of targets found there, and the distinctive characteristics of threats. For instance, there may be a lot of right-wing extremists present and active in a certain area; as a result, the fusion center would pay close attention to their actions.

Similar attention would be paid to drug smuggling along the Mexican border between the United States and Mexico as well as human trafficking. Consequently, strategic goals within those criminal categories would be reasonable, even if all fusion centers should have an all-crimes approach.

As a result, the fusion center should base its substantive outputs on the following three elements:

1. Dangers that have been specifically defined based on thorough and continuing threat assessments within the fusion center's authority.
2. Stakeholder-defined information and intelligence requirements.
3. Priorities at the national level, including those that get outside money, such the National Preparedness Goal 70 or FBI intelligence demands.

Beyond the substantive content, it is important to identify the output format and frequency, especially in light of the many kinds of analyses and products created and their frequency. In rare circumstances, the output format may be influenced by particular features of the fusion center's legal jurisdiction. For instance, email notifications may not be practical inareas with poor electronic communication amongst law enforcement organizations. Similarly, for rural or

dispersed law enforcement units, intelligence alerts and bulletins that are intended as briefings and distributed during roll calls would not be practical. The following output types, in any order, are possible:

Brief summaries of events and actions that may be related to risks locally or worldwide, especially if they show a pattern.Threat assessment: a thorough explanation of threats, targets, the chance that an attack would be launched against a specific target, and prospective assault tactics.Reports on the state of recognized dangers or any changes to their state are known as situational awareness.

Information bulletin: details on recent or upcoming risks, including methodology and threat indicators.Intelligence assessments are thorough analyses of threats, often of a strategic character. Information that is received from a source that is thought to be reputable but has not been verified or examined is known as raw intelligence. Usually, the information is being spread because the danger is urgent and might be catastrophic.

The fusion center will also create case intelligence, which is information pertaining to particular threats, targets, and suspects, in addition to these intelligence products. Instead of following a predetermined timetable, case intelligence is created and shared as soon as the circumstances call for it. The audience for dissemination is smaller and only includes those with a clear need for and right to know the information.

Numerous analytical methods, including link analysis, financial analysis, association matrices, visual investigative analysis, threat profiling, and pattern analysis, may be used to provide the various intelligence outputs. A fusion center would often also be engaged in additional procedures that assist criminal investigations into intelligence targets, such as case correlation, deconfliction, and intelligence support for criminal and terrorist investigations.

The technique of fusing intelligence has a lot of potential for producing successful intelligence operations. This is especially true given the cross-border nature of criminal and terrorist activities and the dangers that may necessitate the use of public safety measures. The four biggest obstacles are: 1. Establish a cooperative and devoted connection among all parties involved; 2. Ensure the confidentiality and safety of personal data; 3. Create procedures and regulations to enable effective, efficient, and legal intelligence activities; and 4. As an analytical center, be consistent.

Conceptually, it might be claimed that Sir Robert Peel's articulation of one of the cornerstones of police in the United Kingdom in 1829 is where the notion for public-private partnerships in law enforcement originated. Peel observed that the public, and therefore the private business sector, required support in order to help maintain communities free from crime since the government could not carry out all police responsibilities on its own. Peel really contended that since the people gave the police their power in a democratic society, they had a duty to work with them to ensure everyone's safety. In the 21st century, this can be interpreted to include two-way information sharing and joint public safety initiatives—responsibilities that both law enforcement and the private sector should embrace. His principle, "The police are the public and the public are the police," infers a reciprocal responsibility.

An observation made in a research by the Vera Institute of Justice that came to the following conclusion served to support this idea:

Nearly every component of crime prevention and investigation is supported by community assistance from the police. To accomplish the primary objective, it is crucial to mobilize the people.

In the past, there hasn't been much interaction between law enforcement and the business sector when it comes to efforts to reduce crime and promote community safety. Such efforts have often dealt with crime problems that were mostly exclusive to a particular neighborhood. The interaction between law enforcement and the business sector has even proven problematic in certain instances. Law enforcement and security guards or private investigators, for instance, have often disagreed professionally, with law enforcement frequently regarding these two groups despondently as "police wannabes." Alarm companies and law enforcement have also frequently had issues with reactions to false alarms.

In other instances, new interactions between law enforcement and the private sector have been thwarted by justifiable barriers like civil rights and privacy concerns raised by law enforcement or the potential to jeopardize investments and profits made by private businesses. Although not impossible, solving these problems calls both originality and ingenuity, both of which involve a lot of work. Too often, the effort has waned, with both parties content to just acknowledge that "we tried" rather than moving on to remove the obstacles. In some instances, it was thought that the prospective benefits did not justify the time and money required to carry out the effort. These viewpoints are starting to change in the wake of 9/11. Cooperating with the corporate sector to achieve practical objectives may be quite fruitful. The Vera Institute has noticed:

The private business sector is perhaps the most potential but least researched external source of support for police reform. Private sector businesses not only attract political attention, but they also provide a lot of resources, skill, and energy that may be helpful to reformers inside police agencies.

Local police have found that private groups may be a reliable source of information. They are significantly more likely than an officer to see or detect anything suspect. Other examples of private sources with useful information include private security personnel, reservation and shop clerks, and luggage handlers. Some organizations are attempting to forge these connections by organizing seminars to educate firms on the best forms of information. Both reducing participant fear and increasing the possibility that they will contact the police with information are goals of these workshops.

It is clear that there is a greater need than ever for successful public-private collaborations as law enforcement reengineers its intelligence programs for homeland security. In addition, the partnerships must be formed using a variety of different models based on the level of danger in a given area. Although there are still challenges, people are beginning to realize that the benefits of these connections are worthwhile investments of both time and money.

The present topic will be restricted to public-private partnerships for intelligence despite the fact that there are several programmatic methods connected to the private sector that are involved with prevention, disaster planning, incident management, and response.

Context and Viewpoint

Recent research on public-private partnerships has been greatly influenced by projects aimed at the expansion of the European Union. A quick review of this past history offers some context.

Western European nations created an agreement that was first called as the European Economic Commonwealth as a way to strengthen their economies globally. It later became the European Community and, as it is known today, the European Union.5 Adopting public-private partnerships was one of the cornerstones of creating a sustainable and economically robust union of varied, multilingual governments. The conceptual framework created by the European Union may be used extensively in the United States.

An agreement of collaboration between independent private and public parties working together to accomplish common goals on the basis of a defined division of duties, tasks, and authority, and with no hierarchy among the parties, is known as a public-private partnership. Mutual trust and appreciation of the potential for the future are the two most crucial prerequisites for a public-private partnership's success.Regarding the last point, P3I in the US would take into account civil rights and privacy problems, preserve company property information, follow national requirements for the security of sensitive information, and be a member of the Information Sharing Environment.

U.S. The necessity to proactively include the private sector as a functional partner in the information/intelligence-sharing process has repeatedly been acknowledged by a broad variety of inquiries, according to the National Standards and Recommendations for Public-Private Partnerships in the U.S. According to the 9/11 Commission's Final Report,The Department of Homeland Security also has a duty to collaborate with the business community to promote readiness as part of its overall mission. This is absolutely acceptable given that the private sector is in charge of 85% of the country's key infrastructure. Indeed, the "first" responders will very definitely be civilians unless a terrorist is targeting a military installation or some protected government building. Therefore, the private sector typically serves as the foundation for both homeland security and national readiness.

No information exchange with the private sector is more essential than when creating intelligence to stop terrorist acts from occurring on American soil. The 9/11 Commission makes the following further observations on the exchange of public and private information:The required technology is already available. The guidelines for gathering, utilizing, sharing, and accessing the sizable repositories of public and private data do not. When it works, information exchange is a potent instrument.The federal Accountability Office noted the following while reviewing the accomplishments of federal information sharing:

Assuring timely and secure sharing of vital information gathered and analyzed by the Departments of Homeland Security and Justice with various parties within the federal, state, and local governments as well as the private sector is one of the challenges in protecting our homeland.The federal, state, and local governments must aggressively work and engage with the business sector to address these concerns, according to the National Strategy for Homeland Security. The National Strategy for Information Sharing said in a similar vein that "private sector information constitutes a significant part in both comprehending the current threat landscape and defending our nation's critical infrastructure from targeted assaults. Law enforcement should include the business sector in its intelligence function, according to the Global Intelligence Working Group.For instance, the following is stated in recommendation number seven of the National Criminal Intelligence Sharing Plan: To identify and stop assaults on the country's vital infrastructures, local, state, tribal, and federal law enforcement organizations must collaborate

with both the public and private sectors. Establishing frequent communications and information-sharing channels should be done.

Because they provide fusion centers with data on crime, such as risk and threat assessments, and subject matter, the public safety and private sector components are essential to the fusion process.The many findings given up to this point clearly show how important public-private information exchange is for homeland security. It is suggested in almost every investigation and evaluation of the usefulness of intelligence, but in the years after the 9/11 attacks, achievements have not achieved the level that was anticipated. Barriers to information sharing between law enforcement and private security are undeniably present, according to a 2005 Bureau of Justice Assistance study solely dedicated to public-private cooperation in homeland security. The study continues, "Information sharing should be a key element of any law enforcement-private security partnership because information is the lifeblood of any law enforcement agency."

The analysis and synthesis unit of a jurisdiction should also develop procedures for information exchange with the neighborhood private sector. Private companies and government safety organizations may exchange useful threat and vulnerability data. However, due to worries about the leak of sensitive or confidential information, governmental and private organizations often impose limits on information exchange with one another. Local firms and industries need to be included in any local information sharing network, according to yet another DHS Lessons Learned/Best Practices paper.19 One of the restrictions is that "Public safety and private security officials should cooperatively establish guidelines that strike a balance between the need to alert the private sector to potential threats and the need to ensure that proprietary information is not improperly disseminated," according to one of the restrictions.20 Another study addressed this issue and said that there is currently no formal procedure in place for state, municipal, tribal, and private sector organizations to provide particular intelligence requests to federal agencies.

The federal government's capacity to comprehend the threats facing the country and deliver timely, actionable, preferably UNCLASSIFIED, and frequently updated homeland security information and intelligence to those on the front lines of the domestic is hindered by a failure to comprehend these entities' needs. These proposals and evaluations make it abundantly evident that the private sector must be included in partnerships for information-sharing. Even with all of these suggestions, integration has been rather slow. Furthermore, the business sector is often the economic backbone of many communities. Beyond those that make up the essential infrastructure, other businesses and sectors have been noted as potential targets of terrorist strikes. Simply put, the suggested and anticipated evolution of information sharing between public and private bodies has not occurred. It is the responsibility of law enforcement authorities to create a procedure and training to address that issue.

The Intelligence Process and P3I

In terms of homeland security in particular, the present model of intelligence handles "all crimes, all hazards, and all threats." In this light, homeland security and law enforcement are two areas of intelligence that state, municipal, and tribal law enforcement organizations are interested in. As a quick recap, law enforcement intelligence outlines dangers to a community that are connected to crime and is the analytical output of raw information. This conventional approach to intelligence concentrates on illegal activities including those connected to terrorism or organized crime. Homeland security intelligence, which is less common, is the analytical output of raw data that describes non-criminal threats to vital public infrastructure, public health, or

community safety for which a law enforcement agency will be responsible for maintaining public order, public safety, and/or order. For instance, if a pandemic flu outbreak occurs in a town, law enforcement authorities would probably need to help with victims, support quarantines, and help with distributing and safeguarding medical supplies. As another example, homeland security intelligence may find that new industry would cause bigger barges to transit a key canal close to a neighborhood, increasing the risk of a barge colliding with a significant bridge. As a consequence, rescue and recovery preparations, traffic management plans, and accident site security would all need to be considered during law enforcement strategic planning. The DHS Target Capability List links both forms of intelligence into the following targeted capability outcome:To achieve coordinated awareness of, prevention of, protection against, and response to a threatened or actual domestic terrorist attack, major disaster, or other emergency, information and intelligence are effectively and promptly shared across Federal, State, local, tribal, territorial, regional, and private sector entities.

Health practitioners who have certain forms of personally identifiable information may face some P3I problems. Plans and procedures for legally handling the exchange of this kind of information and avoiding obstacles in the event that a public health emergency arises are far simpler to address beforehand than they are after a crisis has occurred. In the event of a public health emergency, it would be crucial for medical personnel to let law enforcement know who is at danger or poses a risk. Conflict resolution and service delivery will be accelerated if procedures are put in place with training for both law enforcement and public health experts. The goal of this debate has been to contextualize certain fundamental definitions and ideas in order to give the P3I some context. The connection of public-private partnerships to the ISE from the perspective of state, municipal, and tribal law enforcement authorities is a transitional problem [5]–[7].

CONCLUSION

A clear understanding of the center's purpose and goals must serve as the foundation for a collaborative and strategic approach to the creation of fusion centers. Organizations can create effective and efficient fusion centers that support the identification, prevention, and response to criminal activity and other threats to public safety by establishing a solid governance structure, utilizing cutting-edge analytical tools and technologies, and encouraging a culture of collaboration and information sharing. Utilizing cutting-edge analytical tools and technology to facilitate information processing and analysis is another crucial aspect of creating a fusion center. Data analytics, machine learning, and other cutting-edge methodologies could be used in this to support analysts in extracting patterns, trends, and other insights from massive amounts of data. These technologies may speed up and enhance analysis while also allowing information exchange across various partners and stakeholders.

REFERENCES

[1] M. H. Saeed, W. Fangzong, B. A. Kalwar, and S. Iqbal, “A Review on Microgrids’ Challenges Perspectives,” *IEEE Access*. 2021. doi: 10.1109/ACCESS.2021.3135083.

[2] C. Lewandowski, J. G. Carter, and W. L. Campbell, “The utility of fusion centres to enhance intelligence-led policing: An exploration of end-users,” *Polic.*, 2018, doi: 10.1093/police/pax005.

[3] H. F. V. Cardoso, V. Pereira, and L. Rios, “Chronology of fusion of the primary and secondary ossification centers in the human sacrum and age estimation in child and adolescent skeletons,” *Am. J. Phys. Anthropol.*, 2014, doi: 10.1002/ajpa.22422.

[4] D. Carter, S. Chermak, E. McGarrell, J. Carter, and J. Drew, “Understanding the Intelligence Practices of State, Local, and Tribal Law Enforcement Agencies,” *Police Chief*, 2012.

[5] D. N. Segal *et al.*, “Fusions ending above the sagittal stable vertebrae in adolescent idiopathic scoliosis: does it matter?,” *Spine Deform.*, 2020, doi: 10.1007/s43390-020-00118-0.

[6] J. Luo, Y. Dong, L. Li, and X. Wang, “Microstructure of 2205 duplex stainless steel joint in submerged arc welding by post weld heat treatment,” *J. Manuf. Process.*, 2014, doi: 10.1016/j.jmapro.2013.06.013.

[7] S. Blais, L. Meloche-Dumas, A. Fournier, F. Dallaire, and N. Dahdah, “Long-Term Risk Factors for Dilatation of the Proximal Aorta in a Large Cohort of Children with Bicuspid Aortic Valve,” *Circ. Cardiovasc. Imaging*, 2020, doi: 10.1161/CIRCIMAGING.119.009675.

CHAPTER 17

INFORMATION-SHARING ENVIRONMENT AND THE PRIVATE SECTOR

Pradip Kumar Kashyap, Assistant Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id- pradiprgnul@gmail.com

ABSTRACT:

Information sharing is a critical component of effective law enforcement and public safety efforts. One key area where information sharing can be particularly important is in the relationship between the public sector and private sector organizations. Private sector entities can often provide valuable information and resources to support law enforcement and public safety efforts, but this requires a robust and secure information-sharing environment that allows for the exchange of information and intelligence between public and private sector partners. Developing an effective information-sharing environment between the public sector and private sector requires a number of key factors. These include the establishment of clear policies and guidelines for information sharing, the deployment of advanced technologies to support secure data exchange, and the development of strong relationships and partnerships between public and private sector organizations.

KEYWORDS:

Interagency Cooperation, Law Enforcement Intelligence, National Security, Private Sector, Public-Private Partnership, Risk Management.

INTRODUCTION

The development of the ISE poses a new challenge to both law enforcement and the business sector. The ISE is a defined set of policies and procedures to improve information sharing across five crucial sectors: The Intelligence Community, Federal Law Enforcement, State, Local, and Tribal Law Enforcement, the Private Sector, and Foreign Partners make up the first five categories. The landmark Intelligence Reform and Terrorism Prevention Act of 2004 was passed by Congress and signed by the President in recognition of the need to go beyond individual solutions to create an environment the combination of legal, policy, cultural, organizational, and technological conditions for improving information sharing. In accordance with the Act, the President must create an environment "for the sharing of terrorism information in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties."The ISE's program manager oversaw the creation of an implementation plan based on this statutory mandate in order to provide the means by which the ISE would carry out its statutory duty. Creating a vision, which has effectively become the ISE's ultimate objective, was a crucial beginning point:

In order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, the people, and the interests of the United States of America, we envision a future ISE that represents a trusted partnership among all levels of government in the United States, the private sector, and our foreign partners.The development of an information sharing culture across the intelligence community, law enforcement organizations, and the corporate sector was essential to achieving this aim. This ambitious plan calls for increasing technological connectivity between the entities, developing a common lexicon to improve information quality while maintaining security, and increasing the willingness of all entities to be actively involved in two-way information sharing. The ISE Implementation Plan acknowledged this difficulty and recommended that the commercial sector participate in a coordinated source for information on terrorism, alerts, warnings, and situational awareness. The Implementation Plan continued by noting that private-sector information is essential to comprehending the current threat landscape and averting assaults on the country's key infrastructure [1], [2].

The robust public-private partnership that informs the private sector of incidents, threats, and vulnerabilities and protects private-sector information in a way that the private sector is willing to share it with government partners is also necessary for protecting the interconnected and interdependent U.S. infrastructure.Although going beyond the requirements of the intelligence process, the Sector Coordinating Councils and sector-specific Information Sharing and Analysis Centers established by the National Infrastructure Protection Plan and the National Infrastructure Coordination Center are currently the main channels for sharing terrorism information. Sharing via various channels has, however, so far had conflicting effects. The uncertainty present in the public-private connection is one of the causes. The private sector participants note that after 9/11, the demand from the federal, state, and local governments for vital infrastructure and other information has grown many times over, increasing the burden on business to gather and disclose the information. Due to the infrequent coordination or consistency of requests for private sector information, which leads to redundant requests, these aspects are made even more difficult.28 A reliable collecting strategy must be devised if P3I is to be effective. Six goals from the NIPP29 were outlined and may act as benchmarks for the collection plan:

1. Information sharing to control commercial enterprise risks while safeguarding Americans' other legal rights and their right to privacy.
2. Establishing a national structure and culture for information sharing that sufficiently safeguards corporate risks and proprietary interests while rationalizing demands for terrorist information from the private sector.
3. Establishing a seamless, secure environment where data may be exchanged, kept up to date, and safeguarded.
4. Providing industry with signs of oncoming risks or ongoing assaults by providing access to the integration and analysis of data from many sources.
5. Receiving actionable alerts and warnings concerning specific industries that improve their situational awareness of terrorist threats and enable them to prioritize risks and security investments, and shape the development of plans to ensure the security, continuity, and resiliency of infrastructure operations.
6. Adopting guidelines and procedures that provide the private sector liability and antitrust defenses in conjunction with exchanging information in good faith.

The United States Public Private Partnership is one program that aims to support these projects. USP3 was created with the goal of acting as a coordinating hub for both commercial and public

outreach initiatives, resulting in a cross-sector membership throughout the country. Information exchange within the partnership is done by USP3 members. The project has had just a small amount of involvement, despite the fact that the idea is strong and it has received positive backing, particularly from the DHS. However, local law enforcement should keep an eye on and promote USP3 as a base for building strong alliances with the business sector.

The difficulty is in comprehending the full scope of P3I, identifying the pressing problems that must be tackled, and attaining these goals while safeguarding the vital interests of both private businesses and law enforcement agencies. Although there are often conflicts between these interests, some rules may be depended upon to help both sorts of organizations navigate this mostly unexplored region.

Fundamental Rules for Public-Private Intelligence Partnerships

Through a two-way exchange of unfiltered information and intelligence, the P3I aims to eliminate or lessen dangers to a community from crime and homeland security.The National Governors Association said in its Homeland Security Policy Statement that private sector partners play a critical role in supplying specialists, technology, and infrastructural resources to develop and sustain our nation's security. When dealing with a terrorist attack, the involvement of the business community and the effect on the town's economic sustainability must be taken into account. Using the methodology, the DHS uses to identify vital infrastructure and important resources might help us comprehend private-sector targets inside a community. Certain national infrastructures are so essential to the country's military or economic security that their failure or destruction would be disastrous.

a. Telecommunications
b. Power supply systems
c. Transportation and storage of gas and oil
d. Finance and banking
e. Transportation
f. water delivery methods
g. emergency assistance
h. Constitutional continuity

Every neighborhood in the United States is impacted by these key infrastructure components, making them a top national priority.

DISCUSSION

A "key resource" might differ throughout communities and refers to publicly or privately managed resources that are necessary for the economy's and a government's basic functions. For instance, Hallmark Cards, which employs more than 4,000 individuals at its headquarters in Kansas City, Missouri, although not being a crucial component of the U.S. infrastructure, is a significant contributor to the local economy. A crucial source might could include the whole of a community's sector rather than just one particular enterprise. For instance, the beef cattle industry in Dodge City, Kansas, consists of many beef processing enterprises, a cattle auction house, and cattle feed lots operated by a variety of people and corporations. Together, these companies serve as southern Kansas' economic engine and vital resources [3]–[5].

Although the private sector may play a variety of roles in homeland security, as previously said, the present topic is mainly focused on the intelligence role for prevention. As a result, given the plausible threats in the area, both private critical infrastructures and knowledge resources should be classified according to their risk of becoming targets. The non-law enforcement public sector could also be seen in the same light as the private sector as it performs many tasks and processes information more like the private sector than law enforcement. These organizations will also have access to specialized types of data. For instance, the public health, agriculture and veterinary medicine, mass transit, and aviation departments have access to a wealth of data that could be useful to both law enforcement and homeland security intelligence.

Intelligence depends on unprocessed data. From this vantage point, it's crucial to take into account the fact that the private sector has access to raw data that law enforcement does not, which may be crucial for meeting intelligence needs connected to dangers inside a community or a region. A business security group may have created its own sources or this data may originate from outside sources. Here are a few instances:

a. The corporate security section of an automaker discovers that the same thieves are transporting explosive components to a person in the United States after looking into trans-shipment thefts from an international parts supplier.
b. A global banking company's corporate security hears of dubious money transfers from your city to a bank in Iran that is thought to be housing the accounts of people thought to be terrorists.
c. A huge retail company’s corporate security finds narcotic being trafficked into your neighborhood from Thailand camouflaged in legal shipments of goods.
d. Law enforcement may also seek information from the private sector in order to alert them to potential signs of terrorism or criminal activity. Examples:
e. Freight or package delivery businesses get training on criminal indications from law enforcement intelligence, and their delivery personnel are asked to report suspicious activity based on such signs.
f. Retailers are asked by law enforcement intelligence to alert them if particular goods that are known to be used in funding terrorism or to be a part of other criminal enterprises are being sold in or stolen from their establishments.
g. A representative of a major corporation that sells chemicals is asked by law enforcement intelligence to report any odd purchases of certain goods that may be used in a terrorist attack.

"Business executives often wonder what they can do to help with successful police reform besides providing more money. Skills are one solution. "36 The private sector possesses expertise that isn't easily accessible in law enforcement. This may include access to cutting-edge technology, global audio and video communications, the ability to evaluate dangerous compounds, and a variety of tools including chemical detectors and satellites.

Partnership Types

Depending on available resources, potential risks, and information demands, partnerships may be formed in a variety of ways. They will depend on things like the sorts of risks that exist inside a community, the vulnerability of a region's essential infrastructure and resources, and the readiness of public and private organizational leaders to develop an information-sharing relationship.

Full Collaborations through Personnel Assignment

When a member of the private sector is employed full-time by an intelligence unit or fusion center, this is referred to as a full partnership. The person often represents a whole industry of business, not simply the employer organization. For instance, the Boeing Corporation employs a full-time intelligence analyst assigned to the Washington Joint Analysis Center. Not only the Boeing Corporation, but the whole aircraft manufacturing sector is represented by the Boeing employee. The following criteria must be met in order for a private sector representative to be allocated to WAJAC:

Private Entities: WAJAC will take into account assigning employees from privately held businesses with an interest in homeland security if they have the WAJAC Advisory Board's support.Allegations of favoritism against any one enterprise are avoided when a private-sector employee, with the consent of the WAJAC Advisory Board, represents an entire sector. Additionally, having a single sector representative as opposed to several members from a single sector is just more efficient and productive. Assuring that the sector representative and other participants in the sector have an agreement to disclose necessary information is a difficulty, of course.

A complete partnership assignment should at the very least contain: background check on the employee being hired; a letter of understanding outlining the roles, responsibilities, and procedures of both public and private parties with relation to the employee's assignment; and 3. an acknowledged nondisclosure agreement.In order to establish which industries are most important to have represented in the fusion center or unit, the law enforcement intelligence agency has to evaluate the sectors in its area. Of course, the most probable candidates are those who have significant installations in the area.

Partnership for Full-Time Information Sharing

As the agency works with law enforcement partners, there is constant two-way information exchange between law enforcement and business sector partners under a full-time framework. This is different from a complete partnership in that a person is not transferred to an intelligence or fusion unit; instead, they stay at their existing workplace. This is especially useful when there are ongoing intelligence needs for the commercial sector. When a program for intelligence liaison officers has been formed, it is the model that is employed the most often.

By assigning a specific person to serve as the point of contact for all two-way information exchange, the ILO idea creates a formal connection with the private-sector organization. The ILO is frequently given access to a secure e-mail system, such as the Automated Trusted Information Exchange, after being vetted for security purposes, training on intelligence, counterterrorism, and homeland security intelligence issues, and defined areas of responsibility for information-sharing. In order to enhance efficacy and preserve the close connection that is necessary for maintaining the ILO program, ILOs should also periodically meet with the intelligence group to address problems and procedures. All participating organizations should sign a MOA, and the ILO should sign a nondisclosure agreement, just as with the complete collaboration.

Information security becomes a bigger concern for both parties since the ILO will physically be at his or her place of job. In the MOA, information security procedures should be

described.When the private sector lacks the manpower to send a person to the law enforcement agency but still needs to provide information that is vital for community safety, the ILO program is a useful choice.The ILO performs a variety of significant functions, including but not limited to the following: Gather, document, retrieve, and distribute training resources pertaining to the sector's risks.act as a source for queries from the fusion center or intelligence unit both internally and outside. Gather information and insight on possible dangers to the industry and share it with others. Find sector stakeholders, get in touch with them, and act as their liaison. Become the point of contact for sector members who have queries or information to offer about a danger.

Conduct, plan, and/or conduct training on dangers to the industry. Law enforcement and/or the industry should both benefit from the training. act as the appointed sector representative for any gatherings, groups, task forces, or other organizations discussing sector risks.Keep track of and communicate with the fusion center or intelligence unit on the presence and/or alterations of vital resources and infrastructure for the sector. Conduct regular evaluations of the sector's threats and vulnerabilities. Keep abreast of any risks from terrorists and criminals to the industry by keeping an eye on all sources, especially open sources. familiar with all national laws and legal requirements pertaining to the intelligence role. serve as a subject matter expert for the sector with regard to all technical and industry-specific terminology, tools, and procedures.

Ad-hoc Collaborations

The ad hoc collaboration is used when required. This is a particularly attractive option when no ongoing private sector intelligence needs are required from a specific industry. There is a framework in place for quick information exchange when threats to the industry or organization materialize. In exceptional circumstances, a representative of the private sector may be sent temporarily to the law enforcement organization. The same screening procedures that were used to the ILO, the memorandum of understanding, and the nondisclosure agreement should be applied here.

Law Enforcement-Private Partnership Roadblocks

Due to the intrinsic nature of P3I, open two-way sharing of threat-based intelligence is required between law enforcement organizations and the private sector for both homeland security and law enforcement objectives. Processes must thus guarantee that communication is open and that both the private sector and law enforcement have access to the information they need.Regrettably, this is not simple. The Bureau of Justice Assistance examined the interaction between law enforcement and the business sector and found three major challenges that must be solved to create successful alliances.

Barriers to information sharing is the first obstacle. If efficient information sharing is to occur, a number of obstacles must be removed by law enforcement and the business sector.The following are some of the obstacles a law enforcement organization faces while working with the business sector:Concerns about privacy and civil rights have led to uncertainty around the kinds of information that may be shared with the business sector. Uncertainty over the best way to distribute information that should only be disclosed to law enforcement. under this sense, it is unclear whether the appointment of a private-sector representative under a formal arrangement authorized by an MOU qualifies that individual as an agent of the law enforcement agency. In many instances, state law will have a significant impact on this.

A refusal to provide confidential information, especially when it relates to a possible danger, is an example of a private sector obstacle to law enforcement. Foreign-owned businesses are reluctant to provide the American government with any information. The private sector generally does not want to take the chance of information being public that might hurt earnings. Even while these obstacles to information sharing cannot be removed, they do call for unconventional and inventive solutions to accommodate legal restraints, information security concerns, and laudable business goals.Second obstacle: a lack of trust. The Justice Department's 40 surveys continually reveal a poor degree of trust between private security and law enforcement. The two sectors often see one another as having distinct objectives

as well as several constituencies. The community that a law enforcement agency serves makes up its constituency, but the private sector's constituency comprises not just a larger community but also its investors who have an impact well beyond the local community. Moreover, both law enforcement agencies often have an implicit belief and the corporate sector that, even if one works together, the other may not return the favor. The fact that private security is sometimes seen as inferior to sworn law enforcement adds to the mistrust. Private security professionals come in a wide variety, from security officers to highly trained detectives and analysts.

According to BJA, law enforcement leaders and their teams need to take the following actions to foster trust:

1. Make a vision and passion that unites employees.
2. Make good on your commitment.
3. Ensure uniformity. Credibility is destroyed by abrupt changes or changes that are poorly understood.
4. Communicate.
5. Identify any lingering doubts or worries and resolve them.
6. Observe each detail.
7. Together, law enforcement and business sector partners should get training.
8. Maintain fairness and equality. Both parties need to provide their fair amount of effort and get credit for it.
9. Reiterate how crucial the cooperation is.
10. Acknowledge your errors and grow from them. Errors will be made by both sides.

Misinformation and misunderstanding are the third obstacle. Misinformation and misunderstandings are two of the main reasons for lack of trust. Sometimes, neither

Neither law enforcement nor the private sector fully comprehends what the other does or is capable of. These have often been seen as overwhelming by both sides when taken as a whole. Successful partnerships show that obstacles can be overcome, but doing so needs leadership, dedication, and hard effort.

Communication: Both parties should make explicit and unambiguous statements of their goals, intentions, kinds of information to be communicated, and concerns.

Collaboration: The other must be actively sought out. Wins and losses will occur for each side. To build a trustworthy connection, it is essential to find innovative methods to communicate information.

Coordination: To prevent redundancy and ensure that all operations flow naturally in a seamless public-private information sharing environment, make sure that the actions and responsibilities of each party are clearly defined.

Collaboration: Make plans together in addition to working together. Each party should depend on the other's skills and advantages.

Two Critical Issues to Resolve: Sharing Criminal Information and Private Proprietary Information

Concerns and limitations around civil rights, state legislation, criminal intelligence records rules and policy, and operational security apply to the sharing of criminal information with a private partner. The majority of problems can be fixed, but doing so demands for well drafted policies, MOU clauses, and training. When people or groups are identified, exchanging information becomes a crucial problem for law enforcement since this is when constitutional rights attach.

How to communicate criminal intelligence information when persons and organizations cannot be recognized is perhaps the simplest problem. This could include details on danger scenarios, threat warning signs, and cautions relating to vague threats. The information-sharing limitations in these situations mostly concentrate on the need-to-know and right-to-know criteria. The private-sector representative should be given the right to know by having the MOA between the two parties drafted in a way that designates him or her as an agent of the law enforcement organization. Just as it should be for law enforcement professionals, the need to know is evaluated on a case-by-case basis [6]–[8].

The trickier element of sharing data that may be used to identify people or organizations with private sector partners is doing it legally. Constitutional protections and more stricter constraints are attached to the information and information-sharing procedure after a person or organization has been recognized. Two crucial issues are at stake if this information is to be shared with private-sector employees. The first is how state law handles privacy concerns, namely whether a private-sector partner is regarded as an agent of the law enforcement agency. The right-to-know and need-to-know criteria, which operate in the same way as previously explained, are the second problem. The proper drafting of the MOA, training for all parties, and a safe information-sharing procedure are crucial to success.

There are corporate constraints on exchanging confidential information that belongs to private organizations, just as there are legal and practical limitations on sharing criminal information.

Several Crucial Questions

1. Do you know which private sector organizations in your area need to get involved?
2. Do you now work with any of these businesses in the private sector?
3. Have these groups' representatives undergone any screening?
4. Do any of these organizations and you have a MOA?
5. Have the organizations you work with signed a nondisclosure agreement?

Information that is protected by a patent, copyright, trademark, or other intellectual property right and that pertains to a private organization's internal business operations and that defines a product, service, method, design, or mixture was considered proprietary information. It includes, but is not restricted to, financial data, data or statements, trade secrets, product research and

development, current and future product designs and performance specifications, marketing strategies, plans or tactics, client lists, schematics, computer programs, processes, and know-how that has been explicitly designated and appropriately marked by the company as proprietary information, trade secrets, or company confidential information. For information to be considered proprietary, it must have been created by a private organization and be withheld from the public or the government by another source. Examples of private information include computer programs, business plans, marketing lists, business plans, soft drink recipes, and computer hardware. Proprietary information may have a very wide variety of characteristics. In essence, every firm and product in the world might theoretically have some kind of private knowledge that is normally kept to oneself out of fear of helping rivals or jeopardizing one's own success in the market.

Proprietary information, such as the layout of a production or shipping facility, the locations of backup storage facilities, the chemical components of a chemical product, or the method to disable a particular device, may occasionally be necessary for the prevention or mitigation of a criminal incident or emergency. It is anticipated that the private company would cooperate with law enforcement in such a case by disclosing confidential information. The law enforcement organization must comprehend the importance of the request in order to do this. The success of the business could be harmed by the information's exposure. The law enforcement agency understands the need of obtaining this information, but it also has to be aware of the danger it presents to the private-sector partner. A protocol for disclosing confidential information and a joint-signed declaration of release and nondisclosure are best practices [9], [10].

CONCLUSION

Finally, creating a conducive climate for information exchange requires forging strong ties and collaborations between organizations from the public and commercial sectors. In addition to a dedication to common aims and objectives, this calls for continual partner engagement and communication. The adoption of cutting-edge technology to assist safe data transmission is another important aspect of creating a productive environment for information sharing. To safeguard sensitive information and make sure that it is shared only with authorized parties, this may include the use of encryption, secure data networks, and other cutting-edge technology. In general, creating a productive environment for information exchange between the public and private sectors is essential for enhancing public safety initiatives and law enforcement work. Organizations may develop a robust and secure information-sharing environment that facilitates the interchange of information and intelligence between partners in the public and private sectors by creating clear rules and procedures, using cutting-edge technology, and cultivating strong relationships.

REFERENCES

[1] S. Logesswari, S. Jayanthi, D. KalaiSelvi, S. Muthusundari, and V. Aswin, “A study on cloud computing challenges and its mitigations,” *Mater. Today Proc.*, 2021, doi: 10.1016/j.matpr.2020.10.655.

[2] A. Ziaee Bigdeli, M. Kamal, and S. de Cesare, “Information sharing through inter□organisational systems in local government,” *Transforming Government: People, Process and Policy*. 2013. doi: 10.1108/17506161311325341.

[3] M. Ashok, M. S. M. Al Badi Al Dhaheri, R. Madan, and M. D. Dzandu, "How to counter organisational inertia to enable knowledge management practices adoption in public sector organisations," *J. Knowl. Manag.*, 2021, doi: 10.1108/JKM-09-2020-0700.

[4] S. H. Kim and I. Y. Lee, "IoT device security based on proxy re-encryption," *J. Ambient Intell. Humaniz. Comput.*, 2018, doi: 10.1007/s12652-017-0602-5.

[5] A. Cooley, "Comparative analysis of online accountability practices in three sectors: private, public and nonprofit," *Accounting, Audit. Account. J.*, 2020, doi: 10.1108/AAAJ-03-2019-3919.

[6] J. Ramon Gil-Garcia, I. S. Chengalur-Smith, and P. Duchessi, "Collaborative e-Government: Impediments and benefits of information-sharing projects in the public sector," *Eur. J. Inf. Syst.*, 2007, doi: 10.1057/palgrave.ejis.3000673.

[7] S. Park, J. Ramon Gil-Garcia, T. A. Pardo, M. Sutherland, and A. Roepe, "Cross-boundary information sharing in regulatory contexts: The case of financial markets," *Public Money Manag.*, 2019, doi: 10.1080/09540962.2019.1611237.

[8] Y. M. Akatkin, O. E. Karpov, V. A. Konyavskiy, and E. D. Yasinovskaya, "Digital economy: Conceptual architecture of a digital economic sector ecosystem," *Bus. Informatics*, 2017, doi: 10.17323/1998-0663.2017.4.17.28.

[9] K. Luo, J. Ryu, K. B. Jeong, H. S. Kim, and Y. R. Kim, "Colorimetric assay for the determination of molecular weight distribution and branching characteristics of starch hydrolysates," *Carbohydr. Polym.*, 2021, doi: 10.1016/j.carbpol.2020.117046.

[10] B. Batidzirai *et al.*, "Towards people-private-public partnerships: An integrated community engagement model for capturing energy access needs," *Energy Res. Soc. Sci.*, 2021, doi: 10.1016/j.erss.2021.101975.

CHAPTER 18

DEVELOPING A SUCCESSFUL PUBLIC-PRIVATE PARTNERSHIP FOR INTELLIGENCE

Mr. Aaditya Arora, Assistant Professor
Seedling School of Law & Governance, Jaipur National University, Jaipur, India
Email id-aaditya.arora@jnujaipur.ac.in

ABSTRACT:

Developing a successful public-private partnership for intelligence requires a collaborative and strategic approach that involves multiple stakeholders and is guided by a clear understanding of each party's roles and responsibilities. These partnerships are critical for addressing complex threats and risks that require the pooling of resources and expertise from both the public and private sectors. To develop a successful public-private partnership for intelligence, it is important to establish a clear governance structure that outlines the roles and responsibilities of each partner. This includes defining the scope of the partnership, identifying key decision-makers, and establishing mechanisms for information sharing and collaboration.

KEYWORDS:

Interagency Cooperation, Law Enforcement Intelligence, National Security, Private Sector, Public-Private Partnership, Risk Management.

INTRODUCTION

P3I success requires teamwork and a well-thought-out strategy. The Bureau of Justice Assistance identified 12 crucial elements to develop in its research of public-private ties. A public-private partnership may be established using these elements as a guide. The law enforcement organization must first specify its goals and duties for each of the aforementioned variables. Those in charge of creating and maintaining the relationship assess and improve the response to each element. The chief executive reviews, amends, and approves the final implementation plan, including the people and resource commitments. The following issues need to be addressed in this process:

1. Negotiate and create shared objectives.
2. Determine and create standard responsibilities for both law enforcement and business workers.
3. Learn about the objectives and capabilities of the collaborating companies and agencies.
4. Describe your clearly stated predicted results.
5. Decide on a suitable implementation timeframe.
6. Give everyone involved training on the ideas, goal, and duties.
7. Clearly state the partnership's attainable goals.
8. Determine who is in charge of what duties and what objectives.

9. Make an operational manual outlining how the partnership will run after it has been put into place.
10. Ensure that all partners have agreed on the partnership's future course of action, including its resources and obligations.
11. Declare a shared commitment to provide the required resources.
12. Create a system for evaluation and reporting.
13. Public-Private Partnership with the Denver Police Department

Denver Public-Private Partnership is known as DP3. The Denver Police Department's (DPD) initiative to collaborate with private security experts in the City and County of Denver is represented by DP3.A broadcast alert communication network, which is the core of DP3, provides users with up-to-the-minute information on security concerns, crime trends and incidents in progress, impending large events, BOLO alerts, and similar topics.The DP3 website will also include connections to partner organizations' websites as well as information on crime prevention. These websites provide a wealth of useful tools for preparing large emergencies, home preparation, and security.

DISCUSSION

Benefits of Membership

Public links and information will be posted on the DP3 site, but members will have access to more content. After a brief background and records check, DP3 members will start receiving emails or text messages with notifications. Members will also have access to the document library and the DP3 archives of previous warnings [1]–[3].

Who Should Attend?

Only security directors and supervisors with an established proprietary or contractual security force inside the City and County of Denver are eligible to join DP3. They may also specify that employees are eligible for membership. The DP3 site, however, is accessible. All that is needed to show interest in membership is a quick email to DP3@ ci.denver.co.us, and you will be contacted with instructions and an application. A quick computer records and background check will be conducted on applicants as part of the application and approval procedure.

Following this procedure gives the partnership a strong basis and a distinct goal, as well as a sign of the chief executive's support and dedication. All of this adds up to a clear development strategy that might be presented to prospective partners in the business sector. The private sector must examine, clarify, and accept its obligations related to the aforementioned considerations if the collaboration is to proceed. There may have to discussion process on specific aspects of the strategy that the law enforcement organization must fairly take into account. Finalizing the partnership requires that each party accept its obligations and duties. Following that, when necessary, the development and implementation plan should transition into a shared operating plan with a signed MOA.

If either the law enforcement agency or the private organization tries to adopt crucial elements without participation from the other side, it is a certain prescription for disaster. Don't forget that the private partner will often need to sell the partnership to a bigger corporate structure. As a result, garnering corporate commitments may depend in part on the private entity's ability to demonstrate meaningful engagement into the partnership building process.

Matthew Simeone of the Nassau County, New York Police Department suggested three crucial elements CEOs should take into account when creating a public-private collaboration to assist the intelligence function:Prior to choosing a plan, make sure the appropriate individuals were in the appropriate roles inside the firm.

Tipping Point Leadership: Within any organization, there are individuals, behaviors, and actions that have a disproportionately large impact on output. Therefore, concentrating efforts on locating and then using these characteristics might result in significant change.

Creating a Need for Change: A project involving the sharing of information with the private sector is likely to spark discussion about the kind of information that will be shared inside the agency. For the collaboration to be successful, it is crucial to create an internal campaign that addresses the expected worries of officers and the benefits they would gain from the alliance.

Making a Resource Commitment: As was said in earlier issues, failing to make a resource commitment to a partnership effectively dooms it to failure.

Leveraging the Natural Leaders: The person in charge of creating and implementing the public-private partnership must have faith in the idea, comprehend the idea, have the communication and analytical skills to advance the partnership, and be respected as an informal leader within the organization.

Be Open to Innovation: Within the boundaries of the established standards, agencies should promote creativity and sharing while being open to user innovation. It is not always a terrible idea or a sign that something won't succeed if it hasn't been done before.

Build on Past Successes: Although public-private partnerships for intelligence may be new, the agency may have had prior public-private successes in the areas of community policing or crime prevention that may be used as a springboard for the intelligence program.

InfraGard

It was realized in the 1990s that the U.S. cyber infrastructure, which supports the fundamental aspects of American life, was becoming more vulnerable to terrorist attacks, criminal intrusions, and natural disasters due to the rapid growth of computer networking and reliance on computerization for managing many aspects of government and commerce. The Federal Bureau of Investigation launched a new program in critical infrastructure security to address this problem. Its stated goal is to identify possible threats and create defenses against them. Cybersecurity and cyberthreats received the most attention.

As this project progressed, it became clear that the private sector held a significant chunk of the vital infrastructure. Thus, it was determined that only emerging countries could provide effective protection for key infrastructurea collaboration where the public and commercial sectors exchange information in both directions. This setting was the one in which InfraGard was created.

InfraGard is an information-sharing and analysis project that combines the expertise of many participants while serving their interests. InfraGard is essentially a collaboration between the FBI and the business sector. This group of companies, universities, state and local law enforcement organizations, and other partners shares intelligence in order to stop hostile activities against the United States. An FBI special agent coordinator is appointed to each InfraGard, and the two are

geographically connected. The program managers in the Cyber Division at FBI Headquarters collaborate closely with the FBI coordinator.

The National Infrastructure Protection Center oversaw InfraGard's early development, which had an emphasis on safeguarding cyber infrastructure. Following the events of September 11, 2001, NIPC broadened its focus to encompass both physical and digital threats to critical infrastructures. The mission of InfraGard consequently grew.

The NIPC was given to the DHS in March 2003, and the DHS is now in charge of things pertaining to critical infrastructure protection. InfraGard's continued participation in CIP operations is made possible by the FBI's decision to keep it as an FBI-sponsored program and its collaboration with DHS in support of its CIP goal. Additionally, the FBI has improved InfraGard's capacity to assist with its investigative work, particularly with respect to counterterrorism and cybercrime. Through InfraGard, the FBI and its partners in the critical infrastructure sector of the private sector will regularly exchange significant, two-way intelligence. Members of InfraGard have access to information that helps them secure their assets and, in exchange, provide the government with information that helps it fulfill its obligations to stop and confront terrorism and other crimes. For a more thorough approach to protecting infrastructure, information is exchanged at both the local and national levels [4]–[6].

The FBI developed the following goals to reach its goal:

1. The amount of communication and reporting between InfraGard members and the FBI on issues pertaining to counterterrorism, cybercrime, and other major crime initiatives should be increased.
2. InfraGard members and FBI agents should communicate more and share information about threats to key infrastructures, vulnerabilities, and interdependencies.
3. Offer valuable danger advisories, alerts, and cautions to members.
4. Encourage efficient communication between the DHS and local, state, and federal entities.
5. Establish a forum for members to receive education and training on counterterrorism, counterintelligence, cybercrime, and other topics important for the informed reporting of suspected crimes and attacks against the country and U.S. interests.
6. A well-designed and established program, InfraGard. The local level often sees more in-depth information exchanges, while national level activities are crucial for establishing the tone for the public-private cooperation. Having a special agent coordinator who completely grasps the idea and its value and immerses themselves in the collaboration to make sure it is a fruitful connection is essential to the success.
7. Police and security information network:
8. County of Nassau, New York

The Nassau County Security/Police Information Network is a dynamic, multifaceted relationship between the business sector and the Nassau County Police Department that aims to reduce crime by disseminating vital and timely information. This program is intended to support business continuity plans and homeland security measures, as well as to encourage information sharing that is essential to the success of defending Nassau County citizens and companies.

Sharing information, identifying and debating criminal patterns and countermeasures, and cooperating to safeguard people and property are all objectives of SPIN. The police department

or any other county agency may transmit information through SPIN to the whole public or a particular sector. Additionally, Nassau County's municipal, state, and federal law enforcement agencies, as well as public transit and other governmental organizations, are all connected by SPIN. Because of this, SPIN's multilevel strategy enables communications to be specifically addressed to law enforcement, verified security directors, or chambers of commerce and civic groups.

Members of SPIN are informed through email of developing crises as they happen. Notifications of bank robberies, significant road closures, delays in public transit, significant fires or explosions, civil unrest, public health or weather problems, or any other events compromising public safety or business continuity are included in the messages. Additionally, SPIN is used to send Sex Offender Registry alerts to exposed businesses. Members may communicate with one another or ask questions about safety-related issues using SPIN.

The creation of such a vast network has numerous, far-reaching applications, including: assisting in the capture of criminal suspects; informing users of the most recent criminal trends; assisting in the continuation of business through traffic delay notifications; and facilitating the massive exchange of information. The network also enables the police department to provide participants access to training materials that will improve the safety of everyone who lives in and works in Nassau County. When appropriate, informational briefings are arranged to go over current security-related topics. Domestic terrorism, the Republican National Convention, gang awareness, and the National Response Plan have all been discussed in meetings.

With the recent creation of a Security Advisory Council, SPIN has broadened the scope of its public-private cooperation in recognition of the enormous amount of knowledge, skill, and resources available in the business sector. using the knowledgethe development of policies supporting homeland security, crime-prevention and crime-reduction methods, as well as working toward a coordinated response to important crises. The Council is made up of security experts and police personnel. The first undertaking of the Security Advisory Council is Digital Video.Guidelines for Surveillance, was just finished. The policies were discussed in an SPIN meeting before being published on the department's website.In collaboration with the Nassau County Office of Emergency Management, SPIN is able to send information to any sector of the private sector that is organized into its own email distribution lists, including the whole membership of SPIN.In addition to being rational, SPIN's architecture is also readily customizable and expandable to accommodate agencies of all sizes.

The non-law enforcement government departments and functions that surround its core of law enforcement are some of the simplest to work with and meet and speak with on a daily basis.SPIN, which relies on email and a web portal, has proven very affordable to install, is quicker than face-to-face efforts, requires less personnel, and makes participation simpler for many private-sector organizations, especially those with a small staff. However, it has been experimentally shown to be quite successful.

Terrorism Awareness Program of Jani-King Janitorial Services

The biggest commercial cleaning franchise in the world, Jani-King International, Inc., located in Dallas, has introduced a training program for its franchisees and staff to provide an extra layer of protection to the more than 50,000 buildings that Jani-King cleans. 10,000 franchisees will get

training on how to identify possible risks to workplace and facility security and report them to the appropriate authorities.

Jani-King is of the opinion that everyone would benefit from and profit from a strong and proactive strategy to counterterrorism. According to Jerry Crawford, president of Jani-King, "prevention" is the essential word here. To assist lessen the likelihood of terrorist threats, we wish to establish a security force multiplier.Crawford claims that Jani-King is one of the only industries where big enterprises, educational institutions, nuclear power plants, and utilities figuratively give over the keys to their buildings and provide access to restricted regions. "We feel obligated to take additional steps to help maintain the safety of these buildings,"

Crawford said the training program for Jani-King will explicitly instruct staff members and franchisees on three crucial aspects of terror prevention: awareness, identification, and reporting. According to Crawford, the training will include prospective security risks knowledge, threat identification abilities, and appropriate reporting methods. Crawford presented an example, saying "Franchise owners will not be trained to confront suspicious persons." "Night after night, our teams clean the same buildings. The usual activity is seen. We want our staff members to recognize suspicious behaviour and know how to report it.

Information Sharing, Homeland Security, and the Private Sector

Public-private partnerships play a significant role in all facets of the intelligence process, but the DHS's efforts have given it the most thorough framework. DHS has created a thorough framework for information sharing, guided by law, executive orders, and homeland security presidential directives. Each has the capacity to advance the intelligence process.

In order to handle its connection with the private sector, the DHS model has built a variety of institutional channels. These systems are designed to go beyond intelligence gathering and include the many components of the National Strategy for Homeland Security, which encompass procedures "to protect, prevent, respond to, and recover from" terrorism and other domestic threats, whether they be man-made or natural. Examining these procedures from an intelligence standpoint is the main goal of the present debate.

Private Sector Non-Vetted

Critical Infrastructure Sector Partnership

The owners and operators of the nation's essential infrastructure and knowledge resources, as well as the federal, state, municipal, and tribal governments, share responsibility for protecting the nation's critical infrastructure. For three interconnected reasons, collaboration between the public and private sectors is essential:

1. The majority of the country's vital infrastructure is owned and managed by the private sector, at around 85%.
2. Important information about threats that might damage or destroy the essential infrastructure is available to government authorities.
3. Security initiatives, R&D initiatives, and other resources are within the jurisdiction of both the public and private sectors; they may be more successful if addressed and shared, as necessary, in a partnership environment.

The sharing of sensitive information by the government is restricted, and the private sector is hesitant to make business processes accessible to people outside of the corporate structure, among other factors that hinder information sharing for protecting critical infrastructure. Mechanisms have to be put in place to improve the exchange of crucial information while preserving the duties of each party due to the significant but uncertain understanding by both sides. The NIPP and Homeland Security Presidential Directive 7 establish the general foundation for a planned collaboration between the public and commercial sectors for the security of the CI and KRs. To improve information-sharing policies and practices, this sector partnership framework promotes the creation of Sector Coordinating Councils and Government Coordinating Councils.

Councils for Sector Coordination. Businesses that provide a similar or comparable product or service are referred to as "sector"s. In the airline industry, for example, Delta Airlines and United Airlines are corporate rivals, but they also face similar risk and security issues. In the case of homeland security, sectors are designated in relation to the defense of American sovereignty and people, including everything from the delivery of crucial services to the continuation of the political and economic systems. The sector-wide efforts and initiatives that are intended to enhance the security of the country's vital infrastructure are encouraged and made easier to coordinate by the sector-coordinating councils. They are self-organized, self-led, widely representative of owners and operators in the industry, and they have a critical infrastructure protection and homeland security emphasis. The DHS strongly prefers that an owner or operator serve as the chair of each SCC. However, it is the responsibility of each SCC to define the sector's boundaries, establish the requirements for membership, seek widespread participation and representation of the sector's diversity, and establish the governance, business case, and work procedures of the sector's SCC. Government agencies may suggest including various parts of a sector.

Councils for Coordinating Government. To identify and create cooperative solutions that enhance the preservation of essential infrastructures, the Government Coordinating Councils bring together various federal, state, local, and tribal interests. For every sector involving essential infrastructure and important resources, GCCs act as the SCC's equivalent. To support the country's homeland security mandate, they offer interagency coordination on CI and KR plans and activities, policy, and communication across government and between government and the sector. The GCCs collaborate with the SCCs and aid their efforts to develop, implement, and carry out the essential sector-wide security measures to support the CI and KR sector. The government and its relationships with the owners and operators of CI and KR may provide GCCs with complementary resources.

Advisory Council for the Critical Infrastructure Partnership

The DHS established the Critical Infrastructure Partnership Advisory Council to help coordinate federal infrastructure protection programs with private sector and state, local, territorial, and tribal government infrastructure protection initiatives in order to facilitate the effective defense of our nation's critical infrastructure.

CI and KR owner/operator institutions, as well as their authorized trade or comparable groups listed as members of existing SCCs, are included in the membership of CIPAC. Representatives of the federal, state, municipal, and tribal governments make up the GCC members of CIPAC.Members of SCCs and GCCs may cooperate internally and with the private sector, share

information, and participate in the whole spectrum of critical infrastructure protection operations using the framework provided by CIPAC. It allows them to openly communicate and exchange sensitive information and suggestions on dangers, weaknesses, preventative measures, shared actions, and lessons learned. CIPAC is consequently free from the Federal Advisory body Act's requirements that an advisory body make its operations public.

GCC and SCC members take part in Joint Sector Committees that make up CIPAC. For instance, members of the food and agriculture GCC and SCC make up the food and agricultural Joint Sector Committee. The selected private-sector and agency heads from each Joint Sector Committee make up the one Joint Cross-Sector Committee that is part of the CIPAC.

Terrorism Early Warning Group Special Note

Although the Terrorism Early Warning Group concept's structure and procedures go well beyond both private-sector and intelligence-related concerns, it is crucial to recognize the private-sector involvement.In order to generate a variety of intelligence products at all levels of response that are particularly suited to the user's operational function and needs, 47 TEW groups include analysts from municipal, state, and federal agencies as well as input from the business sector and nonlaw enforcement public sector. Through the incorporation of information and analysis from diverse, interagency teams, TEW groups aim to detect emerging dangers and give early warning. When intelligence is gathered from all possible sources via all-source/all-phase fusion, information and decision support are available at all stages of a threat or a response to a threat [7]–[9].

A TEW tries to identify globally spread dangers and understand their effect on a local community, therefore embodying the idea of thinking globally while responding locally in many ways. This calls for more than just information sharing; it calls for collaborative information fusion and the gathering of intelligence by cooperating nodes dispersed throughout the many sites where terrorists operate, plot, or attempt to launch attacks.49 Because of this, it's important to gather a variety of information from a variety of sources, including the private sector, in a coordinated and integrated manner.

The TEW idea and methodology are founded on the understanding that regional and local agencies both create and consume information. The TEWs must be connected into a nationwide network, which is supported by the tenets listed below:

1. Domestic civil protection intelligence gathering is not only a top-down, nationally controlled operation.
2. The movement of intelligence must be lateral, top-down, and bottom-up. Additionally, there is a need for independent of federal agencies, bilateral police information exchange and collaboration.
3. The local police, public health, and safety organizations may be the first to notice signs.
4. The need for local accountability to safeguard the populace and provide solutions.
5. Access to national intelligence products requires organization, responsibility, and rules.
6. Partners in the processing and dissemination of intelligence are regional entities. Local expertise is very valuable.

Additionally, even while TEW operations place a high priority on prevention and deterrent, the domestic intelligence effort is not just focused on assisting with criminal investigations or pre-

attack, pre-event prevention. In order to create efficient consequence management initiatives during assaults, information sharing and access to a broad variety of intelligence products are required. Anecdotal evidence indicates that the TEW, especially in broad, multijurisdictional regions, is an effective approach for handling complicated diversified information. The TEW idea involves much more than the intelligence process, as was already noted. As a result, it necessitates increasing levels of partner engagement. However, it is a project that has to be looked at when examining any element of public-private partnerships for counterterrorism [10]–[12].

CONCLUSION

The success of these collaborations depends on the public and private sector parties developing strong bonds of trust. In addition to a dedication to common aims and objectives, this calls for constant communication and cooperation. Additionally, it's critical to define precise processes and rules for data protection, security, and information exchange. This entails making sure that each partner conforms with pertinent legal and ethical requirements, that sensitive information is secured, and that it is only shared with authorized individuals. In conclusion, creating a successful public-private partnership for intelligence requires a cooperative and strategic approach that is motivated by a clear understanding of each partner's roles and responsibilities, shared goals and objectives, and established protocols for information sharing, data protection, and security. Public-private partnerships may play a key role in managing complex threats and dangers and enhancing public safety by establishing strong bonds and trust and making the most of each partner's particular skills and resources. This conversation aimed to highlight the significance of P3I and the benefits that these alliances may provide the intelligence gathering process. A public-private partnership's development and implementation processes were discussed, along with the difficulties that would be faced. Even with the benefits of P3I, these partnerships still need everyone's creativity, cooperation, and flexibility to be established successfully. There will be problems that are difficult to address and new connections that change the way things are. However, the value acquired may be crucial for ensuring the safety of our communities.

REFERENCES

[1] P. Lauriola *et al.*, “Advancing global health through environmental and public health tracking,” *International Journal of Environmental Research and Public Health*. 2020. doi: 10.3390/ijerph17061976.

[2] V. Greiman, “Public private partnerships in cyberspace: Building a sustainable collaboration,” 2015.

[3] S. B. Kopelowitz, “A multiple case study investigation into the relationship between the role of the donor and that of the educational leader in policy-making, in Jewish education in North America.,” *Dissertation International Section A: Humanities and Social Sciences*. 2009.

[4] J. A. Morgan, J. R. Porter, D. M. Karrer, and V. M. Rodriguez, “STRATA-1: A public/private/academic partnership for undergraduate applied research,” 2016. doi: 10.18260/p.25881.

[5] N. N. Agarwal *et al.*, “Technological Forecasting & Social Change E-health and wellbeing monitoring using smart healthcare devices□: An empirical investigation,” *Res. Policy*, 2020.

[6] F. Ruiz-Nuñez and Z. Wei, “The institutional and regulatory environment for public-private partnerships in infrastructure in emerging markets and developing economies,” in *Infrastructure Investments: Politics, Barriers and Economic Consequences*, 2017.

[7] D. J. Sessa and J. L. Willett, *Paradigm for Successful Utilization of Renewable Resources*. 1998. doi: 10.4324/9781003040804.

[8] C. C. Cantarelli, B. Flybjerg, E. J. E. Molin, and B. van Wee, “Cost Overruns in Large-Scale Transport Infrastructure Projects,” *Autom. Constr.*, 2018.

[9] C. Rissel, L. Jackson Pulver, and M. Wise, “Editorial – Advancing Indigenous health,” *Heal. Promot. J. Aust.*, 2004, doi: 10.1071/he04179.

[10] D. Sessa and J. Willett, *Paradigm for Successful Utilization of Renewable Resources*. 1998. doi: 10.1201/9781439832035.

[11] J. A. Laub, “Assessing the servant organization; Development of the Organizational Leadership Assessment (OLA) model. Dissertation International,” *Procedia - Soc. Behav. Sci.*, 1999.

[12] J. A. Laub, “Assessing the servant organization; Development of the Organizational Leadership Assessment (OLA) model,” *Diss. Abstr. Int.*, 1999.

CHAPTER 19

MANAGING INFORMATION: A CLOSER LOOK AT SUSPICIOUS ACTIVITY REPORTS, INTELLIGENCE REQUIREMENTS, COLLECTION, ANALYSIS AND PRODUCTS

Dr. Samrat Datta, Associate Professor
Seedling School of Law & Governance, Jaipur National University, Jaipur, India
Email id-samratdatta30@jnujaipur.ac.in

ABSTRACT:

Managing information in the context of law enforcement and public safety requires a systematic approach that involves the collection, analysis, and dissemination of intelligence products based on specific intelligence requirements. One critical tool in this process is the use of Suspicious Activity Reports (SARs), which provide law enforcement agencies with a mechanism for reporting and sharing information about potential threats and suspicious activities. To effectively manage information, law enforcement agencies must establish clear intelligence requirements that are based on specific operational or investigative needs. This involves identifying the types of information that are needed to support operational objectives, as well as the sources and methods that can be used to collect that information.

KEYWORDS:

Counterterrorism, Crime Prevention, Data Management, Law Enforcement Intelligence, Suspicious Activity

INTRODUCTION

The case study that follows is a genuine one from Ford County, Kansas. One of the major cattle-producing regions in the country is Ford County. Here, tens of thousands of cattle are reared and processed annually. The Kansas Bureau of Investigation and the Ford County Sheriff's Office created a program with funding assistance from the National Institute of Justice to ascertain how public safety organizations could work with the private-sector cattle farms, sale barns, and processing plants in case an infectious disease was introduced either intentionally or unintentionally. This was done because of the important role cattle play in the American food supply as well as the economic impact of the cattle industry in Kansas.

Particular Difficulties:

Sharing of Information

These stood out as the most important for the present example despite the fact that there were many additional factors, especially those relating to emergency reactions. Even though there had been several discussions and agreements previous to the simulation, it became clear after a thorough exercise that the private firms and public safety authorities had noticeably divergent opinions on these problems.

Several of the problems that surfaced were:

1. Instead of cooperating, law enforcement often adopted an aggressive posture and provided directives.
2. Because they believed it was inappropriate to share this information with the private sector, law enforcement was hesitant to provide specific sorts of information concerning threats, suspects, and related data.
3. Because they believed public safety authorities wouldn't understand some kinds of crucial information, private corporations often withheld it.
4. Due to the negative economic effects of such acts, private enterprises opposed ceasing all operations.
5. Due to the potential financial consequences, private businesses advocated against stopping orders for cattle that were already being sent. On the other hand, law enforcement often discounted the economic factors.
6. The takeaway from this exercise was that extra preparation was required even though there had been substantial planning by a broad range of individuals with the intention of determining the best way to manage an emergency. Both groups had quite different opinions on the problems.
7. Public-private partnerships are essential and useful, yet they are challenging. In the event of a real danger, the tension and conflict that resulted from an exercise would be amplified. As a result, careful planning, communication, training, and exercise are crucial.

DISCUSSION

Information is the key to everything. The engine that powers the intelligence process is raw data. Constant, bidirectional information flow coming from a variety of sources is ideal. Several procedures established in earlier s are used to manage this information. The goal of this is to expand on the talks of these processes and provide insight into the most recent information management applications for intelligence. There is value in taking a closer look at these integrated processes as tools for both the information gatherer and the intelligence consumer given the rapid evolution of law enforcement intelligence, particularly as influenced by the development of fusion centers, Intelligence-Led Policing, and the Information Sharing Environment [1], [2].

Reporting Suspicious Activity

For a long time, law enforcement intelligence has utilized both requested and impromptu information to learn about potential criminal risks. This information, which was formerly known as "tips and leads," was often given to the intelligence function by police, informants, and sometimes by members of the community. In other instances, intelligence officers would distribute particular sorts of data that were necessary to provide answers to particular inquiries regarding potential dangers to the country; i.e., intelligence needs. While patrol police and criminal detectives often use the public as a source of information through Neighborhood Watch or Crime Stoppers, this is less frequently the case for the intelligence role.

The procedures for tips and leads have evolved along with the mindset and methods of intelligence. It has been acknowledged that a proactive strategy to produce more of this kind of material for the intelligence function has value. Beyond just gathering more data, a better

organized procedure was required to gather, assess, store, and distribute this data. The procedure is changing as a result of coordinated development bythe Department of Justice, the Program Manager's Office for the Information Sharing Environment, and the Intelligence and Analysis Directorate of the Department of Homeland Security on behalf of the Global Intelligence Working Group. The management of suspicious behaviors via the use of Suspicious Activity is what these new efforts collectively refer to.

Reporting Suspicious Activity to a Law Enforcement Agency

An initiative by the Major Cities Chiefs Association provides further context for reporting suspicious conduct as follows:

1. The Suspicious Activity Report procedure focuses on what law enforcement agencies have been doing for years collecting data on criminal activity-related behaviors and incidents and creating a system for information sharing to identify and stop criminal activity, including that connected to domestic and international terrorism.
2. A systematic method for recording and sharing observed actions that are suggestive of criminal conduct is known as suspicious activity reporting. Information including "tips and leads" can originate from the public, business sector partners, or law enforcement officials. To get the SAR incorporated into the intelligence function's analytical process, this information should be put in writing and processed by the agency.
3. Reports of Suspicious Activity come in three different varieties. The financial SAR comes first. The Bank Secrecy Act, which requires a broad variety of financial institutions to record certain sorts of transactions to the Treasury Department, required this. Money laundering or the trafficking of illegal goods are the suspicious activities most often linked to financial SARs.
4. The second is the SAR for all offences. Simply said, this is the recording and reporting of any suspicious conduct linked to a crime. A law enforcement officer can see the action or get a complaint about it. A Field Intelligence Report, Field Interview Report, or Miscellaneous Investigation Report are some of the traditional titles that numerous law enforcement organizations have used for something similar.
5. The Information Sharing Environment Suspicious Activity Report is the third category. Specifically tied to terrorism or crimes that aid or assist terrorist planning and actions, this is the documenting of suspicious activities. An ISE-SAR is handled differently from an all-crimes SAR, as will be discussed later.
6. Line officers at law enforcement agencies normally use the same forms and procedures for both all-crimes and ISE-SARs; however, when the SAR is processed by an intelligence unit or fusion center, the ISE-SAR is handled and disseminated in a different way. The ISE's mandate to combat terrorism and offenses supporting terrorism is the basis for the varied processes.

A law enforcement agency's intelligence strategy for handling reports of suspicious conduct should be its first step. To establish a successful procedure for reporting suspicious behavior, certain organizational elements must be in place. Among them are:

1. A method used across the organization to report questionable conduct. A formal component of the agency's records management system must be a policy governing the format, usage of case numbers, and processing of the SAR.

2. SARs are shared internally with other agency parts and externally, if necessary (for example, with a fusion center), via an agency-wide procedure. If a complaint of suspicious conduct is just made and kept to yourself, it is of little use.
3. Educating employees on the warning signs of potential crimes. The things that are known to be connected to crimes signs, symbols, objects, and behaviors are known as indicators. For instance, much as the presence of certain precursor chemicals is known to be related with "cooking" methamphetamine, certain symbols are known to be specifically tied to right-wing extremist organizations. There will almost always be some kind of signs for any kind of crime. Personnel must thus be educated to spot these signs in order to assist reporting of suspicious behaviour. Importantly, instruction should stress that suspicious activity should be considered based on the "totality of the circumstances," not simply the observation of a single indication.
4. A review and purging procedure for SARs. Not all actions that at first glance seem suspicious are unlawful. As a result, the SAR policy has to establish a procedure for reviewing the SAR and confirming that there is a plausible criminal link. If not, the SAR has to be cleared. Importantly, the review and purge process should include consideration of the agency's privacy policy [3]–[5].

SAR financial

The Bank Secrecy Act mandates that financial institutions submit SARs to tell the federal government of transactions connected to potential legal or regulatory infractions in order to aid law enforcement authorities in their efforts to fight money laundering, terrorism financing, and other financial crimes. The financial SAR was developed to replace several reports needed by various financial regulatory bodies to disclose and then look into financial transactions that could be connected to criminal activity. All financial SARs are submitted via the Financial Crimes Enforcement Network in order to significantly improve the effectiveness of illicit financial investigations.

Even though it is the responsibility of the financial institutions to file the financial SAR, law enforcement intelligence units extensively work with these reports in the course of identifying illegal activity, identifying offenders, developing cases against ongoing criminal enterprises, and identifying emerging threats based on trend and pattern analysis of reported financial irregularities.Since almost every criminal organization requires a financial network, the financial SAR may be a valuable tool in the intelligence gathering process. Because it touches on a broad range of financial institutions and operations, the SAR is a crucial instrument for intelligence analysis.

A mutual fund

Bringing entering or leaving the United States with more than $10,000 in cash or other financial instruments. those who send or receive more than $10,000 in cash or other financial instruments into or out of the United States. An important information source for the intelligence cycle is SARs. The reports often point out behavior associated with dangers that were not previously understood. In other instances, the SAR offers details about an investigation that aid in better understanding a known danger or new aspects of a known threat. The SAR assists in developing new intelligence needs as well. The SAR plays a crucial role in the intelligence cycle, even if it is by no means the sole source of fresh information. This is especially true when it is backed by

police who have received thorough training on the signs of terrorism and crime and who routinely report any suspicious behavior.

Techniques for Reporting Suspicious Activity

The underlying presumption that many individuals encounter suspicious activity in their everyday lives but do not identify it or believe the suspicious conduct is not of sufficient relevance to report is a crucial component of the suspicious activity reporting procedure. As can be shown, the objective is to enhance the reporting of suspicious activities with the expectation that as this reporting rises, so will the likelihood of learning crucial danger information. The following are essentials for success:Recognize questionable conduct that is "focused"gather detailed information on suspicious activitiesMake sure that every action is reported through the appropriate internal or external channels, like a fusion center.

Review and evaluate the data, and if credit is due, distribute it or put it in a database that can be searched.This innovative idea of reporting suspicious activities has two connected elements. The first aspect is the creation of a model for streamlining procedures for detecting suspicious activities. Expanding the group of people who are urged to report questionable activities, such as neighborhood residents and business partners, is the second dimension.

When it comes to the first dimension, "suspicious activity" may refer to a wide variety of actions. Furthermore, a person's definition of what is suspicious will change based on their life experiences, morals, and other societal influences. The right way must beoffered in order to characterize suspicious behaviour in terms of the kinds of information required for the intelligence process. A three-part paradigm, consisting of observe, document, and report, may be utilized to achieve this.

Reporting Suspicious Activity Model

Observe

People must pay attention, but their observations must be focused. To guarantee that the observed conduct has a possible criminal relationship, awareness training is required. Frequently, training involves discussing "indicators" behaviors that are logically connected to possibly illegal conduct. Two essential elements make up indicators: first, the emphasis must be on conduct rather than personal characteristics. "Attributes of an individual" might include perceived4 color, ethnicity, gender, religion, and so forth. Moreover, there must be a fair chance that the conduct may be connected to a crime; that is, the behavior must be more than merely "odd" or "unusual." To put it another way, a person shouldn't be labeled "suspicious" just because they have certain qualities; suspicion must be founded on conduct. The characteristics may be utilized appropriately as part of the description of the suspicious individual if suspicious activities are seen and recorded as they pertain to the planning or commission of a crime. These rules must, of course, be implemented in the context of the observer's specific situation and other available information.

Understanding the actions and symbols that are especially suggestive of criminal conduct is the second crucial element. This implies that training or knowledge regarding shady activity may be helpful to observers. There are training programs available for law enforcement professionals that may provide crucial current knowledge concerning danger indicators, both in-person and online. The State and Local Anti-Terrorism Training Program, which is supported by the United

States, is one such initiative. Justice Assistance Bureau. In-depth information on signs of domestic and international terrorism/criminal extremism is provided to police during SLATT training from the viewpoint of a person who an observer assumes is from the Middle East but is really of a different ethnicity.

Communities Against Terrorism, which is also funded by the BJA, is a program aimed at the non-law enforcement community to provide indicators of suspicious activity. The CAT program helps law enforcement in the development of partnerships with local residents because when local residents are aware of potential indicators of terrorism activities, they may be able to provide law enforcement with useful information. The CAT produces templates of flyers with possible indications that law enforcement may disseminate to certain businesses to help with their outreach efforts.

Document

If the observer explicitly discloses the suspicious individuals and the precise details of the suspicious behavior when suspicious activity is detected, the value of the SAR is boosted. Although law enforcement officials are trained to gather this data, the general population, which reports a lot of suspicious behavior, often lacks this understanding. Community members need to be made aware of the types of information that are most useful through public education campaigns: thorough descriptions of the suspicious individuals and their vehicles, the scene of the activity, the actions that seemed suspicious, and any objects the individual may have that contributed to the suspicious activity are all examples of information that must be recorded. Once again, the CAT software offers the particular information for various company types.

Report

In order to provide uniform standards for recording and reporting SARs for law enforcement officials, new procedures later referred to as the Nationwide SAR Initiative—are being established. These procedures will improve the sharing of SAR information. Since the ISE is driving the process, it initially focuses specifically on terrorism.7 However, because the standards are being developed with assistance from the GIWG and the Criminal Intelligence Coordinating Council, it is intended that they eventually apply to "all crimes and all threats". More uniform reporting of suspicious activity is desired, with cops using a defined reporting procedure.

For neighborhood members, reporting suspicious activity has proven to be more difficult. Information has often not been submitted because the community was simply unsure of how or to whom to report it. The ability of law enforcement organizations to support citizen reporting has improved; for instance, a growing number of law enforcement organizations have created SAR websites, unique phone lines, and initiatives tied to organizations' community-based programs. The objective is to raise awareness of potentially illegal activity, record important details about the behavior, and provide this information to a law enforcement agency. The information may often provide the intelligence analyst crucial parts of the jigsaw they were lacking. In other instances, the intelligence can alert a law enforcement agency to possible illegal conduct that it was previously ignorant of.

Law enforcement is more likely to recognize and reduce risks if measures are implemented to encourage individuals to report suspicious conduct. Making ensuring that suspicions are

grounded in behavior and that the observer gathers as much precise data as possible to report the suspicious activity are important components of this procedure. Once this information has reached the intelligence function, it must be analyzed to determine what else is known about the suspicious behavior and to specify what other information will be required in the future to determine if a threat really exists and, if so, how it may be neutralized.

Personal identifying information and SARs

Whether Personal Identifying Information is included in the report is a critical SAR concern. Any information or piece of data that may reasonably be used to identify a particular person is considered to be PII. Civil rights guidelines and privacy standards must be followed while collecting PII.A PII-SAR is a report that identifies a particular person or offers enough detail about them that it is fairly possible to determine their identity, such as their physical description and home address. Retention, security, and distribution policies must be stringent under these circumstances.

It should be emphasized that SARS are often not characterized as criminal intelligence and the 28 CFR Part 23 criteria are not necessary for SARs. The safest method is to use information management standards that are compliant with the 28 CFR Part 23 rules. However, the recommendations provide a useful framework for defending civil rights and privacy. In order to secure the safety of personal information and civil freedoms, various authorities are now creating SAR-specific standards. Reports describing suspicious situations, signs, and/or behaviors of unidentified people are known as non-PII-SARs. The law enforcement agency has a lot of discretion over how long to keep and share information if PII is not included in the report. Regardless of the SAR format a law enforcement agency chooses, separate protocols for processing SARs including PII and those without should be established.

Putting Limits on Information and Reports of Suspicious Activity

SAR information is sensitive for a number of reasons, including the fact that it is often unclear what led to the reporting of the information and why it was reported in the first place. Law enforcement must thus establish if legal action was mistakenly thought to be illegal and whether the information was provided truthfully. The guidelines provide recognized civil rights and privacy standards to show that the law enforcement agency is doing its part to protect people's rights, despite these potentially restricting factors. When suspicious activity is reported to law enforcement, the agency has a public criminal intelligence records system. Counsel should analyze actual policies with particular attention to each state's legislation.

Due to this sensitivity, the Privacy Committee of the Global Justice Information Sharing Initiative identified six crucial points in the SAR process where information management controls should be implemented to ensure the security and privacy of PII while also enabling the agency to continue its investigation into the behavior. These safeguards are based on the same information management concepts that secure data in a system of criminal intelligence records. The six controls, with minor modifications from the Privacy Committee's findings, are as follows:

1. **Receipt/Collection**. When information about suspicious behavior is received or collected, it should be evaluated for sensitivity and secrecy using corroborating data, if feasible. The best attempt should be taken to confirm or deny the information in order to

determine if there is a criminal predicate or whether the SAR is unsubstantiated as soon as feasible. Information gathering that is primarily expressive activity should be outlawed under the First Amendment.

2. **Storage.** Information about suspicious behavior should be stored in the same manner as data that raises a valid suspicion. A logical separation or labeling of the unverified SAR from other information, accompanying paperwork, and an audit and inspection procedure should all be part of those criteria.
3. **Access.** Access to information concerning suspicious conduct should be treated similarly to access to information that raises the bar of reasonable suspicion because there is ambiguity about the information's trustworthiness and/or veracity. Only where there is a legitimate need for the information and a right to know it to carry out a law enforcement, homeland security, or public safety task may access be granted.
4. **Dissemination.** If suspicious behavior data is routinely gathered and retained for interagency dissemination, it should only be made available to law enforcement, homeland security, and other government agencies in response to an enquiry. the sake of public safety. Unconfirmed suspicious activity involving PII shouldn't be published in bulletins or other similar products on a regular basis, but it can be entered into secure databases and given to the appropriate law enforcement, homeland security, and public safety organizations that have a right to know and need to know the information for the sake of the public.
5. **Retention.** The retention duration for information about suspicious behavior should be determined by policy and be long enough to allow the agency's knowledge and resources to evaluate the material's reliability. Records of suspicious behavior need to be labeled with a "disposition" designation, such as "undetermined/unresolved" or "cleared/unfounded," to make it apparent to the user what state the material has. When establishing retention and purge processes, agencies should take into account the necessity to keep some kind of suspicious activity data for statistical reporting and performance evaluation.
6. **Security.** Similar physical and technological security precautions should be taken as with information raising the bar of reasonable suspicion.

Constant attention to accuracy, privacy, and validating the information in the SAR should permeate every aspect of this procedure, as supported by the PM-ISE's report to Congress:American citizens' civil liberties, information privacy, and other legal rights are of utmost importance. At the local level, SARs will be integrated into the systems and processes already in place to manage other criminal intelligence and crime-related data in order to take advantage of these policies and procedures. Reports containing personally identifiable information that are unfounded or that cannot be reasonably associated with criminal activity will not be shared outside of the originating entity. Multiple levels of review and vetting will be established to ensure that information is lawfully gathered and managed.

The fact that all information may be helpful at some unspecified point in the unforeseeable future complicates these procedures among many law enforcement agents. This conviction results in a strong unwillingness to discard any documents or reports. It is important to keep in mind that most SARs consist of unasked-for suggestions and leads from a variety of reliable sources. There is no need to keep any PII if the follow-up indicates that the accusation in the SAR is baseless [6], [7].

CONCLUSION

Overall, managing information in the context of law enforcement and public safety necessitates a thorough and methodical approach that includes the creation of precise intelligence requirements, the gathering of pertinent information, the analysis of that information to develop intelligence products, and the dissemination of those products to the proper stakeholders. Law enforcement organizations may more accurately detect possible dangers and vulnerabilities and take preventative action to address them by handling information properly and using tools like SARs. Information must be examined once it is gathered to spot patterns and trends that might point to hazards or risks. In order to pinpoint critical insights and create intelligence products that are suited to particular operational or investigative objectives, this process entails evaluating and synthesizing data from a variety of sources. Last but not least, intelligence outputs need to be shared with the right parties, such as other law enforcement agencies, allies in government, and businesses. To guarantee that intelligence products are transmitted in a timely and secure way, this calls for excellent communication and coordination between partners.

REFERENCES

[1] A. Shahaab, "Managing Gender Change Information on Immutable Blockchain in Context of GDPR," *J. Br. Blockchain Assoc.*, 2020, doi: 10.31585/jbba-3-1-(3)2020.

[2] T. N. Haryani, "Pendampingan kelompok informasi masyarakat desa Sumberdodol Kabupaten Magetan dalam pengembangan iklan pariwisata desa," *Aptekmas J. Pengabdi. Kpd. Masy.*, 2020.

[3] S. Hadi, "Dimensi Ekonomi Produktif dalam Regulasi Wakaf di Indonesia," *TAWAZUN J. Sharia Econ. Law*, 2020, doi: 10.21043/tawazun.v3i2.7887.

[4] T. Du Plessis, "Information and Knowledge Management at South African Law Firms," *Potchefstroom Electron. Law J.*, 2017, doi: 10.17159/1727-3781/2011/v14i4a2589.

[5] L. V. Bogatyryova, O. A. Shepeleva, and V. A. Gruzman, "Methods of socio-economic systems analysis in order to diagnose the problems of transformation of law in the context of digitalization," in *IFAC-PapersOnLine*, 2021. doi: 10.1016/j.ifacol.2021.10.434.

[6] I. D. Patdu and A. S. Tenorio, "Establishing the legal framework of telehealth in the philippines," *Acta Med. Philipp.*, 2016, doi: 10.47895/amp.v50i4.763.

[7] P. B. Turnes and R. Ernst, "A framework for transparency in international trade," *Investig. Eur. Dir. y Econ. la Empres.*, 2015, doi: 10.1016/j.iedee.2014.01.001.

CHAPTER 20

POLICY RECOMMENDATIONS FOR DEVELOPING AND MANAGING A SUSPICIOUS ACTIVITY REPORTING SYSTEM

Ms. Surbhi Dubey Dadhich, Assistant Professor
Seedling School of Law & Governance, Jaipur National University, Jaipur, India
Email id- surbhi.dubey@jnujaipur.ac.in

ABSTRACT:

The Suspicious Activity Reporting (SAR) system is a critical tool used by law enforcement agencies to identify and investigate potential threats to public safety. The SAR system allows law enforcement personnel to report and share information about suspicious activities that may be indicative of criminal or terrorist activities. The SAR system is designed to collect information from a wide range of sources, including law enforcement officers, private sector organizations, and members of the public. This information is then analyzed by trained personnel who use a variety of techniques, including data mining and pattern analysis, to identify potential threats and risks.

KEYWORDS:

Confidentiality, Congressional oversight, Intelligence collection, Judicial oversight, Law enforcement intelligence, Privacy protection, Probable cause.

INTRODUCTION

As has been made clear in this debate, law enforcement organizations are working more and more on creating a system that is both thorough and organized in order to encourage the reporting of suspicious conduct.With assistance from the Departments of Justice and Homeland Security, the Major Cities Chiefs Association and the Global Justice Information Sharing Initiative took on this assignment. This initiative produced a number of important suggestions, some of which are as follows:

1. Agencies should inform policymakers on the problems and procedures involved in reporting suspicious behavior in order to win their support.
2. It is important to assess all privacy and civil liberties policies and training to ensure that they adhere to national standards and current legal requirements.
3. In order to preserve privacy and civil rights, it is important that information management for the SARs process be connected with systems and procedures already in place for managing criminal investigation information and criminal intelligence.

Transparency is essential for gaining support, hence the SAR policy should be made known to the general public. To prevent crimes, especially those related to domestic and international terrorism, it is essential to collect, process, report, analyze, and share information on suspicious

activities. The SAR procedure need to focus on all offenses. The SARs procedure should apply SARs to the relevant criminal records management system or criminal intelligence records system using criminal information management protocols. Submissions for suspicious activity should not circumvent the usual 911 reporting mechanisms, the local law enforcement agency, or the agency with original authority [1], [2].

It is the receiving agency's obligation to notify the affected agency right once and to discuss coordination, deconfliction, investigation, and vetting processes with the affected agency whenever an agency gets information that has an impact on another jurisdiction. The impacted agency would be in charge of further disseminating the material once it had been reviewed. To guarantee that SARs are sent to fusion centers and regional Joint Terrorism Task Forces in a timely manner, a procedure should be devised. Determining and disseminating patterns in terrorist activity, regionally targeted threat reports, threats to important infrastructure, and general situational awareness should all continue to receive attention.

In order to identify trends throughout the nation, there is a need for a standard national technique, including similar data codes, for exchanging suspicious activity data. An important step in the SAR process is training. All staff from relevant agencies must get training to identify actions and occurrences suggestive of criminal conduct related to both domestic and foreign terrorism. The effectiveness of the initiative depends on include public outreach, law enforcement, and the corporate sector in the data gathering process. Create a uniform national approach to timely horizontal and vertical SAR data sharing that complies with civil liberties and privacy protections.

Create a uniform training curriculum to provide consistent SAR training throughout the country.These suggestions aim to safeguard civil freedoms while maximizing the usefulness of information about suspicious activities. The paper emphasizes that although these suggestions are meant to harmonize the SAR process, each jurisdiction will need to adopt rules and processes that take into consideration the particular conditions and connections in that community.

DISCUSSION

The Nationwide Suspicious Activity Reporting Initiative

The Nationwide Suspicious Activity Reporting Initiative actively promotes initiatives to safeguard American citizens' civil rights and privacy while also defending local communities against terrorism and other violent crime. The National Strategy for Information requires the establishment of a unified, standardized, and integrated process to gather, document, process, analyze, and share information regarding circumstances potentially associated with criminal activity related to terrorism in a way that rigourously protects Americans' civil liberties and privacy. The NSI is the result of a number of separate but related activities over the past several years. The NSIS requirements are addressed via a cycle of 12 interconnected operational actions known as the NSI process. The long-term objective of the NSI is for the majority of federal, state, local, and tribal law enforcement agencies to take part in a standardized, integrated method of acquiring, recording, processing, evaluating, and exchanging information concerning suspicious activities [3], [4].

"Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity" is the definition of suspicious activity. Although the Nationwide SAR

Cycle was created to improve our capacity to recognize, record, and communicate suspicious behavior connected to terrorism, the technology principles and procedural steps may be used to handle any new criminal issue. The NSI cycle purposefully adopted this methodology because terrorists may participate in a wide spectrum of illegal conduct as they plot, organize, and carry out their attacks.

The Problem. The use of locally generated information to identify and mitigate emerging crime trends, including those potentially related to terrorism, has been hampered by the lack of unified operational processes and a standardized technological approach for gathering, handling, and sharing terrorism-related suspicious activities. Additionally, the absence of uniform privacy and civil liberties laws may result in the improper gathering and storage of data, which may jeopardize Americans' right to privacy and freedom of speech.

The Answer. The NSI expands on the information-gathering efforts that law enforcement and other agencies have been doing for years to identify behaviors and events that are probably indicative of criminal conduct. Frontline and analytical staff are educated to recognize and differentiate between lawful and criminal acts as part of this standardized approach. Additionally, prior to being made accessible to other analytical and investigative staff, prospective SARs are examined and validated via the adoption of clearly defined business rules. Since fusion centers, authorized federal, state, local, and tribal law enforcement agencies, DHS Headquarters, and the FBI's JTTFs and Field Intelligence Groups can all access terrorism-related SARs thanks to common data and technical architecture standards, patterns and trends can be found by analyzing information at a greater level than is typically recognized within a single jurisdiction, state, or territory.

The NSI cycle takes into account the unique risks and vulnerabilities faced by tribal, state, and municipal law enforcement organizations. The cycle's initial step encourages governments to undertake risk assessments and utilize the results to identify and record their top information requirements. The training given to frontline law enforcement personnel and analysts about those behaviors and situations that are arguably suggestive of pre-operational planning connected to criminal activity, including those possibly related to terrorism, is guided by those information requirements. Therefore, the NSI approach and technical principles may be used to handle any developing crime issue, regardless of whether the detected risk is connected to illicit narcotics, violent gang activity, terrorism, or other types of crime.

The Advantage. More effective protection of privacy and civil rights via improved identification of criminal conduct by law enforcement of behaviors and situations. Investigators, analysts, and homeland security experts now have better access to crucial data, helping them to identify new threats to our local communities more quickly. Initial findings have already shown their importance to regional counterterrorism initiatives. For instance, 1,500 SAR were recorded in one jurisdiction during a 12-month period, and of those 1,500, more than 65 were sent to the JTTF, leading in 21 charges and convictions in state court for acts linked to terrorism. Although the significance of seeing and reporting suspicious activity is widely acknowledged, the project is not without its detractors. The following statement was issued by the American Civil Liberties Union about reporting of suspicious activity:

This too wide reporting power allows law enforcement officials to gather personal data, harass just about anybody they choose, and then transmit that data to the intelligence community. Suspicious activity report policing exposes law-abiding citizens to government intrusion into

their private affairs without justification and opens the door to racial profiling and other unlawful police actions. The importance of training is a result of these issues. It must be underlined that the main goal is to gather data on actions that serve as early warning signs of criminal conduct. Unusual or strange conduct or circumstances would not be taken into account unless there was a clear connection between them and a prospective crime. Beyond training, it's crucial to have continual supervision and a reliable evaluation system to record the process' efficacy.

Reporting suspicious conduct is becoming acknowledged as a crucial component of modern intelligence gathering. It may be a useful instrument for gathering important raw data when the right procedures and systems are in place. The procedures are still under development, thus the reader is advised of this. SARs also need to be carefully developed and controlled since they are delicate from the standpoint of civil rights. Even though there has been notable development, problems still exist. The following has been noticed by the PM- ISE:

The biggest difficulty facing the ISE may be encouraging an information-sharing culture. Sharing the appropriate information with those who need it is not just a choice in the post-9/11 environment; it is a basic value firmly rooted in law and regulation. The objective is obvious, but obtaining it will need focused effort. ISE cultural change initiatives seek to ensure that this principle is clearly understood and that managers are held accountable for implementing change in their organizations. The NSIS declares, "We will...change government culture to one in which information is regularly and responsibly shared and only withheld by exception."

Suspicious Activity Reporting: How to Make It Part of Your Agency's Daily Operations

1. Recognize the value of SAR, comprehend your part in the process, and be aware that your participation counts. Effective leadership is a crucial component. Obtain internal and external support from staff, leadership, and policymakers.
2. Create a safe, uniform reporting format and data gathering procedure for communicating suspicious behavior. Define and disseminate terrorism-related activity patterns, threat reporting with a focus on particular regions, threats to vital infrastructure, and overall situational awareness.
3. Leverage and adopt the use of common national standards like the ISE Functional Standard for Suspicious Activity Reporting, the State and Local Agency Information Exchange Package Document for SAR Reporting, the National Information Exchange Model, and the Records Management System and Computer Aided Dispatch functional standards to improve the ability to analyze suspicious activity data quickly and accurately.
4. The National Criminal Intelligence Sharing Plan, the Fusion Center Guidelines, the Findings and Recommendations of the Suspicious Activity Report Support and Implementation Project, and privacy and civil liberties templates are a few examples of appropriate guidelines and concepts that you should incorporate into your operations. To build and integrate the SAR process, use the IEPD for the SAR for Local and State Entities.
5. Implement and abide by your organization's privacy policy to preserve citizen privacy and civil rights. Your privacy and civil liberties policy should be examined and updated as appropriate to make sure that information collection, documentation, processing, and sharing linked to terrorism-related criminal conduct is particularly handled. Inform the people about the policy.

6. Institute the SAR procedure inside your agency and TRAIN people. Make sure that the people in charge of law enforcement and public safety are aware of the SAR procedure and any internal rules or procedures that apply to the sharing of pertinent information. Find out about the training programs that are available to improve or expand skills, such as the State and Local Anti-Terrorism Training Program.
7. Standardize the reporting of such data and INSTITUTIONALIZE the collection of information about suspicious activity at the local level so that it may be shared with other suitable public safety partners, such as your criminal intelligence unit, state or regional fusion center, Joint Terrorism Task Force, and other law enforcement and public safety partners.
8. Educate community members, companies, and partners on how to report suspicious behavior and who to report it to. Integrate initiatives like Communities Against Terrorism into your neighborhood. Create outreach materials to educate the public on identifying and reporting actions and occurrences suggestive of criminal activity related to domestic and worldwide terrorism.
9. Collaborate with other fusion centers located in states or significant metropolitan areas, the business sector, and public safety. Encourage interagency cooperation to make the most of each other's resources and establish a productive and efficient environment for information exchange.
10. Join a significant information sharing network, such as the Regional Information Sharing Systems, Law Enforcement Online from the Federal Bureau of Investigation, or the U.S. The Homeland Security Information Network of the Department of Homeland Security. Utilize tried-and-true technologies to communicate, exchange information, and get access to more resources.

Federal agencies generate and make accessible intelligence and other informational products to assist state and large metropolitan area fusion centers in developing geographic risk assessments.

Required Intelligence

Law enforcement is relying more and more on the usage of intelligence requirements to specify the kinds of raw data required to provide a more thorough analysis of threats as the ISE and fusion centers have expanded. Missing data is referred to as a "intelligence gap" and is necessary for efficient intelligence analysis. The knowledge required to close the gap is referred to as a "intelligence requirement". Both the gaps and the needs must be recognized and specified when managing information.

The threat environment is dynamic, so these known factors must be continuously monitored to verify the threat and determine whether a change in the threat picture is taking place. The intelligence analyst must integrate currently held information to determine what we know about a threat: these are the "known knowns." In many cases, even while we are aware of the existence of a danger in general, we are unaware of its precise characteristics, including the attack's technique, intended target, and potential timing. The objective is to continuously monitor suspicious activities and gather data from various sources that may give us an indicator of a new threat. These threats are the "known unknowns." Lastly, there are threats that may be developing, either by a known suspect or a suspect who is completely unknown to us, that we are simply unaware of. When these new signs are discovered, specifications are established to more accurately identify the danger and individuals who pose it.

The layperson would see Secretary Rumsfeld's comments as nonsensical, but in reality, he was addressing intelligence needs and gaps.Although it has long been used in national security intelligence to establish information needs concerning threats, the notion of intelligence requirements is relatively new to law enforcement intelligence. It takes a thorough approach to information gathering and analysis in order to provide the most complete picture of a danger and potential countermeasures. By explicitly concentrating on information needs rather than taking a wide dragnet approach to information collecting or waiting for the accidental discovery of crucial data, the application of requirements also improves the intelligence process' effectiveness.

To draw an example, piecing together a jigsaw puzzle without knowing what the finished image would look like is similar to the work of an intelligence analyst.The analyst must figure out how each piece of information fits together to generate a discernible picture. The gaps in the information are the missing parts, and gathering the missing pieces and filling in the gaps will help complete the image. New needs often surface when more components are located. Once enough data has been gathered, the image is crystal clear and the danger is better comprehended. It is necessary to go into more detail about the problems and procedures associated to requirements-driven intelligence since, of course, in reality it is not that straightforward.

Closing Gaps and Meeting Requirements

The method of gathering information must be targeted in order to meet certain information demands. This improves the process' effectiveness and guarantees that the appropriate information requirements are being focused. In the past, police enforcement used a strategy that was mostly dependent on instinct on what was suspect. Frequently, it was only a simple hunch based on actions or remarks that looked unexpected, excessive, or out of the ordinary. This procedure lacked objectivity and scientific rigor and was often skewed according to the officer's opinions, values, and beliefs. This procedure gathered large amounts of varied raw data, which was then sent to analysts and investigators for examination in the hope that real danger information may surface. The requirements-driven method to information collecting differs from this tradition-driven approach in a number of ways. Fundamentally, the requirements-driven approach is more scientific and, as a result, more objective, focused, effective, and trouble-free when it comes to civil rights issues. On this final point, the criminal predicate is easier to state since intelligence needs are often the result of an ongoing criminal investigation.The tradition-driven strategy is similar to casting a net in order to gather as much data as possible while assuming that there is a danger. The massive amount of information will reveal information and criminal activity's proof. It is less productive, less successful, and more likely to expose civil rights violations.Intelligence that is driven by requirements is more laser-like. It focuses particularly on the kinds of data we need to comprehend a carefully defined area of hazard.

Implementing the Idea in Law Enforcement

Former Executive Assistant Director Maureen Baginski employed requirements-driven intelligence throughout the FBI Intelligence Directorate's reengineering process. The phrase "The absence of evidence is not the absence of a threat" often said by Baginski and previously cited in Chapter 4's overview of the intelligence process perfectly captures this idea. This astute comment helps us to comprehend the significance of requirements-driven intelligence. Imagine a law enforcement official asking the Regional Intelligence Fusion Center whether there is a danger from terrorism in the area where their organization operates. In response, it can be said that there is "no evidence to suggest a terrorist threat within the region," yet there might really be an

unidentified threat in the neighborhood for which no proof has been found. Timothy McVeigh, who detonated the bomb at the Murrah Federal Building in Oklahoma City, was one of many unidentified threats in the neighborhood. Muhammad Atta, who helped plot the September 11 attacks by operating out of communities in the United States, was another unidentified danger. Although these two clearly posed hazards to their communities, no proof of such threats had been found.

We need a way to recognize these unidentified dangers, evaluate the harm they represent, and decide what steps to take to stop or lessen the threat. The procedure is challenging, particularly for a state, municipal, or tribal law enforcement organization that could have limited information gathering and analytical skills. Finding evidence of such threats requires both labor and resources in the form of efficient information sharing, strong connections with intelligence networks, continuous information exchange, and ongoing information collection, assessment, and analysis within the purview of an agency. The usefulness of fusion centers, which will have all of these qualities, and the need for agencies to be fusion center partners are reinforced by these demands. The fusion procedure is specifically designed to make optimal use of the intelligence needs model. While requirements-driven intelligence will benefit a law enforcement organization, its objectives need a time and resource investment. To participate to the process at a state or regional level, a law enforcement agency must have the bare minimum of intelligence capabilities, especially if it wants to be a reliable partner with an intelligence fusion center [5]–[7].

Comparing Crime Analysis and Intelligence Requirements

The knowledge required to make judgments about how to effectively safeguard a community from risks presented by organized crime and terrorism may be thought of as intelligence needs. Executives and managers have the trustworthy information they need to plan an operational response to a danger when requirements are met. As an example, SLTLE agencies often base operational choices about occurrences of predatory crime on the needs of crime analysis. In fact, this serves as the process's fuel. Particularly, specific patterns of crime arise as a consequence of timely examination of reported crime. Response strategies are developed to deal with both the crimes that have already occurred and the probable forecast of crimes that will occur if the crime series is not stopped, based on information derived from that analysis such as the type of crime, modus operandi, time and geographic factors, suspect descriptions, etc. To catch these serial offenders, the agency may use saturation patrol, undercover agents, dummies, surveillance, or a mix of tactics. The best operational judgments cannot be made without the data from the outcome of the criminal analysis.

Of fact, given the intrinsic distinctions between criminal investigation and criminal intelligence, crime analysis needs are significantly simpler to provide than intelligence requirements. In essence, investigations are motivated by crime, while intelligence is driven by danger. Investigations thus respond to crimes that have already happened and a known quantified universe of facts that have been discovered throughout the inquiry. In contrast, intelligence takes action as soon as a danger is recognized. In essence, intelligence is more probabilistic and pre-crime, which presents problems for both operations and civil rights.

CONCLUSION

In general, law enforcement agencies utilize the SAR system as a vital tool to recognize and counteract possible threats to public safety. Law enforcement authorities can prevent criminal or

terrorist behavior and defend the communities they serve by gathering and evaluating information about suspicious actions. The SAR system's capacity to detect possible hazards before they develop into more major situations is one of its main advantages. Law enforcement authorities may take proactive measures to stop criminal or terrorist conduct before it happens by gathering and evaluating information about suspicious actions. The abuse of SAR data, particularly the possibility of racial or religious profiling, is a worry as well. To solve these issues, law enforcement organizations must make sure that all SAR data is gathered and utilized in a morally and legally correct way and that the proper privacy safeguards are in place to protect people's rights.

REFERENCES

[1] D. Chaikin, "Commercial corruption and money laundering: a preliminary analysis," *J. Financ. Crime*, 2008, doi: 10.1108/13590790810882865.

[2] T. Nitin, S. R. Singh, and P. G. Singh, "Intrusion Detection and Prevention System (IDPS) Technology-Network Behavior Analysis System (NBAS)," *ISCA J. Eng. Sci.*, 2012.

[3] B. Santangelo and M. A. Jacobs, "Ask not for whom the bell tolls, it may toll for you next: intensified anti□money□laundering enforcement transforms the regulatory landscape," *J. Invest. Compliance*, 2005, doi: 10.1108/15285810510634650.

[4] N. Rébé, "Existing Compliance Measures to Prevent Terrorism Financing," in *Counter-Terrorism Financing*, 2019. doi: 10.1163/9789004409675_006.

[5] E. Bizuneh *et al.*, "Report of the International Leprosy Association technical forum: Paris, France 22-28 February 2002," 2002.

[6] E. Bizuneh *et al.*, "Report of the International Leprosy Association Technical Forum: 25-28 February 2002, Paris, France," *Lepr. Rev.*, 2002.

[7] ILA, "Report of the International Leprosy Association Technical Forum. Paris, France, 22-28 February 2002 -The Diagnosis and Classification of Leprosy," *Int.J.Lepr.Other Mycobact.Dis.*, 2002.

CHAPTER 21

REQUIREMENTS AND STRATEGIC PRIORITIES

Prof. (Dr.) Mita Poddar, Professor
Seedling School of Law & Governance, Jaipur National University, Jaipur, India
Email id- hod.law@jnujaipur.ac.in

ABSTRACT:

Requirements and strategic priorities are essential elements of the intelligence process. Requirements refer to the information needed to support operational and strategic objectives, while strategic priorities refer to the overarching goals and objectives of an organization or agency. To effectively manage requirements and strategic priorities, it is essential to establish a clear understanding of the information needed to support operational and strategic decision-making. This may involve conducting a comprehensive analysis of existing information, as well as identifying gaps in knowledge and areas where additional information is needed.

KEYWORDS:

Strategic Priorities, Priorities, Strategy, Planning.

INTRODUCTION

The purpose of the unit or fusion center should guide intelligence efforts; for instance, a High Intensity Drug Trafficking Area intelligence center's mission would be to concentrate on the manufacture and distribution of illicit substances. Similar to this, the Immigration and Customs Enforcement division of the DHS focuses its intelligence efforts on smuggling people and illegal goods over American borders. However, the majority of state, municipal, and tribal intelligence operations now take a "crimes, threats, hazards" stance. Actually, using all crimes for information gathering is a bit of a misnomer. Practically speaking, even an all-crimes intelligence operation must prioritize the forms of crime that will be the focus of intelligence operations since this involves such a broad range of crime types. This priority, as mentioned in the six discussions of strategic priorities, will be determined by geography, the criminal history of the area, and unique issues that facilitate threats from organized crime and terrorism, such as the presence of seaports, international airports, or special commercial industries, such as critical infrastructure or key resources [1], [2].

Mission-related needs for intelligence are also necessary. The goal of what are known as priority intelligence needs is to keep the emphasis on threats and crimes that have been determined to have the greatest potential to cause concern in the jurisdiction. However, we are aware that dangers and offenses evolve with time. Drug use, for instance, sees periodic shifts in patterns throughout the nation's various regions. Methamphetamines are a serious issue in certain

locations, whereas crack cocaine use may be a problem in others. In both situations, the main drug issue will develop. Due to these shifts in criminal issues, reevaluating intelligence targets should be a part of both strategic intelligence analysis and the reevaluation component of the intelligence process.

Different types of requirements

There are several methods to characterize intelligence needs, thus there isn't one set way to categorize the various kinds of requirements that law enforcement organizations utilize. The goal of this discussion is to explain and show the links between the many models and terminologies that are now in use.Depending on their function, requirements may be described in many ways. These many categorizations do not conflict with one another. There is a connection between the various kinds, with the various characterizations basically pertaining to their goals, as seen in the Venn diagram of 103.

For the goal of understanding various aspects of a threat, the intelligence unit or fusion center defines functional requirements. To assist the analyst in comprehending the functional development of threats, information is gathered via SARs and the collection plan linked with active enquiries. This is often a systematic process in which, as new data is gathered and processed, a clearer picture of the danger develops, which in turn aids in the definition of new needs. This iterative procedure keeps improving the danger picture until the threat is neutralized or disappears.

Four different categories of functional needs exist:

Analyst explained. The intelligence analyst finds a hole in the data over the course of the analysis that must be filled in order to complete a thorough and correct analysis. Three SARs belonging to an analyst point to a link between the three as potential criminal preparation. The information required to verify this connection is included in the intelligence needs. Defining a threat. dangers inside the jurisdiction that are regularly monitored in order to gauge the threat. For instance, keeping an eye on a known white supremacist organization that has issued criminal threats and learning about changes to its leadership, membership, and/or operations might assist spot impending dangers. Targets are watched to determine their susceptibility and risk based on the characteristics of known threats. In a brand-new community that it claims is located in an ecologically sensitive location, the Earth Liberation Front has threatened to burn down homes and destroy construction tools. The needs would be to gather data on the targets' susceptibility for a threat assessment.

Event or incident specified. In the event that an incident or scheduled event takes place, requirements will be established in order to identify any possible dangers connected to the incident or planned event. For instance, there is a good chance that anarchists will show up to the graduation if the president of the World Bank is asked to deliver the commencement speech at a nearby institution. While some anarchists may peacefully protest, others are more prone to damage property and cause trouble. The fact that the incident was planned led to the need for intelligence. To allow a knowledge of all aspects of a threat, there are important information demands for each sort of functional need. Both homeland security/all-hazards intelligence and law enforcement must comply with threat standards. These information requirements, as their name suggests, aid analysts in precisely defining threats. The analyst requires a broad range of accurate information from dependable sources that can provide as much insight as possible about

the danger picture, regardless of whether the threat is coming from a terrorist organization or from a pandemic disease. The term "methodological requirements" refers to the process used to get the information. In general, there are two kinds:

1. Ongoing information collection is necessary to track risks that are continuously and formally present within a community.
2. Case specifications. Information that analysts require to assess the presence and nature of a threat based on unauthorized tips, leads, reports of suspicious activities, and/or other information gathered throughout the intelligence gathering process.

Another aspect of requirements is determined by the sort of analysis that intelligence consumers seek; for instance, a partner agency in a fusion center may ask for a certain type of analysis for its region. Therefore, the requirements process will be led by this request. These are the many kinds of demands:

1. Tactical. What data is required to neutralize or avert an immediate or short-term threat?
2. Operational. What information is required to stop or lessen a long-term or emerging threat?
3. Strategic. What potential changes in the threat environment may affect operational planning and resource allocation in the next months or years?

Law enforcement-specific criteria, or legal requirements, overlap these in a special way. Remember that the only legal basis for law enforcement organizations to perform an intelligence function is their obligation to uphold the law. As a consequence, every data must be conceptually seen as having the potential to lead to a criminal investigation or prosecution. The burden of proof in a trial must thus be established, therefore information is required at the very least to help establish the criminal predicate. It will be necessary to identify requirements that contribute to establishing the corpus deletion or the components of a particular crime in relation to the intelligence targets [3]–[5].

DISCUSSION

Requirements and Criminal Evidence

Due to the fact that this problem is exclusive to law enforcement intelligence, it deserves further consideration. Requirements are information that the national security intelligence community uses to influence decision-making on threat prevention and policy. Development and tactical reactions. However, although many of these similar needs are met in law enforcement intelligence, there is the additional dimension that information gathered from requirements may also be utilized as criminal evidence. In addition to ensuring that information gathered throughout the requirements process complies with the rules of criminal procedure, intelligence requirements for a law enforcement agency must also take into account the civil rights obligations that law enforcement agents must maintain.

Law enforcement may find this to be a difficult procedure since there is always a balancing act. Information gathered on a person may sometimes need to be weighed against any danger to the public's safety and recorded accordingly. In other situations, the cops may be investigating a SAR to confirm the validity of the tip and establish both a criminal motive and a danger level. There are various situations when judgments must be made concerning information gathering

and storage that are fraught with risk. Using a circumspect viewpoint, the following key principles should assist direct the information gathering procedure for legal requirements:

1. Observe the rules governing criminal process and evidence.
2. Always act in good faith based on recorded justification and evidence, which is the foundation for information gathering and storage.
3. If there is a danger to community safety, you should record the supporting facts and arguments and, to the degree you can, confirm them.

Decisions must be based on facts, and the more accurate and thorough the information, the more solid the choice. In a similar vein, knowledge that provides a precise solution is more beneficial than generic information. A choice to adopt a new program requires an executive to consider both the easier aspect of what benefits would be lost if the program is not executed, as well as the particular costs, advantages, and dangers of the program. Typically, the knowledge sought is based on probability, experience of others, experimentation, reasoning, or, sometimes, an informed estimate rather than being definitive. The decision-making process becomes more challenging and risky when there is insufficient accurate information.

The operational setting for criminal intelligence follows the same procedure. Information for a thorough study is required in order to properly evaluate the hazards posed by a terrorist organization or criminal business. Critical information is often absent throughout the analytical process, preventing a thorough and correct evaluation of the problem. In order to address concerns about criminal or terrorist threats, the collection process concentrates on gathering the precise information specified in the requirement.17 The fulfillment of the intelligence requirement provides crucial information for making strategic or operational decisions regarding how to respond to the threat [6]. The goal of this conversation was to provide some insight on the needs for law enforcement intelligence in terms of intelligence requirements. The next stage is to start gathering the information after those requirements have been established.

Collection

Information requirements for ILP and the intelligence process have been examined in relation to information gathering. By taking a wider view of the data, the following topic expands on the last one. Information that is brought into the intelligence process for analysis is referred to as collection. It is the creation of raw data, and as will be shown, information gathering by law enforcement agencies is not always done in a direct manner.

Basically, there are three ways that information might enter the intelligence process:

1. It is purposefully looked for and gathered a task collection.
2. It is gathered as a part of regular collection, another law enforcement action.
3. It is provided voluntarily to law enforcement.

In response to intelligence needs, tasked collection is normally carried out as a consequence of a collection plan, which is characterized as follows:

1. A strategy for collecting data from all accessible sources in order to fulfill an intelligence demand. Specifically, a rational strategy for converting the key information into orders or requests to sources in the needed amount of time.

2. An analyst will generally design the collection strategy, as was previously mentioned in paragraph 6 to identify what categories of information are required, where the information may be located, and how it will be obtained.

How the data will be collected and how it will be acquired. The analyst will have a variety of alternatives, including open sources, limited databases,conducting interviews, and more. The question, "Where might I find this information and how will I get it? " is the key.The collection strategy serves as a guide for addressing this query. In certain circumstances, operational forces will be required for support. In these situations, intelligence professionals should cooperate with operational managers or supervisors to describe the information that is required, the rationale behind the need, and the function of the operational units in gathering the information. A basic explanation of the "why" can aid in securing collaboration and commitment, even in situations when the "why" must remain private.

Explicit explanations of the kinds of information required should be given when operational units help in collecting. In a similar vein, deadlines for when the information is required should be set. Precautions, if any, throughout the gathering procedure should also be communicated to operational units. In certain situations, measures may be taken to ensure the safety of the officers; in other situations, the precaution may be to gather the information subtly so as not to draw attention to itself. Effective communication between intelligence and operational staff is obviously crucial.

The second technique, referred to as routine collection, involves gathering data as part of ordinary operations and law enforcement activities. It focuses on ongoing intelligence needs or other matters of intelligence importance that are well-known and need for a steady stream of raw data. Normally, information gathered in this manner is filed as an information or intelligence report, but it may also be documented elsewhere, including information from or included inside the following:

Crime statistics

Criminal investigations, including standalone operational databases and case management systems that are proactive or reactive:

1. Firearms licensing to track patterns and identify known offenders
2. Meetings and events related to community and partnerships
3. Records of custody.

The types of routine collecting are many. As an example, the intelligence commander in one state has instructed the Open-Source Center to send him or her an email anytime any kind of material mentioning his or her state is put into the OSC. As a result, the commander now frequently gets an email regarding the entry. From the standpoint of criminal intelligence, the material would often be of little or no use, but when it is useful, it may have gone unnoticed if not for regular collecting.

The general public, local connections, and business partners provide law enforcement with information that has been voluntarily provided. The need for intelligence is the main driver of its acquisition. Depending on the kind of information acquired, information is often documented and filed on a SAR or another type of information report.

Information Gathering from Correctional Institutions

In the course of data gathering, correctional institutions are often disregarded sources of information. In order to identify dangers that exist in prison facilities, prisons departments are increasingly establishing and deploying Security Intelligence Threat Groups, a technique focused on intelligence for information gathering and analysis. Contrary to popular belief, many prisoners have close ties to criminal organizations outside of prison. There is a ton of data showing that gangs, drug dealers, and extreme ideological organizations all have contacts huge the outside world, tend to be aware of the criminal organization's actions, and sometimes even have influence over them. Corrections organizations have a broader scope for information gathering and may be a valuable source of information for the intelligence process.

Corrections IT systems include a significant amount of unconventional information and intelligence. Corrections is really in a position that allows it to get information that other law enforcement agencies are unable to. A framework for social networking can be developed by law enforcement and homeland security personnel to better understand the synergistic relationship between the criminal enterprise and the terrorist network that threatens our nation. Information like inmate visitor data, criminal associate data, and telephone record data are just a few examples of the intelligence sources that have the potential to offer useful insight.

The kinds of data that correctional organizations may gather and keep are quite important. Although using the information to combat gangs has often proven beneficial, such programs need to be expanded. The Corrections/Law Enforcement Intelligence Gathering and Sharing Project22 was formed by the National Institute of Justice as a way to improve threat detection. Monitoring initiatives like these may be valuable for fostering information sharing in addition to collaborating with prison organizations in a law enforcement agency's territory. It's crucial to keep in mind that there is a separate standard for material obtained for use in a criminal intelligence records system, regardless of the technique utilized to get the informationbetween data that includes no identifying information and data that identifies people or organizations.

Analysis

Without analysis, intelligence does not exist. According to the kind of data/information available and the sort of analysis being conducted, several methodologies and analytical tools are employed for intelligence analysis rather than a single methodology.This discussion's goal is to educate the analyst's audience about the process rather than to impart analytical techniques. The end-user should become a better-informed consumer as a result of these insights. A law enforcement officer will also have greater insights while reacting to intelligence needs if they have a better knowledge of analysis.One of the most important steps in the intelligence process is intelligence analysis, which is often described as a unidimensional activity. A closer look at the analysis function reveals that it is a process that calls for three major skill sets. As a result, the acquisition of information, talents, and skills must be in line with these skill sets.

Research is the first talent, and it entails gathering various types of information and evaluating their worth, relevance, and materiality to the evaluation. Collection differs somewhat from research. Gaining knowledge via research entails discovering details and viewpoints on a topic of interest. Examples include looking up anarchists' blogs on the internet to learn more about their beliefs and line of reasoning; reviewing studies on the traits and methods used in human smuggling; reading reports and articles on a particular topic, like the personality traits of

someone planning a suicide attack; or any other kind of data collection that offers insight—as opposed to evidence—about a specific topic. Research and collecting might certainly overlap, but rather than being redundant, their duties are more complimentary. Methodologies for both research and evaluation must be included in analysts' KSAs. Both open source material and information that is only available to law enforcement must be familiar with and accessible to the analyst. Although information will be gathered from a variety of sources other than the analyst, research skills are still necessary in order to go further into the material.

The intelligence analyst has to be more than just a conduit for data. The analyst must be proactive in two ways: the first is to specify and communicate the intelligence needs to close information gaps and provide a more thorough and reliable analysis of a danger, a person, or a target. The second strategy is to gather data from various sources. The analyst must actively look for the information, regardless of whether it is available from a data bank, fusion center, a commercial partner, or an investigator. As a consequence of the post-9/11 intelligence reengineering, information-sharing systems and techniques have substantially grown.

All necessary information may be guaranteed to arrive at the analyst's desk thanks to a system or procedure. Redundancy will be added to the collection process by the analyst's proactive efforts to make sure it is as thorough as feasible. The Law Enforcement Analytic Standard #11-Collection Follow-Up Standard supports this:

1. Analysts must assess the collection process while it is being carried out by investigators and others to see whether the needs of the collection plan are being satisfied. They must also find new sources of information.
2. As well as recognize data that might be advantageous to other situations or activities. Analysts must, wherever feasible, forward the information to the appropriate organization for further action.
3. The Method of Analysis
4. Policies and procedures must provide analysts the power to look for the information they need and include some kind of accountability mechanism to make sure the information is being supplied. Because the intelligence analyst is sometimes seen as having a lesser professional stature than a sworn officer in many law enforcement agencies, it may occasionally be difficult for analysts to provide guidance to investigators.

Although this organizational culture artifact is gradually evolving as analysts are seen as practicing professionals more and more, this viewpoint still exists. In order to guarantee that analysts have the organizational authority to get the information they want, it is crucial for the intelligence process to do this. The scientific method of issue resolution is basically what analysis, the second skill set, entails. It is predicated on both inductive and deductive reasoning, a fair evaluation of the available data, objectivity in the interpretation of the facts, hypothesis testing, critical thought, and evidence-based decision making. Astrophysicist Carl Sagan, who is now deceased, provided this explanation of how science works:

More than any other collection of information, science is a method of thinking. Its objective is to learn how the world functions, to look for any patterns that may exist, and to delve into the connections between things, starting with subatomic particles and moving on to living creatures, the human social community, and ultimately the universe as a whole. Our intuition is not always a reliable source of information. Science is built on experimentation, on a willingness to question conventional wisdom, and on an openness to seeing the cosmos as it really is. Our perceptions

may be affected by training and bias or simply due to the limits of our sense organs. As a result, bravery is necessary for science at the very least, the willingness to challenge received knowledge. A scientific mindset involves critically analyzing the reality and considering the possibility that many other possible universes exist. You will be conducting science if you spend any time spinning ideas, determining if they make sense, whether they are consistent with what is already known, and considering tests you may use to support or refute your hypotheses.

In order to extract meaning from a complex collection of information, intelligence analysts basically follow the procedure Sagan describes. Science, according to Sagan, is to ascertain "...what regularities there may be." Because these patterns in criminal behavior are crucial for predicting crime and choosing preventative tactics, law enforcement works to understand the modus operandi of criminals. Law enforcement intelligence analysts look for connections between criminal conspirators, between various sorts of evidence, and between illegal transactions, much as Sagan said that science attempts "to penetrate to the connection of things."

Analyzing intelligence is a cerebral activity with real-world uses. It is not something that most people find simple. Structure, critical thinking, self-discipline, and a deep understanding of the objective are all necessary. "Structure" refers to the capacity for organization, the observance of standard analytical procedures without cutting corners, and the assurance that all relevant data and supporting evidence are included into the study. "Critical thinking" refers to the analyst's adherence to logical, as opposed to intuitive, reasoning. Additionally, it implies that the analyst will reach conclusions based on actual facts rather than presumptive evidence. For the analyst to stay impartial and resist being swayed by emotion or other circumstances, "self discipline" is crucial. This impartiality also implies that the "weight" of the evidence is taken into account. The analyst must possess "substantive knowledge" about the intended crime in addition to possessing analytical KSAs. The analyst must comprehend the lingo, ideologies, and workings of the criminal business whether the target is a Jihadist network, a drug cartel, or a money laundering network.

The substantive knowledge required for efficient analysis may be developed via training, programs, continuing education, and self-directed education; however, it is more difficult to combine thinking abilities with substantive information. The methods and methods of analysis may be taught, but the best way to develop critical thinking is via "mental calisthenics" and experience. A sequence of written exercises or puzzles that force a person to come up with a solution are referred to as mental calisthenics. Finding the best or most likely option from among several possible ones is the next difficult task. This method is widely used in problem-based learning, a technique that centers the curriculum on a single issue. The analytic skill set is the most challenging to successfully train in an analyst and is also the most crucial. The inquiry may require the learner to either solve an issue or make a choice [7], [8].

Reporting is the third group of abilities. There are phases in the analysis process when decision-makers and investigators must be informed of the results.The reporting process converts analytical results into illustrative status reports or useful information. A descriptive status report basically outlines an intelligence target's personality, method, likely outcomes, and likely future actions. The report could include cover presently available evidence, intelligence needs, and mysterious events connected to crime that need further investigation. These reports are often made to help with planning and directing an investigation, assigning resources, determining the risk to prospective victims, learning more about threat times, preparing for action, and

developing mitigation methods. In the reporting process of modern intelligence, the analyst creates "intelligence products."

A law enforcement agency has the necessary knowledge to create an operational response to threats when it possesses actionable intelligence. Three elements within this approach support efficient analysis:

1. The general quality of the information a choice was based on. Information accuracy is crucial. When information is examined, conclusions are reached using the analyst's knowledge of the available facts. The accuracy of the analysis will naturally suffer if the data is incomplete or skewed.
2. A larger body of data to strengthen the information's comprehensiveness and bolster other facts. The analysis becomes more precise with an increase in the quantity of high-quality data. Raw as volume rises, information is refined and analysis quality improves. The important thing is to make sure that the information is correct and relevant in quantity, which is a crucial aspect of the fusion process.
3. Increased information specificity. The possibility of recognizing small threats is higher when the raw data is more precise.

CONCLUSION

Overall, the effectiveness of intelligence operations depends on the efficient management of needs and strategic priorities. Organizations may make sure they can gather and analyze the data required to support operational and strategic decision-making and, ultimately, accomplish their goals and objectives by creating explicit needs and prioritizing strategic objectives. The creation of efficient feedback mechanisms and the installation of transparent communication channels are also necessary for the proper management of needs and strategic priorities. This might include having formal reporting systems in place as well as holding frequent meetings and stakeholder engagements. Making sure information is gathered and evaluated quickly and effectively is one of the main problems in managing needs and strategic goals. This necessitates the creation of a strong data management system, as well as the deployment of efficient data collecting and analysis technologies.

REFERENCES

[1] A. Sobczak and D. M. Berry, “Distributed priority ranking of strategic preliminary requirements for management information systems in economic organizations,” *Inf. Softw. Technol.*, 2007, doi: 10.1016/j.infsof.2006.10.006.

[2] M. Lehto and J. Limnéll, “Strategic leadership in cyber security, case Finland,” *Inf. Secur. J.*, 2021, doi: 10.1080/19393555.2020.1813851.

[3] A. B. Raidén, A. R. J. Dainty, and R. H. Neale, “Balancing employee needs, project requirements and organisational priorities in team deployment,” *Constr. Manag. Econ.*, 2006, doi: 10.1080/01446190600647191.

[4] C. Morciano, M. C. Errico, C. Faralli, and L. Minghetti, “An analysis of the strategic plan development processes of major public organisations funding health research in nine high-income countries worldwide,” *Heal. Res. Policy Syst.*, 2020, doi: 10.1186/s12961-020-00620-x.

[5] A. Tursunbayeva, S. Di Lauro, and C. Pagliari, "People analytics—A scoping review of conceptual boundaries and value propositions," *International Journal of Information Management*. 2018. doi: 10.1016/j.ijinfomgt.2018.08.002.

[6] Y. Lin, J. Luo, L. Zhou, S. Ma, and Z. Zhou, "Servitization strategy: Strategic priority, capacity requirement, and organizational feature," in *Proceedings of 2011 IEEE International Conference on Service Operations, Logistics and Informatics, SOLI 2011*, 2011. doi: 10.1109/SOLI.2011.5986554.

[7] O. Luca, F. Gaman, and E. Răuță, "Towards a national harmonized framework for urban plans and strategies in Romania," *Sustain.*, 2021, doi: 10.3390/su13041930.

[8] T. Kamal, Q. Zhang, M. A. Akbar, M. Shafiq, A. Gumaei, and A. Alsanad, "Identification and Prioritization of Agile Requirements Change Management Success Factors in the Domain of Global Software Development," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2976723.

CHAPTER 22

INTELLIGENCE OUTPUTS AND PRODUCTS AND QUALITY OF THE INFORMATION

Ms. Kriti Sanadhya, Assistant Professor
Seedling School of Law & Governance, Jaipur National University, Jaipur, India
Email id- kriti.sanadhya@jnujaipur.ac.in

ABSTRACT:

Intelligence outputs and products refer to the results of the intelligence cycle, which involves the collection, analysis, and dissemination of information to support law enforcement and public safety objectives. These outputs and products are designed to provide actionable intelligence that can be used to inform operational and investigative decision-making. Intelligence products can take many forms, including briefings, reports, alerts, and assessments. These products may be tailored to specific operational or investigative needs, and may include information on a range of topics, including criminal activity, terrorist threats, and public safety risks.

KEYWORDS:

Intelligence, Information, Outputs, Products, Quality.

INTRODUCTION

The analysis gains more worth. The nature of the raw data is essential to producing effective analysis, regardless of the expertise of the analyst or the analytical tools at hand.

Tools for Analysis

The intelligence analyst may use a variety of analytical tools. In essence, "tools" refers to methodological approaches that aid in the organization, integration, comparison, correlation, and illustration of a body of unprocessed data. Each analyst tool offers a piece of fresh knowledge—or at least new insight about the data that, taken together, contributes to the analysis and/or leads to the development of new intelligence needs. None of the analyst tools will alone create actionable intelligence [1]–[3].

The actual analysis depends on the analyst's capacity for critical thought and integration of the results of these many approaches into a coherent, actionable intelligence product. These outputs from analytical tools may be used in these products to display complicated linkages, such as a link analysis chart that shows the relationships and hierarchy of those participating in a criminal operation or an illegal commodity flow chart.

Even if the intelligence consumer does not necessarily need to know how to conduct these various sorts of studies, it is nevertheless beneficial to be aware of the many analytical tools that are available and the kinds of data they may provide. Although not a complete list, the most

typical tools26 that an intelligence consumer would run across are as followsflow of activity. The stages a criminal organization utilizes, the activity flow is similar to a modus operandi or mode of operation and specifies specific occurrences, dates, and a description of the activities that transpired. In order to better comprehend the development of the company, the episodes are connected in a flow chart.

The activity flow assembles a sophisticated criminal business and may be used to intervene in the enterprise and identify any holes. If gaps are found, intelligence needs will be employed to fill them so that the enterprise's activities can be completely mapped to help with prosecution and prevention.Matrix of associations. In order to identify the correlating factors that are crucial to the operations of the criminal enterprise and to eliminate those that do not, this matrix attempts to correlate two or more factors in a criminal enterprise by recording the frequency with which certain factors occur at the same time. Similar considerations may include associating a list of phone numbers, for example. The variables may sometimes be fundamentally unrelated but nevertheless provide information when they are connected, as in the case of comparing the travel habits of two intelligence targets when a phone conversation or financial transaction occurs first.

Commodity flow and visual forensic analysis. a visual representation of the transactions involved in the transfer of an illegal product via a criminal business. For instance, the flow of Afghan heroin from Afghanistan to a city in Middle America would display each transaction and method of smuggling, as well as the associated expenditures. Analysis of communication flow. An examination of phone, text message, and email traffic may provide significant information. An analysis may provide important corroboration and proof of wrongdoing by identifying the parties with whom intelligence targets are speaking, the frequency of the communications, their origins and destinations, the duration of the communications, and if there were attachments to e-mails. An examination of communications traffic may be useful in addition to the substance of conversations, which will undoubtedly include relevant information.

Criminal behavior analysis. a broad phrase covering a variety of related disciplines, including mapping, the identification of crime or event series, crime trend analysis, hot spot analysis, and general profile analysis.Business profiles of criminals. Similar to how a regular firm would be discussed, such profiles provide in-depth studies of how criminal activities or strategies function. Examination of social and demographic trends. an analytical approach that focused on shifting demographics and how they affected crime. Additionally, it examines socioeconomic issues including homelessness and unemployment, as well as demographic changes, societal views, and activities that may have an impact on crime.Analysis of event flows. Charts that show a sequence of significant events or incidents and their link to one another, such as a criminal participant's travel, financial transactions, or other crucial events in the facilitation of the crime.

The goal of various financial analysis approaches is to connect various financial transactions, taking into account factors like the kind of transaction, the persons involved, the origin, intermediary, and destination of the transaction, as well as a comparative comparison of revenue and expenses. The goal is to track the patterns of transactions with intelligence targets and spot anomalies or suspect financial activity. Financial analysis is a crucial technique since almost all crimes involve money in some way.The analyst will form an assumption on the connections between individuals and groups involved in the criminal enterprise, the transactions required for the enterprise to function, and the essential goods or resources required for the business to succeed. Hypothesis testing uses the ions to determine whether all the elements in the enterprise

have been identified that can be used to stop the enterprise from continuing and, ideally, determining the criminal liability of participants, in contrast to the previous items on this list, which are visual ions of various elements of the enterprise.

Link Evaluation. a diagram showing the affiliations between each of the organizations and all of the proven and suspected participants in the criminal activity.consumer profiles. The profiles are evaluations of the criminal market around a certain product or service, such prostitution or the sale of stolen goods, in a given location. They are updated and evaluated often.network examination. In addition to outlining the connections that people make to build criminal networks, this research also discusses the relevance of those connections, the roles that people play, and the advantages and disadvantages of a criminal organization.appraisal of operational intelligence. In the event of a sizable intelligence gathering plan or other large-scale operation, such an evaluation assesses incoming information to keep the focus of an operation on previously established goals.

Results evaluation. An evaluation of the efficiency of law enforcement efforts, such as the efficiency of patrol tactics, crime-reduction programs, or a specific investigative strategy.risk assessment. an evaluation of the dangers that certain criminals or groups provide to specific prospective victims, the wider public, and law enforcement authorities. Analysis of the target profile. a description of criminals, their criminal activities, lifestyle, affiliations, the danger they provide, and their strengths and weaknesses in order to concentrate the inquiry that is aimed at them. Profiles may also put a special emphasis on victims and weak people.

DISCUSSION

Predictive Analysis

A quick explanation of the notion may be helpful to the consumer of information since predictive analysis is becoming more and more common as a method for intelligence analysis. The business sector, where econometric models are employed to anticipate market developments, is where predictive analysis has mostly drawn from. A manufacturing firm may change its production, workforce size, and supply chain by analyzing economic factors in the current market, supported by analysis of known trend data (such as changes in a sector's economics during different times of the year), to enable it to continue professional operations while meeting supply demands under a variety of circumstances. In such case, the study offers management and operations strategic guidance for choosing between various futures that will enable them to prevent needless financial losses while still providing a high level of customer service.

Does the predominantly qualitative field of law enforcement intelligence analysis allow for the successful use of such a quantitative approach? Although predictive analysis has significant uses in intelligence analysis, it does not provide as rigorous an analysis as more quantitative domains with longer cycles of predic change, such the economic world. Despite this, it has significant applications in intelligence. However, these applications will need a wide-ranging and sometimes labor-intensive research effort, a diversified analytic approach, and an expanded reporting system that delivers varying results dependent on the development of social and political trends. The intelligence analyst may keep track of these patterns over time to improve the status and threat implications of the ones being seen.

A rational prediction of danger characteristics is produced using predictive analysis, a critical-thinking process that incorporates known quantitative and qualitative elements, such as occurrences, events, political, and social dynamics. The term "predictive" is deceptive in many respects since it is almost difficult to accurately forecast occurrences that are dependent on human behavior and the many factors that might affect that behavior. The procedure is a probabilistic analytical exercise that accumulates a variety of data, continuously tracks data changes, and adjusts the prediction in light of the fresh inputs. Predictive analysis is iterative, always seeking fresh inputs of data to improve the prediction, much like the intelligence process itself.

Predictive analysis' iterative nature is a complement to requirements-driven intelligence. This method continually looks for information to fill any intelligence blanks or gaps in our understanding of threats, and then finds, gathers, and analyzes data to fill those voids. In order to create the most complete knowledge base possible, intelligence requirements the information needed to fill a gap provide continuous input into the intelligence cycle. Although it may also be used to help define ongoing intelligence needs, predictive analysis in law enforcement can have the most influence on strategic intelligence. This analytical method won't predict dangers per se, but it can predict environmental changes that can modify factors that lead to risks.

Critical Parameters for Threat Analysis

The capacity to gather data on a number of important factors connected to the intelligence target is crucial to analytical procedures that aim to help us comprehend any kind of danger. Again, each aspect significantly affects the kind of intelligence that is needed.Intent. What is the intelligence target's declared purpose? Has it altered? How may any recent acts or occurrences affect the target's stated intentions?

History: What actions or historical behavior does the intelligence target or group have? History often sheds light on potential future actions, strategies, and objectives. This entails locating and evaluating incidents that led up to earlier assaults or violent tendencies shown by the intelligence target.Capability. What competencies does the organization or the target possess? Have they received training to carry out terrorist or criminal acts? Do they have the necessary personnel, equipment, funds, documentation, and means of transportation to carry out the crime?

Opportunity: Any uncommon or special possibilities that might aid in an assault are they arising? If so, what type of access will the intelligence target have to that opportunity? Are there any indications that an assault or crime was planned to take place when a chance arose?Resolve. Does the intended intelligence target or group genuinely intend to carry out the attack? Does the intelligence target genuinely constitute a danger, or is it just a threat on their part? Exist any suggestions for thwarting the desire to launch an attack? Learning the traits of the leader is a crucial factor associated to "resolve," especially in the case of ideological groupings. The possibility that the group will carry out its goal rises if the leader is charismatic.

Threat assessments are inextricably linked to the needs for and analysis of intelligence. The relationships are systemic, so any changes to one will have an impact on the others.The complicated work of intelligence analysis is the inspection and evaluation of data in order to make judgments on a certain subject. Due to the absence of philosophical ideas, it is not an intellectual activity. As a substitute, intelligence analysis is a task that significantly relies on reality and necessitates an unbiased way of thinking. It is mostly process-driven and calls for

ongoing, in-depth study utilizing data from both classified and non-classified sources. Information must be gathered for analysis in order to find connections, reveal trends, and separate fact from opinion. This procedure compels the questioning of data in order to validate facts and possibilities. The information will then be scrutinized to identify tendencies that would eventually result in an event or pattern. After drawing a conclusion from the data, an evaluation is created and provided to consumers so they may base their choices on our results in an educated manner.Because analysis offers the intelligence that characterizes criminal dangers and the options to control those threats, analysis is a crucial component of information management. Intelligence products must be used to convey this knowledge.

Products and Outputs of Intelligence

The result of analysis, or intelligence, must be presented in a reporting format that facilitates the most effective consumption and use of the data. The intelligence product is what is being discussed here. In Integrated Intelligence and Crime Analysis, Ratcliffe made the following observation about the relationship between analysis and products: criminal intelligence is the production of an intelligence knowledge product that supports decision-making in the fields of law enforcement, crime reduction, and crime prevention. An intelligence knowledge product is one that may affect a decision-maker's thinking in this setting. It is the outcome of a criminal intelligence study and may be presented orally, in writing, in a briefing, or in any mix of these. If the insight is timely and affects the recipient's decision-making, it might even be the result of a quick telephone discussion.

Typically, many product varieties are created to satisfy the requirements of various customers and analyses. The output of a tactical analysis will be different from that of a strategic analysis. A product created to inform cops of criminal signs will be different from one created for a thorough evaluation of a particular criminal activity. A patrol briefing on a criminal danger is different from an executive briefing on the same concern. Whatever the product type, all should include these five essential components in the context of the product's intent:

1. Identify the information's intended audience.
2. Clearly communicate the vital facts the target customer needs to know.
3. Determine the time intervals during which the intelligence is usable.
4. If necessary, provide any extra intelligence needs.
5. In light of the study, provide operational advice.

Products should ideally consist of a number of consistently generated intelligence reports with a certain message and structure. They are most helpful when each item has a specified function, is presented consistently, clearly, and attractively, and contains just the essential information the customer needs. An intelligence unit or fusion center should typically produce at least three different kinds of products:

1. Products designed to fend against recognized hazards.
2. Threat alerts are products that show signs of threatening actions and threatened targets.
3. Products that detail changes in the threat profile from terrorism or crime to a territory.

While the majority of law enforcement personnel are quite acquainted with records and reports from investigations, they are less comfortable with intelligence products. There are no

distinctions that the customer has to be aware of. There will be more utilization of the items if the differentiation is understood clearly.

a. Law enforcement intelligence reports, records, and products Criminal Investigation Reports and Records
b. Prosecution is the main objective
c. A report is evidence of a criminal offense that had occurred.
d. Report is an official document that serves as evidence.
e. Motive is not a necessary component of the offence under the law.
f. The corpus delicti is recorded, and threat-based prevention is the main objective.
g. Report emphasizes alleged criminal threats
h. Report contains details related to a threat investigation.
i. Motive is a crucial forecasting tool.

In order to develop theories concerning criminal dangers, information is recorded.

In 10-4, two major divisions in law enforcement intelligence outputs are described. The first is "case intelligence," which has as a crucial feature the identification of specific people or groups. An important point to remember is that with case intelligence, civil rights attach to people who have been identified in any type of intelligence report. Conceptually, its ultimate goal is the arrest and prosecution of particularly-described persons as a means of preventing a threat from materializing. The second category, "intelligence advisory products," outlines common criminal activity and threat indicators that law enforcement personnel should be aware of. In order to preserve public safety and prevent a criminal occurrence from happening, it is important for law enforcement professionals to be aware of the signs and, if seen, to take necessary action. In general, there aren't any overt civil rights concerns with advisory goods until a person or group is recognized as being connected to the illegal indications.

Based on the administrative mandate of the unit, each intelligence unit or fusion center may identify the kinds of goods it needs to create. Some, like a transit law enforcement agency, are formed to address certain jurisdictional requirements. Law enforcement intelligence reports often fall into one of two basic typologies. The report's nature and the kind of analysis being done.

What Kind of Intelligence Report Is It?

In order to satisfy the requirements of various audiences, several types of intelligence reports are produced. An "Intelligence Alert" might be a quick report outlining the essentialinformation about people or signs connected to a time-sensitive danger. An "Intelligence Bulletin" may provide more thorough information on potential signs or risks that are not immediately present. In general, a "Intelligence Assessment" shows how a danger has evolved over time and from what historical viewpoint. There are currently no standard categories for intelligence reports across all agency types and governmental levels; rather, each agency or fusion center creates reports that often adhere to these broad standards. Training for law enforcement employees on the products utilized in their jurisdictions and the purpose of each report type is necessary.

The Type of Analysis

The fact that certain terms have distinct meanings for the military, federal law enforcement, and the intelligence community compared to state, local, and tribal law enforcement may be contributing to the confusion in the world of intelligence reporting. The latter is the topic of the

present conversation. Before, the distinctions between tactical analysis and strategic analysis were discussed from the viewpoint of law enforcement. Again, despite the fact that there are no consistent classifications of particular report types based on the types of analyses that were carried out, suffice it to say that intelligence users should be aware that some report outputs will describe threats requiring an operational response while other reports will describe changes in the threat landscape. There are or will be further report kinds. We are increasingly seeing new report types emerge that are based on technology and range from text messaging to Podcasts. Intelligence briefings are oral summaries of analyses that require yet another different approach to reporting and pay homage to the frequently repeated comment of Sgt. Joe Friday in the old television series Dragnet: "I want the facts, just the facts." Regardless of the reporting mechanism, it is critical that each report type provides the data required for the intended consumer to successfully carry out his or her duties.

Intelligence Products' Features

1. **Actionable:** The final result should have enough accurate information to allow for the creation of some kind of operational activity or reaction.
2. **Accurate:** Since the analytical process is often probabilistic, it is uncommon to get specific findings or projections. Although this is the case, every effort should be taken to be as precise as possible, with any shortcomings in the findings being made explicit.
3. **Objective:** Products of intelligence ought to be impartial. A balanced presentation of all the data is required, including the knowns, unknowns, strengths, and weaknesses of the study.
4. **Relevant:** Threats that are strategic priorities or emerging threats that potentially have a substantial impact on regional public safety should be the main focus of the study and the products.
5. **Timely:** There are two aspects to timeliness. First, the danger should be one that is currently causing worry in the intelligence product. Second, the product should be made accessible whenever possible so that operational units have as much time as possible to plan and implement a reaction.
6. **Comprehensive:** The intelligence output should provide as much details as feasible regarding the threat's many manifestations.

Avoid these Techniques When Using Intelligence Products

Some methods connected to intelligence products have evolved in the post-9/11 atmosphere, where the crucial term is "information sharing," but which really causes more issues than it solves. Information has to be "targeted," or shared with those who can utilize it in a productive way. Unfortunately, this adage has been disregarded far too often. Avoiding these three core habits can help you produce better intelligence products. You may refer to them as the "three don'ts of information sharing."

1. Avoid repackaging another organization's intelligence offerings. Since most agencies will already have the original product, repackaging it would be redundant and maybe misleading. If the same information is delivered under two distinct agency names while still being the same product, a repackaged product offers minimal value and could be deceptive. Furthermore, if a product from another agency is merely repackaged, the original agency won't be able to respond to questions for further information.

2. Avoid telling everyone everything. Both getting no information and receiving too much information might be unproductive. Personnel have a tendency to pay little attention to any information when they are bombarded with a cascade of information that is of little value to them. Separating the wheat from the chaff is the responsibility of the intelligence function, not the consumer. It is crucial to provide knowledge to those who need it.
3. Avoid adopting a "publish or perish" mentality. This could be a systematic issue. Managers want to know how productive intelligence analysts are, but it may be challenging to measure productivity in the intelligence department. The creation of intelligence products is one activity that can be readily counted, and some intelligence units and fusion centers have used "products" as a measure of effectiveness. Although it is apparent how this has changed, product publishing is not a solely reliable indicator of success. If the product isn't useful, it doesn't matter how "interesting" it is. The quality and usability of the items should be measured instead of their quantity. Of course, this is challenging and rather arbitrary. It might be challenging to conduct evaluations successfully.

Products for Intelligence Should Contain Products for Intelligence Should AvoidThose in charge of the intelligence function should respond positively to the following queries about intelligence products in order to prevent the issues represented in the "don'ts" of intelligence goods:

1. Operational and tactical intelligence. Does the intelligence product provide enough information about a danger in your region or service area to allow operational staff to create tactical plans or initiatives to thwart or lessen a threat identified?
2. Intelligence on strategy. Does the intelligence product provide enough information on the traits, operating principles, or changes in the threat environment as they pertain to your area or service area to allow for successful judgments to be made about strategic priorities and resource allocation?

Dissemination That Is Actionable. Who in your region or service area has a right to know and a need to know this information for threat prevention, mitigation, and/or planning, given the nature of the danger and the substance of the intelligence product? intelligence goods are how crucial danger information gets to the public. A crucial procedure is identifying the kind of goods that will benefit an intelligence unit's or fusion center's consumer the most and getting the correct product into the hands of those who need it [4]–[6].

CONCLUSION

In general, the effectiveness of law enforcement and public safety activities depends on the creation of efficient intelligence products. These solutions may aid in the identification and mitigation of possible threats and dangers as well as the safety and security of the communities they serve by providing actionable information to assist operational and investigative decision-making. Making sure that intelligence products are distributed to the right stakeholders in a timely and safe way is one of the biggest problems in generating intelligence products. To safeguard sensitive information from unwanted access, this may include the use of secure communication methods, such as encrypted messaging systems or secure databases. Unfortunately, when we observe events throughout the world with the false assumption that they won't touch us, it often leads to a provincial viewpoint that is not helpful. Just as global economic events have an impact on our communities, international terrorist and criminal activity events may have an impact on us locally. As a basic example, terrorism, war, financial markets,

and political unrest in OPEC will all have an impact on the prices we pay at our neighborhood gas stations. We must acknowledge that terrorism and criminal activity may have an influence on our communities via international planning, finance, and logistical assistance. Thus, local intelligence analysts must take into account the broader implications of international events, such as the Hezbollah-Israeli war, and how they might affect local and regional responses to people who support Islamic terrorism. If the analyst lacks this knowledge, there will be a need to close these intelligence gaps and use them locally.

REFERENCES

[1] J. Zhang and Z. Li, "Intelligent Tea-Picking System Based on Active Computer Vision and Internet of Things," *Secur. Commun. Networks*, 2021, doi: 10.1155/2021/5302783.

[2] M. Mohammed, A. Romli, R. Mohamed, and A. Noormazlinah, "Eco-Ontology for supporting Interoperability in Product Life Cycle within Product Sustainability," *IOP Conf. Ser. Mater. Sci. Eng.*, 2021, doi: 10.1088/1757-899x/1092/1/012049.

[3] D. P. Kalarani, "Empowering Artificial Intelligence and Cyber Security Challenges in Smart Manufacturing," *Turkish J. Comput. Math. Educ.*, 2021, doi: 10.17762/turcomat.v12i6.1280.

[4] C. Yongqiang, L. I. Shaofang, L. Hongmei, T. Pin, and C. Yilin, "Application of intelligent technology in animal husbandry and aquaculture industry," in *14th International Conference on Computer Science and Education, ICCSE 2019*, 2019. doi: 10.1109/ICCSE.2019.8845527.

[5] F. H. Galezan, M. R. Bayati, O. Safari, and A. Rohani, "Evaluating the Rearing condition of Rainbow Trout (Oncorhynchus Mykiss) Using Fuzzy Inference System," *Aquac. Eng.*, 2020, doi: 10.1016/j.aquaeng.2020.102051.

[6] S. Liu *et al.*, "Key technology trends analysis of TFT-LCD," *Chinese J. Liq. Cryst. Displays*, 2018, doi: 10.3788/YJYXS20183306.0457.

CHAPTER 23

OPEN-SOURCE INFORMATION AND INTELLIGENCE: A PERSPECTIVE FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT AGENCIES

Mr. Aaditya Arora, Assistant Professor
Seedling School of Law & Governance, Jaipur National University, Jaipur, India
Email id-aaditya.arora@jnujaipur.ac.in

ABSTRACT:

Open-source information and intelligence refer to the collection and analysis of publicly available information to support law enforcement and intelligence operations. With the proliferation of social media platforms and other digital technologies, open-source information has become an increasingly valuable source of intelligence for law enforcement agencies and other organizations. Open-source information can take many forms, including social media posts, news articles, blog posts, and other publicly available information. By leveraging advanced data analytics tools, law enforcement agencies can analyze this information to identify potential threats and risks, and to develop intelligence products that can inform operational and investigative decision-making.

KEYWORDS:

Agencies, Analysis, Information, Intelligence, Investigation, Law enforcement.

INTRODUCTION

Open sources of information have traditionally been devalued when it comes to the gathering of data for the intelligence process.Since there is such a wide variety of trustworthy, diversified material accessible for analysis, open-source information is often among the most valuable for intelligence. This is especially true given the rapid development of networking. A lot has been written on the use of open-source data in corporate intelligence and, to a greater and greater extent, in national security intelligence. The present debate will put open source use in the law enforcement community into context and highlight significant restrictions that may be placed on the preservation of certain categories of open source data [1], [2]. Technology development has significantly altered the nature of open-source knowledge. To put things in perspective, the Internet became the main place to go for all kinds of information as the public adopted the World Wide Web in great numbers starting in the mid- to late 1990s.

More information, including audio and video files, was being stored and processed as computer memory and processing rates grew. Faster, more discerning search software has been created as a result of the widespread use of wireless computing and the integration of computers into almost every area of everyday life. The variety and quantity of material offered has also risen from content producers. The convenience and utility of open-source information have been greatly enhanced by technical advancement as well as by the public's willingness to use it.

But there is a catch: More information does not always mean better information. Users of open sources must exercise caution by ensuring that the data gathered from them is reliable and accurate before using it to guide decisions. Without quality assurance, information is of little use. Making wise end-user judgments regarding which information should be saved and which information should be deleted is difficult, especially when one has access to vast volumes of information.

Getting to Know "Open Source"

A newfound interest has emerged in the idea of using open sources for information and intelligence, especially when it comes to law enforcement and the intelligence community. Perspective will be provided by a quick explanation of the idea and how it is used in the present situation.

DISCUSSION

Why Is there Value in Open-Source Information?

Because of the false belief that persons, movements, and situations that pose dangers would not have information that is accessible about their purpose, attributes, or behavior in the open, open-source information has often had a second-class standing in the intelligence community.

This presumption is false for six key reasons.

a. First, there are people who represent a danger due to their radical ideologies—even those who advocate violence to achieve their aims—and who normally wish to spread their views and goals in order to influence others to accept them. They often publish this material in print, online, on broadcast media that supports their cause, and via shortwave transmissions.
b. Second, thieves utilize the internet as a mostly anonymous tool to trade in illegal goods. Criminals may readily enter the U.S. market from abroad and use strategies to make them hard to find, both of which increase the allure.
c. Third, in some states, the custodian of certain types of information is allowed to make it publicly available due to policy, regulation, or law. For instance, public databases contain information about driver's licenses, property ownership, voter registration, sex offenders, salaries of public employees, and a wide range of other informa
d. Fourth, they favor the release of certain information. Numerous factors, including marketing, company names and addresses, research reports, phone numbers, and business addresses, might cause this. When information is studied collectively, a surprising amount of additional knowledge may be discovered in addition to the insights that can be acquired from the individual bits of information.
e. Fifth, non-law enforcement organizations like the media or advocacy groups may undertake investigations that end up in the public domain. To further the goals of their enterprise or cause, these sources could divulge private data, descriptions of conduct, intimate connections, activities of a certain group, and details of an occurrence.
f. Finally, information is often made public due to a person's negligence. Examples include a public figure using an open microphone to make an embarrassing remark or an individual posting damning details on a blog. In these situations, open sources often provide useful information that may be exploited in the intelligence gathering process.

Categories and Definitions

Any legally and morally attainable information that identifies people, activities, places, organizations, events, or trends is considered to be an open source of information. Open source data is simply defined as the following by the Office of the Director of National Intelligence:information that is legally accessible to the public and that anybody may legally request, buy, or observe.

Either of these definitions makes clear how wide-ranging the category of material that constitutes open source is. One benefit of open-source data for law enforcement is that it may be looked for and gathered without the need for a court order. Civil liberties concerns arise when open-source data is retained for intelligence purposes, as will be explained later. The primary distinction between open source and closed source data is that open-source data cannot be obtained via the use of illegal or unethical means. Although open-source data has essentially always existed, networking has greatly expanded its accessibility. A strategic intelligence report on patterns in global terrorism, for instance, could require an analyst to visit the

U.S. The Department of Homeland Security-funded terrorist database, the FBI terrorism reports website, the Israeli Defense Forces terrorism statistics center website, and the Department of State Counterterrorism Office website may all be used to obtain the different reports and data. If the analyst was writing a report on right-wing extremists, he or she might go to the Southern Poverty Law Center website to download reports or to a website for white supremacy like Stormfront website to read materials. The analyst would then conduct additional research by clicking on hyperlinks to obtain more raw data in order to write a report independently.

First Resort's Resource

More and more often, open sources are referred to be the source of last resort. This implies that as the initial stage in the information-collection process, analysts and information gatherers should use open sources of information. Open sources may provide significant insights that may give a line of investigation useful direction, especially when information gaps, whether tactical or strategic, are uncovered.

Unknown graffiti or a distinctive tattoo may be searched via image files. A blog search can provide unique insights about virtually any extremist group just as information may be obtained about a particular issue. Similarly, insightful information about Hezbollah31 can be found by conducting a blog search. If a particular crime trend emerges within a community, for example, an open-source search of newspapers nationwide can identify other locations where crimes with similar modus operandi have occurred.

Similarly, in order to better grasp the jihadist threat by efficiently mining the Internet and other open sources for information, it is important to be aware of the ideologies, vocabulary, reasoning, and views of jihadists. A greater tactical grasp of how jihadists utilize the web-television capabilities, chat rooms, and "news" sites to train troops and generate money is also allegedly possible as a result of such an initiative. In order to successfully combat the danger presented by jihadists, these commentators believe that the United Nations must have the capacity to comprehend and influence other communities — "not in their council of states but in their villages and slums." In such cases, it is said, open sources can provide policymakers with the data that should matter the most.

Open-source software has several advantages when used as a last option. Open sources may often provide an efficient, effective, and quick insight into a problem when a danger or issue first arises, which may frequently verify the necessity for additional investigation. Similar to other methods of generating context and perspective, open sources may provide a comprehensive picture of a person or danger. Furthermore, the intrinsic nature of many closed sources may frequently overlook linkages and insights that can be found in open sources.

In 1947, Allen Dulles calculated that more than 80% of the "information required for guidance of our national policy" was accessible via public sources. In a 1997 New York Times interview, George Kennan increased the estimate to above 95%.It is only appropriate to utilize these sources as the beginning point in a line of research given the expected quantity of important knowledge that is accessible via open sources. Both for national security and law enforcement, the application is equally legitimate. The examples, which are all based on real-world situations, demonstrate this idea:

A property developer claims that he has received a threat from a mysterious extremist environmental organization warning that "he will pay the price" if he continues with the development of condos in a sensitive area. A brief scan of news articles reveals the environmental group's existence in other places, its prior operations and assaults, and the attack strategies. This might be a crucial factor in determining the precise intelligence needs and preventive strategies in the present situation.

Law enforcement receives information that a violent radical Islamic preacher will be visiting the area to address a local gathering. An open-source search yields details about the speaker's prior addresses, their substance, and any public safety problems that may have arisen in connection with those remarks.The owner of a nursery claims that a guy recently bought an abnormally big amount of fertilizer while operating a rented vehicle. Although a criminal background check came out clean, the person's address and others who were known to use the same address were found using an open-source search of a commercial integrated database. Some of the man's acquaintances are found on a right-wing extremist website, according to a search engine.

According to a trusted source, a dangerous gang is gradually settling in the area. In order to learn more about the gang, identify gang traits, find examples of the gang's graffiti and tattoos, and disseminate the material, an intelligence analyst performs an open-source search. A gang of anarchists declares that they would protest the World Bank president who is scheduled to speak at a nearby university's graduating ceremony. Anarchists want to significantly disrupt the demonstrations by damaging targeted property and avoiding arrest, according to a search of anarchist websites.Each time, a fast open-source search was conducted after the original tip or lead to learn more. The open-source information offered more than just the information gave analysts deeper understanding of the danger and helped them to specify clear intelligence needs in order to completely articulate the threat picture.Open sources are not only quick, but they also pose a small threat to civil rights as a source of first resort. Open sources are also less costly than conventional law enforcement intelligence gathering techniques.

Initiatives on a national scale: The National Open-Source Enterprise

By virtue of the Intelligence Reform and Terrorism Prevention Act of 2004, the Office of the Director of National Intelligence was established. The creation of a thorough national intelligence strategy, along with the creation of an environment that maximizes the sharing of

intelligence and information among the intelligence community, law enforcement, the private sector, and international partners, was one of the ODNI's mandates. The ISE calls for the creation of a uniform intelligence language as well as standardized security and information-sharing guidelines. One technique used by the ODNI was the development of the National Open-Source Enterprise, which was designed to optimize effective, efficient, and comprehensive information collecting in support of the intelligence process.The ODNI says that as this business has grown:

It is crucial that our decision-makers, war combatants, law enforcement, and homeland security authorities get accurate, usable, and timely intelligence assistance given the difficulties and risks the United States confronts in the twenty-first century. The gathering of national intelligence via an integrated collecting enterprise, the core of which is a strong, distributed, open-source exploitation capacity known as the National Open-Source Enterprise, is one aspect of this new approach to intelligence.The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction made the following observations, which The NOSE expands upon:

There is a greater need than ever for the intelligence community to rapidly and readily grasp a broad variety of foreign nations and cultures; knowledge that is often documented in open sources. The constantly-shifting nature of our intelligence demands.The following are some of the additional duties of members of the Intelligence Community as a result of Intelligence Community Directive 301, which established NOSE:

a. All open-source materials, goods, and services should be accessible to the whole intelligence community.
b. Through the Assistant Deputy Director of National Intelligence for Open Source, coordinate all open-source resources and initiatives.
c. Every department or organization should appoint a lead open-source coordinator.
d. Support the Open-Source Center's Director in hiring the necessary personnel.
e. Utilize all available open source knowledge, skills, and resources to perform analysis and guide gathering techniques.
f. For open sources, use a structured intelligence requirements method.

These obligations show a significant dedication to open source initiatives. The OSC, previously the Foreign Broadcast Information Service, was established as a substantial undertaking in this area, with the CIA acting as its Executive Agent.

On subjects including military affairs, politics, the environment, social concerns, economics, science and technology, and military affairs, OSC provides in-depth coverage of open source intelligence material that is gathered from sources all around the globe. Radio, television, newspapers, magazines, books, and other unrestricted information sources including databases and gray literature are used to get the information.

The website may be accessed using a regular Internet connection and contains a vast quantity of information in both text and multimedia. The website's registration process, which involves confirming employment and that the requester has a need to know sensitive homeland security information, is open to state, municipal, and tribal law enforcement employees. The main benefit of the OSC to law enforcement is the free access to numerous commercial databases, even though there is a lot of material there that will be of interest to many SLTLE agencies even if it is only marginally relevant. The approach taken by these and other open source initiatives shows

how important and valuable the creation of a new open source capacity is. Furthermore, the NOSE becomes even more significance in light of the ISE's deployment, the objectives of information exchange within the Intelligence Community, as well as with SLTLE and the private sector.

Law enforcement intelligence and open source

The intelligence community refers to the techniques employed in the gathering and processing of intelligence on both wide and narrow scales collectively as "tradecraft". Even if the phrase is seldom used in law enforcement, it is nonetheless important to comprehend what it means in light of recent ISE advancements. Open-source tradecraft has two implications for law enforcement as a result. It generally refers to how open sources may be exploited in the intelligence process at the macro level. At the granular level, it refers to the explicit processes for carrying out open-source searches as well as gathering and analyzing unprocessed open-source data. The remaining conversations center on open source expertise for both federal and state law enforcement [3]–[5].

A law enforcement officer or analyst should not be discouraged from utilizing information just because it was gathered from an open source. In fact, open sources often provide excellent, insightful evidence. NOSE is effectively implementing the recommendation made in the 9/11 Commission's Final Report to establish a new "Open-Source Agency" to the U.S. intelligence system. The use of open sources in law enforcement intelligence has specific uses and guidelines that differ somewhat from open-source exploitation by Intelligence Community agencies, but this is true of almost every other area of intelligence concerns. The fundamental difference between the two is that theOnly open-source data identifying people and/or organizations where there is a criminal relationship should be collected and stored by SLTLE agency.Numerous open-source apps for law enforcement intelligence should be adopted as regular procedure in the intelligence process, as will be explained.

Criminals Likewise Employ Open Source

A crucial witness in a 2006 Crips gang-related double homicide in Riverside County was a 15-year-old Sierra Vista High School student who was shot on October 13, 2007, in front of his southwest Las Vegas house. Authorities in California believe that another juvenile shotTo stop him, Demontre Carroll struck him in the back. The attacker found the boy via his MySpace profile, who had moved from Southern California to Las Vegas as a result of threats to his life.

CONCLUSION

In general, police enforcement agencies and other organizations are using open-source information and intelligence as a more crucial instrument. Agencies may improve their operational and investigative capacities as well as better safeguard the people they serve by making use of this priceless resource.

Law enforcement organizations must create strong data analytics tools and procedures that are intended to gather, examine, and distribute open-source data in a responsible and ethical way in order to handle these difficulties. To speed up the study and distribution of open-source material, this may include using machine learning techniques, natural language processing, and other cutting-edge technology.

REFERENCES

[1] O. Ivanenko, "Use Of Open Sources Of Information In The Interests Of Intelligence And Ensuring Information Security," *Mest J.*, 2021, Doi: 10.12709/Mest.09.09.01.05.

[2] C. Y. Lee, T. E. Davis, And E. K. Noji, "Suicide Bombing Of The Mineralnye Vody Train: Case Study In Using Open-Source Information For Open-Source Health Intelligence," *Prehosp. Disaster Med.*, 2007, Doi: 10.1017/S1049023x00004866.

[3] V. Herrington, "Open Source Information And The Military Intelligence Library.," *Mil. Intell. Prof. Bull.*, 2005.

[4] J. Crowe And T. S. Davidson, "The 'Grey' Intersection Of Open Source Information And Intelligence," In *Gl-Conference Series: Conference Proceedings*, 2009.

[5] B. Biderman, "Michael Bazzell, Open Source Intelligence Techniques. Resources For Searching And Analyzing Online Information," *Stud. Politol.*, 2019, Doi: 10.33896/Spolit.2019.54.11.

CHAPTER 24

LAW ENFORCEMENT APPLICATIONS OF OPEN SOURCE

Prof. (Dr.) Mita Poddar, Professor
Seedling School of Law & Governance, Jaipur National University, Jaipur, India
Email id- hod.law@jnujaipur.ac.in

ABSTRACT:

Open-source intelligence (OSINT) refers to the collection, analysis, and use of publicly available information for intelligence purposes. Law enforcement agencies have increasingly recognized the value of OSINT as a tool for enhancing their investigative and operational capabilities. OSINT can provide law enforcement agencies with valuable insights into criminal activities and potential threats. By monitoring social media platforms, online forums, and other publicly available sources, agencies can identify and track individuals involved in criminal activities, as well as track the movement of drugs, weapons, and other illegal goods.

KEYWORDS:

Intelligence, Illegal, Law Enforcement, Open Source,Suspicious Activity.

INTRODUCTION

Open source has tactical and strategic uses for law enforcement intelligence, including the following. Locating and confirming facts. Finding and verifying a variety of information is perhaps one of the most frequent applications of open sources in law enforcement. Through open-source public and commercial databases and directories, it is simple to find personal identifying information, addresses and phone numbers, e-mail addresses, automobiles known to have been used, and property records, among a broad range of other facts. Sociable media. MySpace and other social networking sites provide a plethora of information on users and the people they communicate with. Social networking websites include user and friend identities, sometimes with images, as well as private communications and declarations about values and conduct. In addition to contact information, likes and dislikes are often included, covering anything from politics to entertainment to persons [1]–[3].A lot of information is accessible as an open source, even while certain information, like a private communication, is subject to legal action.

Identifying those who commit crimes. Unexpectedly often, individuals will say things that are damning in public forums. It has been reported in the media, but it happens most often on websites that are either social networking sites or websites that focus on a certain deviant or illegal activity. The "deep web" has been used by sexual predators, drug dealers, those selling stolen goods, and criminal extremists, for instance. While damning remarks by themselves will not satisfy the standard of evidence required for conviction, they unmistakably create a criminal predicate and provide grounds for additional investigation.

Having an understanding of and applying ideas. Understanding the driving force or logic behind those who engage in criminal conduct is a crucial component of analysis that helps define and anticipate dangers. Websites may be a useful resource, especially in the case of ideological fanatics. Extremist websites often explain their views as well as the actions or changes that their movement will bring about. Additionally, digging deeper and reading blogs might reveal more about a person's ideas and activities, including damning remarks. Recognizing criminal tactics. Getting information from blogs, websites, and/or the media may provide you valuable insight into the objectives and tactics of criminal activity. In many instances, it is simple to pinpoint the methods used by violent serial offenders, criminal fanatics, and criminal organizations. This might be useful knowledge for creating preventative tactics; for instance, anarchists deploy the "black bloc" strategy, which involves property damage and other potentially illegal behaviors. Multiple free resources are available for learning the strategies [4], [5].

Recognizing new patterns and challenges in crime. New and developing crime patterns may be discovered via open sources, just as criminal tactics can. Certain forms of crime often follow a predictable geographic pattern of dispersion. Good examples are gang activities and drug trafficking. Monitoring new and evolving crimes or changes in crime patterns over a large geographic area may often provide insight into future crime issues for a region. For instance, the development of methamphetamine hydrochloride began in populated regions on both sides of the United States. It followed a pretty predictable route that made forecasting possible as it spread to rural regions and the Midwest. A large portion of the material was readily recognizable because to media accounts.

An illustration of "Pushed" Open-Source Data

A number of direct action protests took place in San Francisco in March 2008. Demonstrators voiced opposition to U.S. policies toward Israel, economic concerns, and global warming in addition to their main emphasis on the war in Iraq. On "direct action" websites, several protesters said they would engage in civil disobedience, and arrests were expected. The author looked up many direct action web sites associated with the event to find out more about the demonstrations and the preparations. One website offered day-long text updates on plans and activities for mobile devices. The author joined up for the SMS service and had information about the protest "pushed" to his phone, allowing him to keep track of events and be to designated sites of civil disobedience before most protesters.The papers were available online in almost real time, demonstrating how open source knowledge can be presented in a variety of ways thanks to technology. A word of caution: Just as law enforcement looks for information that might shed light on criminal activity, those who engage in illegal activity may also try to spread false material on their websites in an effort to deceive police enforcement officials. This raises special concerns for ideological organizations that could try to persuade law enforcement to take an unlawful action or just divert law enforcement's attention from the group's actual operations. This highlights the need of checking sources and material.

DISCUSSION

Open Sources and Civil Rights

SLTLE agencies, in contrast to Intelligence Community agencies and the private sector, are required to exercise extreme caution in the handling of open source material because to special regulations governing the storage of information in a criminal intelligence records system.

For an SLTLE agency, the raw data that may be gleaned from public sources often falls into two categories: 1. Details on people and organizations, plus 2. aggregate data that is anonymous. In principle, no matter how unimportant a particular piece of information may seem, when a law enforcement agency undertakes an open source search for information, the agency should presume that civil rights protections extend to any material that identifies people or organizations. On the other hand, as a general rule, no civil rights apply to generalized information or descriptions of problems, movements, philosophies, etc. that do not include personal or organizational identifiers. When the material concerns First Amendment-protected expressive conduct, it is especially important. It is simple to find information on blogs and websites that makes extreme claims about a wide range of behaviors, such as support for global terrorism, support for the legalization of drugs, vehement opposition to the policies of government officials, support for pedophilia, racist beliefs, and so on. It might be difficult to tell the difference between utterances that have a criminal connection and strong expressive opinions.

The variations are often minute. Despite being extreme, the expressive remarks are less clear. Additionally, even in these examples, more information would be required to establish a criminal predicate.The essential principle is not the source of the information, but what information is being retained by a law enforcement agency. It is good practice to assume that any information identifying individuals or organizations collected from open sources must be 28 CFR Part 23-compliant.44 Therefore, there must be evidence establishing a reasonable suspicion that there is a nexus between the person or organization identified in the open source and a crime; this is known as the "criminal predicate test." The following are some examples of open source software:

The criminal predicate test for intelligence records normally does not apply if data is being gathered from public sources as part of a criminal investigation into a crime that has already happened. Instead of the criminal intelligence records system, the law enforcement agency's records management system would be used to store information from a criminal investigation. Without the need for a criminal foundation, open source data may be used to analyze the conduct of prior protests or demonstrations, the strategies employed in other protests and demonstrations, the results, and the actions and behaviors of the protesters and demonstrators.The basic norm is that an open source enquiry identifies individuals who have been detained during a protest or demonstration; this information may be preserved without a distinct criminal predicate being established, although there is considerable controversy about this. Probable cause, which is a higher standard than the "reasonable suspicion" needed for the criminal predicate, has been established if a person has been arrested.

- If a law enforcement agency receives a report of suspicious activity indicating that a particular person may have committed a crime while participating in a protest or demonstration, that information might be kept in a short-term criminal intelligence file until more evidence can be gathered to confirm the accuracy of the report. When this occurs, the The criminal intelligence records policy of the law enforcement agency should be observed.As long as specific people or organizations are not identified, law enforcement agencies are permitted to gather, analyze, and retain descriptive information about extremist ideological beliefs, behaviors of those who support those beliefs, changes and trends in extremists' beliefs or collective behavior, methods advocated for achieving the goals of the extremist ideology, and potential targets of the extremists' actions.

It is enticing and simple to compile intelligence dossiers on people who are just suspect using open source data. Similar to this, it is simple to search a social networking site to see if anything intriguing can be found about a certain individual. However, just like with any other kind of criminal intelligence material, law enforcement officers must adhere to 28 CFR Part 23-compliant protocols while gathering and storing open source information in a criminal intelligence records system. It's worth saying again:

The question is not whether the data came from an open source, but rather whether a law enforcement organization can appropriately store the data. Decisions must be made with the purpose of information retention, not the information's source, in mind.It's crucial to keep in mind that laws, whether they pertain to intelligence records laws, open records legislation, state freedom of information acts, or state privacy acts, differ by state and location. State laws governing criminal intelligence records should be carefully examined since there is enough variation across the states.

Working with Internet Service Providers and Web-Based Businesses Open source searches sometimes result in the have to employ legal channels in order to get further information on an enquiry. Of course, there are serious privacy issues raised when a law enforcement agency requests details on a person's particular actions when they are a client or customer of a private firm.Even if this procedure goes beyond open sources, it is important to keep in mind that Internet service providers and businesses that run social networking websites often have a written policy and guide to explicitly engage with law enforcement organizations. Although the reader should be aware of this since a legal procedure must be employed and information that is not publicly available is being sought, this information is not publicly available when the process extends beyond what is publicly accessible on the Internet [6].

Indicators of Authorship and Copyrighted Materials in Intelligence Reports and Process

A significant portion of the open-source data gathered during the intelligence process is in the public domain, or data for which no copyright is asserted. In other situations, such as with certain commercial databases, the information's rights have been purchased via a contract in line with customary government procurement practices. However, in many other instances, agencies get copyright data without the consent of the copyright owners. Too often, information used in law enforcement agency products from intelligence reports to training manuals is taken from other sources without any mention of the original source. Four main factors make attribution significant:

1. It provides confirmation and backing for the report's proposed line of reasoning, inference, or conclusion.
2. It enables the user to independently assess the original source and allows the user to access the original source for further information on the issue.
3. Usually, attribution complies with legal requirements for items protected by copyright.
4. Giving due credit for other people's thoughts, ideas, creativity, and effort is the morally just and ethical thing to do.

The ODNI has highlighted the importance of attribution via Intelligence Community Directive 206, Sourcing Requirements for Disseminated Analytic Products47.Endnote citations for sources must be included in all published analytical output. All relevant, substantial reporting or other material that influences the product's analytical conclusions, evaluations, estimations, alternative

hypotheses and viewpoints, or confidence levels must be included in these endnotes. The following idea serves as the foundation for the significance of attributing information to the original source:

1. Consumers may better grasp the amount and quality of material supporting intelligence analysis thanks to thorough and consistent documentation, which also increases the analysis's credibility and transparency.
2. Naturally, not all credited content is copyrighted, especially when it comes to public data. The majority of publicly available information and documents that were first gathered by the law enforcement agency are not copyrighted. For the sake of legitimacy in these situations, attribution is crucial.

Information that is not part of public records should be properly cited, especially if it comes from a copyrighted source. A strategic intelligence product may employ data from a book on terrorism, a television network film showcasing terrorist attack techniques, or the unique concepts and ideas of a consultant for an intelligence report. All should be regarded as copyrighted content and given proper credit to their originating sources. A copyright is a kind of protection offered by American law to creators of original works, including textual works, both published and unpublished, as well as audio and video files. The owner of copyright has the sole right of use, distribution, limitation of distribution, and the ability to grant others permission to reproduce copies, use the copyrighted material, create derivative works based on the original, rent, sell, or otherwise transfer the copyright, all under the protection of federal copyright law.

To the same extent as any other person or organization, law enforcement authorities are required to abide with copyright laws. The "fair use" exception allows use of the resources without requesting permission from the copyright owner, even though it is crucial to recognize and respect copyrighted works. The fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by law, is not considered a violation of the copyright when it is done for purposes like criticism, comment, news reporting, teaching, scholarship, or research. The following considerations must be taken into account when assessing whether a specific use of a work constitutes a fair use:

1. The reason and nature of the usage, including whether it is being done for profit or for educational reasons.
2. The composition of the protected work.
3. The size and importance of the fraction utilized in proportion to the whole copyrighted work.
4. The impact of the usage on the copyrighted work's potential market or value.

If a fair use determination is established after taking into account all of the aforementioned elements, the fact that a work is unpublished should not by itself preclude such a determination.According to a Congressional Research Service assessment, copyright law affects open source intelligence specifically:Like other users of public information, intelligence organizations are bound by the "fair use" law when employing such copyrighted material. It is obvious that law enforcement organizations must adhere to copyright regulations. Beyond the legal responsibilities, providing attribution of material where appropriate is just good manners.When law enforcement organizations hire a commercial vendor whose work is copyright protected, problems with copyright and credit arise. Users of the information must be careful to comprehend the service contract's copyright consequences. Law enforcement

employees should always include copyrighted content in their searches when gathering data and creating intelligence reports, make sure to present accurate information sourcing, and be knowledgeable with the correct steps under the fair use exemption.

Utilizing Metrics for Open Source

The usefulness of open source material has been extensively explored, but the only way to really assess its efficacy is to make sure that it is carefully created and assessed to fit the demands of the intelligence context in which it is being utilized. The lack of commonly used metrics or measures for open source intelligence is a problem, too.To make sure intelligence activities are achieving their intended aims and doing so without wasting resources, responsible managers must create outcome measurements for them.

These simple open source metrics might be used:

1. a total number of open sources mentioned in intelligence reports
2. the percentage of all analyses that employ open sources
3. percentage of time that open sources are used as a last option for intelligence needs
4. Compared to closed source environments, finding necessary information takes longer in open source environments.

These measurements indicate more than what is presently utilized, although being fairly superficial. Furthermore, when open source data is combined with data from closed sources by all-source analysts, it may be difficult to determine the exact contribution of open source data to a given intelligence product. Given its wider accessibility, the nature of the topics that today's analysts must cover, and the higher emphasis put on it by senior intelligence executives, it is projected that open source material will be relied upon more often. The qualitative contribution open sources provide to the analysis is the ultimate open source measure. Even if it is challenging to quantify, long-term evaluations should be produced in order to concentrate on the most effective open sources and the methods for incorporating them into the intelligence process.

Open-Source Information for Intelligence Operations

It is clear that information about almost any issue may be accessed on the Internet, even though open sources contain material that is not just obtainable online. In fact, there is often too much information available. The exploration and gathering process might start to become more manageable if you have some perspective on the many categories of open source information that are particularly valuable for law enforcement intelligence.Open Source Information from Subscription Services and the Media Identifying Individuals and Organizations

Subscription database services and media reports are two open sources that commonly identify persons and organizations that need extra attention. The appropriateness of their usage is often contested. Both can be effectively employed and are quite valuable for law enforcement intelligence. The restrictions for retention in criminal intelligence records systems must be implemented in the same way as any other information, just as in the case of any open source, and it is important to understand the sources' nature.

A large quantity of information regarding people, groups, criminal trends, movements, and criminal extremist ideologies may also be found by searching media sources58. With skilled employees and a worldwide network of informants, news organizations may do research and

explore almost any topic that would be of interest to a general audience. Responsible news companies often also have editorial guidelines to make sure that the data utilized in news articles is accurate, trustworthy, and verified. Because crime and criminal extremism are significant news, journalists often try to understand as much as they can about these events. Details that are helpful in the intelligence process are typically included in the depth of information. The news media may publicly name people and Criminal organizations often connect comparable people and situations across a variety of geographical locations. A search of news articles may provide both crucial leads and crucial, previously unknown information regarding an area of study. But a word of warning: not all media outlets follow the same strict guidelines.Like any other source, the media outlet's ethics and reputation must be assessed.

Systems that enable information searches from both public and private databases have been created by a number of businesses employing proprietary data integration software. Examples of the many data kinds that may be acquired. Businesses like AutoTrack, Accurint, Lexis-Nexis, RiverGlass, and others enable the creation of very precise information about individuals into a summary report. Although there is a cost associated with these services, they are still considered open source since anybody may buy the data without the need for a court order or covert data gathering techniques. The criminal predicate rule continues to apply to material stored in law enforcement intelligence databases, which is crucial to note given that both subscription services and media sources may supply a large amount of detail about people and organizations.

National Center for Media Exploitation

Initiatives taken by the Intelligence Community in relation to media information are noteworthy on a similar note. The National Media Exploitation Center of the Central Intelligence Agency was founded in late 2001 in response to the enormous volume of material that is readily available and accessible from the international news media. To collaborate with the FBI, CIA, and Defense Intelligence [7], [8].

CONCLUSION

Overall, the use of OSINT has grown in importance as a tool for law enforcement organizations looking to improve their operational and investigative capacities. By making use of this priceless resource, organizations may enhance their capacity to identify and stop criminal activity, as well as better safeguard the communities they serve. Law enforcement organizations must establish solid rules and practices for the gathering, analyzing, and disseminating of OSINT in order to meet these problems. This might include the creation of clear standards for the management and storage of sensitive data as well as the use of sophisticated data analytics tools and machine learning algorithms to speed up information analysis and dissemination.

REFERENCES

[1] D. Wijnberg and N. A. Le-Khac, “Identifying interception possibilities for WhatsApp communication,” *Forensic Sci. Int. Digit. Investig.*, 2021, doi: 10.1016/j.fsidi.2021.301132.

[2] S. O. Ogunlana, “Halting Boko Haram / Islamic State’s West Africa Province propaganda in cyberspace with cybersecurity technologies,” *J. Strateg. Secur.*, 2019, doi: 10.5038/1944-0472.12.1.1707.

[3] H. Jo, J. Kim, P. Porras, V. Yegneswaran, and S. Shin, "GapFinder: Finding Inconsistency of Security Information from Unstructured Text," *IEEE Trans. Inf. Forensics Secur.*, 2021, doi: 10.1109/TIFS.2020.3003570.

[4] M. J. Hernandez Mediná, C. C. Pinzón Hernández, D. O. Díaz López, J. C. Garcia Ruiz, and R. A. Pinto Rico, "Open source intelligence (OSINT) in a colombian context and sentiment analysis," *Rev. vínculos*, 2018, doi: 10.14483/2322939x.13504.

[5] N. E. Stone, "Social Media Canvassing Using Twitter and Web GIS to Aid in Solving Crime," *Phys. Rev. B*, 2017.

[6] H. Christianto, "Ajaran Sifat Melawan Hukum Materiil Sebagai Upaya Harmonisasi Ketentuan Hukum Pidana Pornografi Melalui Internet," *Ijcls (Indonesian J. Crim. Law Stud.*, 2017, Doi: 10.15294/Ijcls.V2i1.10813.

[7] B. Yulianto And Setiono, "Android-Based Public Transport Violation Reporting Application," in *IOP Conference Series: Earth and Environmental Science*, 2021. doi: 10.1088/1755-1315/832/1/012038.

[8] P. M. Barone and R. M. Di Maggio, "Low-Cost CSI Using Forensic GPR, 3D Reconstruction, and GIS," *J. Geogr. Inf. Syst.*, 2019, doi: 10.4236/jgis.2019.115030.

CHAPTER 25

SOCIAL NETWORKING CONCEPT AND ISSUES FOR OPEN SOURCE

Ms. Manali Rathore Chauhan, Assistant Professor
Seedling School of Law & Governance, Jaipur National University, Jaipur, India
Email id-manali.rathore@jnujaipur.ac.in

ABSTRACT:

Social networking platforms have become an increasingly important source of open-source intelligence (OSINT) for law enforcement agencies. These platforms allow individuals and organizations to connect and share information with each other, creating a vast network of publicly available information that can be used to support intelligence gathering and analysis. However, the use of social networking platforms for OSINT also presents several challenges and issues. One of the key challenges is the sheer volume of information available on these platforms, which can make it difficult to identify and extract relevant information. Law enforcement agencies must therefore develop effective search and filtering strategies to identify relevant data.

KEYWORDS:

Agency, Issues, Law Enforcement, Open Source, Social Networking.

INTRODUCTION

A social network is a connected, communicative structure of individuals made up of "nodes" that may either be a single person or a group of people. The common interest may be anything that can be defined, including music, a profession, a personal philosophy, a political affiliation, a sexual orientation, a hobby, and so on. This is the foundation of the connection. Depending on the many characteristics, each node could have different connections. One individual could belong to many social networks, for instance. A person who works as an accountant could also be passionate about motorcycles, country music, and fantasy football. Each variable can indicate a person's participation in several social networks. For those who adhere to radical ideas, belong to gangs, or engage in illicit behaviors like drug usage or pedophilia, similar social network models may be developed [1], [2].

While social networks have existed in some capacity since the beginning of time, the development of the Internet has given rise to new virtual social networks, exemplified by websites like MySpace, FaceBook, Bebo, Twitter, and SocialGrid. Other less complex and well-known social networking websites serve a range of interests. Ironically, users of social networks regularly publish material that may be used to prove a criminal case against them, or at the very least, be used to incriminate them. While it's possible to come across gang members or Earth

Liberation Front sympathizers on well-known websites like MySpace, there are a lot more underground websites where you may discover comments suggesting illegal activities. Because of this, innovative search techniques become crucial. Usually, using simple search parameters won't provide the desired results; instead, you need to utilize words and phrases that are specific to the social structure. As a consequence, learning about a social network's history is crucial as a first step.

YouTube offers a unique sort of social networking.70 The majority of readers are aware that anybody may upload films to our website for viewing by everyone. The videos include everything from comedy to confessionals regarding various topics. Videos about Hamas, Hezbollah, MS-1373, and other groups are among those present. The videos might be supportive of the cause in some situations while being critical of it in others. Viewing the films might provide fresh perspectives and visuals, including representations of the organization under investigation's signs and symbols.

The user needs register for an account and join the social network in order to search effectively. The law enforcement user should develop a phony identity and email address for the purposes of intelligence enquiries. Important: Before moving on, some moral and legal boundaries need to be thoroughly investigated. The necessity to ensure that remarks and actions by a law enforcement professional do not persuade someone to do a certain action that they would not have taken otherwise is of special significance. That is being caught. A law enforcement organization should create guidelines for the creation of fake identities and the use of such identities for intelligence purposes, including social networking.75 Despite the warning, the importance of utilizing each social networking website's search engine cannot be overstated.

DISCUSSION

Newsletters and Blogs

Strategic intelligence heavily relies on the monitoring of many threat-related indicators. These are essentially ongoing intelligence needs. Newsletters and blogs are two examples of open-source resources that are especially helpful for this purpose. Both paper and electronic newsletters are available, but the latter is becoming more common since it is more current and typically has hyperlinks that take the reader to sources with more in-depth information on the topic. In a certain subject area, problems, trends, and innovations are highlighted in newsletters. Blogs are online forums for debate where authors and readers may share their thoughts and ideas on a certain subject. In many situations, a single source will offer both a newsletter and a blog; for instance, Secrecy News76 from the Federation of American Scientists is a particularly helpful newsletter and blog for intelligence matters.

In general, newsletters and blogs fall into one of four major categories:

1. **Academic/professional and governmental:** These sources often rank among the most objective, although one can never completely rule out an author's or editor's accidental ideological impact. However, despite this warning, these sources are most likely to make claims based on verified data and instead of relying on emotive reasons, base your analysis and conclusions on logic and the scientific process. These sites typically convey facts and data more impartially and almost always give facts and data attribution.

2. **Private Sources:**These profit-driven sources, as their name suggests, often aim to provide information that helps sell goods or services. Despite the fact that the source's goal is to profit.Despite this, the sources may be highly trustworthy. In fact, the trustworthiness of these sources is often a key selling factor for the company. Although the material is usually correct, it is unlikely to offer information about alternatives.
3. **Advocacy Teams:**These sources have an agenda based on their ideologies and objectives. A right-wing extremist source's newsletter will provide material that backs their beliefs. Similar to that, debates on an environmental extremist blog will further their objectives. Readers should be aware of their perspectives and take them into consideration while doing analyses. These materials may be very instructive for comprehending an ideology or advocacy stance when used in this manner.
4. **Pundits:** Numerous people write online as commentators and critics on almost every issue. Pundits serve a number of employers, including news outlets, entertainment media, professional associationsetc. and others are independent critics who exclusively work for themselves, often in order to debate an interest rather than as a method of making money.

It is crucial to understand that pundits often remark on hot button issues from their own ideologies or points of view rather than trying to be neutral. For commentators who blog for news organizations, the same is true. Their observations and arguments are often convincing and helpful, yet they are also biased. As news and policy experts by nature, pundits often do research that identifies topics and information sources that could otherwise be easily overlooked. As a result, they are often reliable sources of unfiltered information that may be verified by unbiased sources [3]–[5].

Continually reading blogs and subscribing to emails may provide you a wealth of knowledge about trends, problems, and oddities. The issue should be actively investigated through other information sources to ascertain its reliability and validity and to assess the likely impact on one's area of responsibility when a new issue of concern starts to emerge on a regular basis, especially if it is reflected in multiple sources. There is benefit in depending on websites that aggregate blogs, newsletters, and news since the number of blogs and newsletters on the internet is unknown, and they are dynamic in both their existence and substance. These websites often feature search engines that only allow inquiries related to the site's topics and wide category organization for its material. Both elements help to reduce the scope of a search. Two such sites that aggregate information completely are

Wikis

Wiki software makes it simple for users to create, modify, and connect pages. Wikis, also known as community web sites or wikis, are often used to build collaborative websites and power them. Businesses are using these partnerships more often to create cost-efficient intranets and for knowledge management.80 More precisely, the cumulative business knowledge of all employees of an organization may be recorded, improved upon, and shared in a dynamic virtual environment.Wikis are often created with the notion that errors should be simple to fix rather than difficult to commit. Wikis provide a way to confirm the accuracy of recent contributions to the main body of pages even though they are public. The "Recent Changes" page—a particular list numbered recent modifications, or a list of all the updates done within a certain time frame—is the most popular, appearing on practically every wiki.

Wikis that are openly edited are subject to criticism for being readily manipulated, while supporters claim that the user base can identify bad information and remove it. The safest approach when using a public wiki is to utilize it as a pointing system and confirm the relevant information.There are many different kinds of wikis, some of which have a very specific focus. For instance, the ODNI OSC offers access to a wiki called Intellipedia that is specifically focused on intelligence. While primarily focused on the Intelligence Community, it contains information that is also helpful to SLTLE. When researching a subject or problem about which the information gatherer knows nothing, wikis may be a useful resource. Most wikis include external links to resources, which aids in the process of corroboration.From an intelligence standpoint, the wiki may provide subject matter expertise on a topic as well as pointers to other material.

The RSS feed

Blog posts, news headlines, and podcasts are just a few examples of the often-updated information that is published using the RSS family of web feed formats. Either the whole text or a summary of the information from a related website may be found in an RSS document. With RSS, subscribers may get automatic updates on websites that they are interested. When offered on a website, RSS feeds have the advantage from an open source standpoint of notifying subscribers of any new information or content updates without them having to visit each site individually. It improves the user's access to information and makes it more timely.

Literature in Gray

Gray literature is unpublished knowledge that is made freely accessible to a certain audience, generally without being published. Even when it is open, the material is sometimes difficult to locate or acquire. According to the American Library Association:The hardest parts of the process are identification because there is little indexing and acquisition because availability is often tainted by uncertainty. Additionally, the lack of editorial oversight raises concerns regarding veracity and accuracy.Gray literature has traditionally been referred to as any non-commercially published documentation material and is often made up of technical reports, working papers, financial records, and conference proceedings. These kinds of materials are increasingly accessible online, yet typical search engines often miss them.

This author has a broader understanding of gray literature, especially as it relates to the law enforcement intelligence gathering process. Gray literature's three main components are as follows: Existing documents of importance; the data is available; since the knowledge is not widely disseminated, finding it might be challenging. Therefore, the term "gray literature" ought to be used to describe all writings that fit these three criteria rather than only academic or scientific works. Gray materials include pamphlets created by a right-wing extremist and distributed at a local gun show or flyers created by anarchists and given out during a protest. In both situations, the materials are not released for profit but rather with the intention of being shared as widely and publicly as possible.

These unpublished documents are scarce, which makes it challenging to discover or identify them. The most probable method of collecting gray literature is by a human collector rather than via networking, and it must be investigated in light of the sorts of possible books that already exist and where they may be placed.

Internet Depth

The internet is a complicated system that houses a vast range of information in different forms. The vast majority of individuals typically visit websites using A mix of static and moving information. The fixed material, which is the most often discovered in conventional searches, has a tendency to alter little over time. With the exception of file names and file extensions, the dynamic information on many websites is far bigger than the fixed documents and is more likely to be overlooked in conventional searches.

The massive store of information that search engines and directories don't have direct access to, like databases, is referred to as the deep web or invisible web. Information in databases is often unavailable to the software spiders and crawlers that build search engine indexes, unlike pages on the visible Web.

According to estimates, the deep web has 500 times as much material as the visible web. The unseen web is made up of five major categories of content:

1. **The Information in Online Databases:**Databases contain information that can only be accessed via database queries; search engine web crawlers do not index databases. This is different from fixed, static web pages, which provide direct access to content. Databases may be used to provide a sizable quantity of worthwhile content for the web.
2. **Text-Free Files:**These include of software, graphic files, multimedia files, and papers in formats like the Por Document Format. Web Crawling is limited in its ability to search the contents of these kinds of files. File names and extensions may be recognized by web spiders of these files, but the web crawling algorithm is unable to determine their contents. Since they are essentially files that are not in HTML90 format, standard searches are unable to find a lot of information and data in these files.
3. **Sites with Scripts:** These are websites that use script coding rather than HTML and/or have URLs that start with
4. Website content that is password- or restriction-restricted. Search engines won't be able to access the content of websites with access restrictions imposed by strict password security or a Virtual Private Network. Depending on what sorts of information are collected from these types of websites, there is a continuum of identifiable and nonidentifiable data. of data the site owners decide to make available to the public, as well as the level of protection used on the website. It is sufficient to say that a significant portion of the material from these sites cannot be found using conventional search engines.
5. Intentionally omitted pages by their proprietors. If a web page developer doesn't want their website to be indexed by search engines, they may include specific meta tags that tell most search engine crawlers to stay away from the page.

Undoubtedly, if it could be found and recovered, a lot of open-source data from the deep web may be beneficial to the intelligence gathering process. The deep web can be searched, but not using conventional search methods. Finding tools that can identify useful open-source deep web data is the main objective.92 Using search utilities built to investigate certain databases is the most efficient technique to search the deep web. Even though this just covers a small section of the deep web, the knowledge gleaned from these databases may be quite useful even if it isn't always practical. In order to get the needed information, deep web searches of databases generally involve visiting many different websites.

The Dark Internet

Similar to how it has in real society, the underground web is a cultural dynamic that has developed on the Internet. According to a Business Week story, it was as follows. You are going to explore the Internet's shadowy side, so beware. Every perverse craving may be satiated there, where criminality is rife. Casinos, pornographic stores, and drug traffickers populate thousands of virtual streets. Terrorists and con artists hide behind what seem to be legitimate websites. And sometimes, a police officer would walk around, usually looking disoriented.

The underground culture, where transactions often straddle the boundary between legal and illegal conduct, is reflected in many widely accessible websites. These obvious locations—whether trading in illicit goods or engaging in any other kind of criminal activity—are often simple to uncover by diligent regular search procedures, despite the fact that they are almost hard to police. Although the sites are often run from abroad, their owners need to be somewhat easy to find in order to generate a profit for their operations. However, they do not want to be extremely noticeable or call attention to their activities.

There are other kind of subterranean deep web sites that aim to conceal their operations from the visible online world. They must, however, be reachable for their audience, with URLs being transferred between individuals by those involved in the clandestine operations. Examples of open-source material that may be found on the dark web include identity thieves selling credit card information they stole, pedophiles trading pictures, traffickers illegally selling dangerous narcotics, and criminal extremists organizing an event. Even while law enforcement intelligence is very interested in this kind of material, finding it takes time and effort. A criminal investigation may provide evidence and leads with the use of laborious deep online searches and blog and content reading. However, compared to conventional techniques of investigation, this procedure will be quicker and more efficient in identifying illegal concerns.

There is some hope that the procedure will become simpler. The Symantec Corporation beta-tested a new piece of software called Dark Vision in the middle of 2006; it searches chat rooms and deep-underground websites for sensitive information that is being sold.The initial strategy was to go after carder websites—deep-underground websites where credit card information stolen by identity thieves is sold. The program offers a breakthrough that may be used to combat various forms of illegal behavior, even if Symantec is unsure of when or even if it will be released. Incriminating information is widely accessible in open-source on the dark web. Finding this important information is a difficulty in terms of developing the search skills and dedicating the time.

Using Open Source for Law Enforcement from a Wider Angle

For law enforcement intelligence, the importance of certain online resources, such as directories, extremist websites, and social networking sites, is obvious. However, there is a vast variety of material that has value for the intelligence process but is less immediately obvious, for example:

Information identifying a name of an unknown geographic location and describing a potential hazard.

1. Information required for a strategic intelligence evaluation on the demographics of a certain region.

2. Information that has to be translated to American standards, such as foreign sources' measurements of money, distance, weight, temperatures, or garment sizes.
3. Real-time tracking information for private or commercial aircraft.
4. Legal description of the disputed house's GPS coordinates or picture.
5. A satellite picture of the specified place.
6. The need for digital video conversion in order for it to be seen on a police enforcement computer.
7. The requirement to locate a target's relatives for intelligence purposes.
8. An eclectic selection of web-based open sources includes all of these needs as well as many more.

It's vital to remember that internet open sources provide quick access to material that is both unique and essential to a thorough examination.

Open Sources and Homeland Security Intelligence

America's law enforcement organizations are responsible for upholding order and maintaining public safety in addition to implementing the criminal law. Law enforcement must assist in the rescue and recovery of victims during a natural catastrophe, such as a flood, tornado, or hurricane, as well as safeguard the public from damage and preserve property. Law enforcement authorities have traditionally had major responsibility for maintaining public safety and order in disasters including airplane crashes, building collapses, and public health emergencies. Many of these public safety tasks have grown more formalized as a result of the development of new national homeland security programs in the wake of 9/11.

A new kind of noncriminal intelligence called homeland security intelligence has arisen, particularly with the expansion of intelligence fusion centers that operate under the guiding principle of all dangers, all threats, and all crimes.

It is to be emphasized that intelligence is founded on prevention and is by nature a pre-incident role, regardless of whether the incidence is criminal or entirely noncriminal. Law enforcement requires a wide range of information to effectively prepare for homeland security threats identified through analysis.

Homeland security intelligence may once again be defined as "the analytic output of raw information that describes noncriminal threats to critical infrastructure, public health, or community safety." When gathering information and learning about the traits and dangers offered by pandemic flu, hazardous items, or other direct or accidental hazards posed by a homeland security catastrophe, open sources may be very helpful [6]–[8].

Environmental Chemistry offers a wide range of information on hazardous materials, the Centers for Disease Control offers information on health risks, and the National Center for Biotechnology Information of the National Institutes of Health offers a collection of online searchable databases with a wide range of useful information. It would be impossible to explore all of the dangers to national security in depth.

The main thing to keep in mind is that, given that the process for gathering law enforcement intelligence now includes gathering information about homeland security, especially at the state fusion center level, analysts and information gatherers should actively use open sources as the first step in gathering this crucial information.

Processes and Protocols Available Freely

It is possible to rely on a variety of tools and methods to increase the efficiency of the open-source data collecting process and improve the information's quality. The talk that follows serves as an introduction to the procedure.

Utilizing a Collection Plan from an Open-Source

Anyone who has visited the Internet is aware of how quickly one may be drawn away from their initial line of inquiry into a region of usually relevant but sometimes irrelevant material by the capacity to search various information and journey down an unexpected route of hyperlinks. This is counterproductive from an intelligence standpoint and puts at risk the gathering of unnecessary and sometimes distracting data. When utilizing networking to look for open-source material, the user is advised to create an open source collection strategy.

A collection strategy fundamentally serves as a study approach that aims to concentrate the open-source data gathering procedure. The collection strategy focuses on source searching that is specified by clearly stated agenda items rather than using a dragnet method, such as the following:

a. Required intelligence
b. Investigate a problem with an impending danger.
c. Locating data to back up tips and leads that have been received
d. To find out if a danger is present and having an impact in other regions, do some research on it.
e. Investigate a variety of innovative threat management strategies.
f. Obtain a corpus of knowledge on a certain intelligence target
g. Learn about the threat circumstances that are now in place and how they are evolving in your area.
h. The following should be in the plan:
i. Certain information kinds are required.
j. Locating the sources most likely to have the requested information.
k. Important details relating to a particular danger.
l. Information about dangers and their logistics.
m. Materials used in committing a crime or committing a terrorist attack, as well as how those materials are employed.

Certain traits pertaining to the intelligence objective.The important thing to remember is that open-source information gathering via networking works best when it has a clearly defined goal.

Tools and Methods

The ability to search effectively is maybe the most crucial foundational skill to master for any form of networking environment. The most typical method is to launch one's preferred search engine and utilize the built-in search function to get the required information. With this approach, some accomplishments are attained, but the outcomes often present a great amount of related information that frequently lacks the necessary specificity. In order to find the necessary information, narrowing the search may be more effective. Making a pre-search strategy with a focus on the search criteria is the first stage.

In addition to this strategy, consider the following search-narrowing advice:

Recognizing and correctly interpreting pertinent information requires an understanding of the culture of the intelligence target. A greater range of search words and phrases may be produced if the target culture or the content being searched is well understood. Additionally, identifying the sources or search engine to utilize may be made easier by refining the phrases.

Define the information-seeking categories carefully based on the culture evaluation. To do this, depend on the idea of collective exhaustiveness; specifically, make an effort to search all derivative words that describe the information or phenomena that the search is looking for. Dissect the material once it has been defined to come up with alternate names, synonyms, jargon, symbols, abbreviations, and alternative spellings.For deep online searches, this is very crucial.

By restricting searches to specifically designated regions, specialty search engines146 may aid in narrowing down a search. One may learn vital information from patterns in terrorism or crime to the identities of people or organizations that could be connected to threats by using a search engine that only prioritizes news websites147. Additionally, compared to many other websites, news websites often make it simpler to evaluate the quality of the material.There are more and more free internet translation services from several languages to English. Usually, these websites allow users to enter text for translation or a website link to translate the contents of the URL [9]–[11].

CONCLUSION

Finally, there are significant privacy and civil rights problems raised by the exploitation of social networking sites for OSINT. Law enforcement organizations are required to take precautions to preserve the privacy and security of people whose information may be gathered or analyzed and to make sure that they are not gathering or processing information in a way that violates the rights of particular people or groups. Law enforcement authorities must establish precise regulations and processes for the gathering, analyzing, and disseminating of information collected via social networking sites in order to handle these difficulties and problems. This can include the formulation of precise policies for the handling and storage of sensitive data as well as the use of specific tools and technology for data collecting and analysis. Overall, law enforcement organizations looking to improve their intelligence collection and analytic skills have a lot to gain from using social networking sites for OSINT. However, authorities need to be aware of the difficulties and problems with using these platforms and take action to make sure they are utilized in a way that respects people's civil rights and privacy.

REFERENCES

[1] E. Barsky, “Introducing Web 2.0: weblogs and podcasting for health librarians,” *J. Can. Heal. Libr. Assoc. / J. l’Association des bibliothèques la santé du Canada*, 2006, doi: 10.5596/c06-013.

[2] T. Coenen, D. Kenis, C. Van Damme, and E. Matthys, “Knowledge sharing over social networking systems: Architecture, usage patterns and their application,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006. doi: 10.1007/11915034_42.

[3] R. Cartwright, “An Internet of Things Architecture for Cloud-Fit Professional Media Workflow,” *SMPTE Motion Imaging J.*, 2018, doi: 10.5594/JMI.2018.2816879.

[4] R. M. García Sanz, “Redes sociales online□: fuentes de acceso públicoo ficheros de datos personales privados□: aplicación de las directivasde protección de datos y privacidad en las comunicaciones electrónicas,” *Rev. Derecho Político*, 2011, doi: 10.5944/rdp.81.2011.9151.

[5] R. G. Sanz, “Redes sociales online: fuentes de acceso públicoo ficheros de datos personales privados: aplicación de las directivasde protección de datos y privacidad en las,” *Rev. Derecho Político*, 2011.

[6] Danya Bashir and M. Minhas, “Transforming Education in the Arab World□: Breaking Barriers in the Age of Social Learning,” *Dubai Sch. Gov.*, 2013.

[7] “Educational psychology and the Internet,” *Choice Rev. Online*, 2016, doi: 10.5860/choice.197461.

[8] M. Glassman, *Educational Psychology and the Internet*. 2016. doi: 10.1017/CBO9781316155134.

[9] V. Arquilla, G. Simonelli, D. Genco, and F. Guaricci, “New Perspectives For An Open And Peer Educational Model In Design Field: The Co.Meta Project,” in *INTED2016 Proceedings*, 2016. doi: 10.21125/inted.2016.1457.

[10] B. J. Koops, J. H. Hoepman, and R. Leenes, “Open-source intelligence and privacy by design,” *Comput. Law Secur. Rev.*, 2013, doi: 10.1016/j.clsr.2013.09.005.

[11] S. Kowalczyk, “Jeremy Rifkin’s utopia of the economy of abundance,” *Kwart. Nauk o Przedsiębiorstwie*, 2017, doi: 10.5604/01.3001.0010.4678.