From Battlefield to Beat: Adapting Order of Battle Analysis for Organized Crime Assessment

Henry W. Prunckun*

Abstract

This paper adapts the military Order of Battle (OOB) analytical framework to improve law enforcement agencies' assessments of organized crime. Although some police departments and federal agencies have sporadically used OOB-inspired methods, inconsistent application and a lack of standardization have limited their effectiveness. As organized crime groups have become more complex and existing analytic methods often remain fragmented or retrospective, this study demonstrates that OOB—focused on composition, disposition, and capabilities—offers a systematic, comparative, and forward-looking approach to criminal intelligence. Rather than empirically testing operational outcomes, the paper uses comparative analysis and an illustrative application to show how OOB may help analysts organize intelligence, identify gaps, and communicate assessments more consistently. The paper should therefore be read as a conceptual framework-building study rather than an empirical test of operational outcomes; its purpose is to show how a military-derived analytic logic can be adapted for civilian intelligence analysis without importing military tactics, equipment, or command culture into policing.

Keywords: *Order of Battle, Intelligence-Led Policing, Organized Crime, Criminal Networks, Law Enforcement Analysis, Strategic Assessments*

INTRODUCTION

Given the adaptive, networked, and highly concealed nature of organized crime, intelligence-led policing has become a leading strategy in modern law enforcement (Ratcliffe, 2016). Despite advances in analytical techniques and operational methods, evaluating organized criminal groups remains challenging for police agencies worldwide (Levi & Maguire, 2004). Criminal organizations are marked by their flexibility, fluid membership, secretive operations, and strategic use of social, technological, and geographic opportunities (Morselli, 2009).

While military and national security agencies have long used rigorous methods, such as Order of Battle (OOB) analysis, to evaluate adversaries, law enforcement agencies seldom adopt this approach for tackling organized crime (Bowen et al., 1975; U.S. Department of the Army, 1994). In fact, OOB is the second step in the broader Intelligence Preparation of the Battlespace (IPB) cycle—defining and detailing an adversary's composition, disposition, and capabilities—so incorporating OOB into policing effectively adapts IPB principles for

* Corresponding author; Australian Graduate School of Policing and Security, Charles Sturt University, Sydney. Email: hprunckun@csu.edu.au

criminal-group analysis (Johnson, 1991a, 1991b). Research indicates that IPB can be tailored to enhance intelligence support for police tactical units, thereby improving completeness and detail during operational tasks (Boyd, 2020).

This absence is more than theoretical. The lack of a structured methodology limits police analysts' ability to reliably assess the makeup, disposition, and capabilities of criminal organizations, weakening efforts both operationally and strategically (Sheptycki, 2004). At times, law enforcement evaluations rely on makeshift approaches, case-specific intelligence, or fragmented analytical methods that can obscure patterns and connections within criminal groups (Bouchard & Morselli, 2014). Because some organized crime networks exhibit functional complexity, resilience, and geographic reach, law enforcement agencies may benefit from adapting selected military intelligence assessment methods as civilian analytical frameworks (Boyd, 2020; Williams, 2001).

This paper argues that adapting Order of Battle analysis for policing provides advantages for evaluating and, hence, disrupting organized criminal groups (Calderón et al., 2015). By applying this framework, law enforcement agencies stand to enhance analytical rigor, facilitate better cross-jurisdictional intelligence sharing, and improve both tactical actions and long-term strategic planning (Morselli, 2009; Paoli, 2002; Ratcliffe, 2016). In doing so, the paper aims to advance the development of intelligence-led policing (Ratcliffe, 2008) by establishing a methodological link between military and law-enforcement analytical practices.

The contribution of this paper is not to claim that law enforcement has never used OOB-like thinking. Rather, it argues that such thinking has remained partial, uneven, and under-standardized. Elements resembling OOB already appear in intelligence products that map group structure, geographic presence, and operational capacity; however, these elements are rarely treated as a distinct analytical framework with consistent terminology, training, reporting formats, and criteria for comparison. This paper extends previous work on adapting Intelligence Preparation of the Battlespace to policing, particularly Boyd's (2020) analysis of tactical intelligence support, by focusing specifically on the Order of Battle component as a standardized framework for the strategic assessment of organized crime.

To illustrate the practical value of this approach, the paper applies the OOB framework to a notional case study of the Sinaloa Cartel, demonstrating how structured analysis can clarify criminal operations and more effectively inform law enforcement strategies (Kilcullen, 2013). This paper should therefore be read as a framework-building essay, not as an empirical study. The claims advanced here concern the conceptual fit, analytic logic, and potential utility of OOB for policing; empirical validation is a matter for future research.

The argument advanced here should not be read as an endorsement of police militarisation. Its concern is analytical: whether a structured method originally developed in military intelligence can be adapted to a civilian framework for organizing information about criminal groups. In this sense, the proposed adaptation is methodological rather than operational. Its

legitimacy depends on being embedded within ordinary policing constraints, including legality, proportionality, accountability, privacy protection, and civilian oversight.

REVIEW OF CURRENT PRACTICES

Modern law enforcement employs a range of techniques to evaluate organized crime, including crime statistics, intelligence summaries, social network analysis, and risk assessment matrices. Despite the strengths of these methods, they are typically employed in isolation due to organizational constraints and the absence of a unified analytical framework (Ratcliffe, 2016; Levi & Maguire, 2004). Boyd (2020) further identifies IPB as a mature process of collection, collation, and analysis that police intelligence units can adopt, highlighting how military-derived analytical workflows can be translated into forward-looking police intelligence practices.

Crime statistics remain the most widely used measure, serving as both a gauge of organized crime activity and a basis for resource allocation. However, the usefulness of these statistics is limited by underreporting, inconsistent definitions, and a failure to reflect the complexity of criminal networks. Consequently, relying on quantitative data can obscure the adaptability of organized criminal groups (Levi & Maguire, 2004; Williams, 2001).

Ad hoc intelligence summaries, created in response to threats or specific investigations, are another common practice. These reports compile available information about group membership, criminal activities, and recent incidents. While they are helpful in the short term, such intelligence products are rarely standardized, resulting in variability in depth and quality. The episodic nature of their production also hinders long-term analysis and prevents the accumulation of institutional knowledge (Sheptycki, 2004; Bouchard & Morselli, 2014).

Social network analysis is important for visualizing and measuring relationships within and between criminal groups. This approach helps identify key figures, vital points, and weaknesses in networks. However, its broader use in law enforcement is limited by incomplete data, varying levels of analytic expertise, and the absence of standard frameworks, which makes it hard to apply findings across different cases (Morselli, 2009; Sparrow, 1991; Xu & Chen, 2005).

Risk matrices, which prioritize individuals or groups based on evaluated threat levels, are used by police agencies to manage limited resources more effectively. These techniques provide a sense of objectivity and help in sorting cases. However, they rely on subjective criteria, untested assumptions, and incomplete data, which reduces their reliability and usefulness in operations (Ratcliffe, 2016; Levi & Maguire, 2004).

The organizational situation of law enforcement further complicates these analytical challenges. For example, specialized units, such as Gang Intelligence Units, Organized Crime Task Forces, and C3 (Command, Control, Communication) policing initiatives, are created to concentrate expertise and resources on specific criminal threats. While these units achieve successes, their methods of intelligence gathering and analysis tend to be unique and shaped

by local priorities. This fragmentation hampers the development of consistent analytical standards and inadvertently obstructs the systematic sharing of intelligence across jurisdictions (Sheptycki, 2004; Carter, 2004; Decker & Curry, 2002).

Together, these practices show a field in which analytic creativity exists but is constrained by structural, methodological, and organizational challenges. The lack of a formal, widely accepted framework for evaluating organized crime groups, naturally, leads to inconsistency and hampers the implementation of strategic, evidence-based interventions (Bright & Deegan, 2021). This situation highlights the need for a more rigorous, transferable, and systematic method, such as Order of Battle analysis, that can provide greater coherence and effectiveness in policing organized crime (Heuer & Pherson, 2014).

Although various analytic techniques are used today, an underlying issue remains: the lack of standardized practices among law enforcement agencies. Organizations involved in policing, both within and across different regions, vary in their methods, reporting standards, terminology, and data-sharing approaches due to differing institutional goals, resources, and legal systems. These differences hinder effective collaboration between agencies, slowing the exchange of intelligence and impeding the development of scalable, shared solutions (Ratcliffe, 2016; Sheptycki, 2004; Williams, 2001).

Another gap involves the insufficient focus on long-term and comparative analyses. Most existing intelligence frameworks prioritize immediate operational needs over ongoing assessment. This short-term approach limits agencies' ability to track the development of organized crime groups, identify emerging threats, and proactively adjust strategies before threats manifest. Without analytical mechanisms to track trends across time and jurisdictions, agencies react to incidents rather than anticipate and disrupt criminal activity (Ratcliffe, 2016; Levi & Maguire, 2004).

Current practices are also hindered by a natural tendency to emphasize retrospective over prospective analysis. Law enforcement techniques typically rely on historical crime data, completed investigations, and retrospective intelligence reports (Lum & Koper, 2017; Maguire & John, 2006). While helpful for understanding past criminal activities and networks, these methods are insufficient for predicting future threats. This backward-looking focus creates a strategic vulnerability, underscoring the need to include more forward-looking analytical approaches in standard police work (Pherson & Pherson, 2020).

Furthermore, communication challenges persist in translating intelligence analysis into practical decision-making support. Intelligence products can fail to provide actionable insights for operational commanders or policymakers when they are overly technical or abstract. This gap between analysis and operational use—the "translation gap"—reduces the impact of analytic work on strategic decisions and may weaken trust in intelligence-driven approaches among senior decision-makers (Innes, 2014; Stelfox, 2007).

Addressing these analytic and communication limitations requires adopting a structured and proactive analytical approach, such as Order of Battle analysis from military practice, to close these important gaps. Using a unified, systematic method could improve analytic

consistency, promote cross-agency intelligence sharing, support strategic foresight, and increase the clarity and operational relevance of intelligence products, ultimately boosting law enforcement's ability to anticipate and effectively disrupt organized crime (Levi & Maguire, 2004; Pherson & Pherson, 2020; Shelley, 2014).

Despite these challenges, it is important to recognize that some law enforcement and security-intelligence practices already incorporate elements that resemble OOB analysis, particularly when analysts assess the structure, geographic presence, and operational capacity of criminal organizations or terrorist networks (Brodeur, 2010; Carter & Carter, 2009). The problem is not the complete absence of OOB-style thinking, but its uneven use. Because these elements are usually embedded within broader intelligence products rather than applied as a distinct framework, terminology, depth of analysis, reporting expectations, and training requirements remain inconsistent. This fragmented practice strengthens the case for a standardized OOB-based approach aligned with structured analytic methods, including the frameworks promoted by Pherson and Pherson (2020).

UNDERSTANDING ORDER OF BATTLE

Order of Battle analysis originated as a systematic approach to military intelligence, designed to help commanders understand not only the size of enemy forces but also their structure, deployment, and combat potential. Although lists of units existed in the Napoleonic era, the discipline of OOB matured in the twentieth century, as large-scale, industrialized warfare required detailed, reliable intelligence to support both battlefield tactics and long-term campaign planning. For example, during World War II, OOB analysis integrated data from reconnaissance, intercepted communications, and prisoner interrogations to create comprehensive profiles of opposing armies (Bowen et al., 1975; Freedman, 1994).

Although OOB analysis has strong conceptual foundations, it has long faced practical and methodological issues in military contexts. Historical reviews and practitioner surveys indicate that methods for processing OOB intelligence often lack formal standards, resulting in assessments that are more retrospective than current or predictive (Bowen et al., 1975; Coates & McCourt, 1976). Analysts struggle to integrate the extensive, detailed information required for effective OOB, which can lead to information overload or critical gaps in combat effectiveness. These limitations sometimes reduce OOB's usefulness for real-time operational decisions, as OOB sections tend to serve as historical references rather than sources of actionable intelligence. Additionally, the way OOB elements are perceived and used varies among users, suggesting that without solid methodological support, OOB may be applied inconsistently, even within the military environment where it was developed.

At its core, OOB breaks down an adversary into three essential components (Bowen et al., 1975; Freedman, 1994; US Department of the Army, 1994):

- Composition: The organizational elements—such as divisions, brigades, and command hierarchies—that define which actors or units make up the force. In a

military context, this might include identifying armored, infantry, and support units, as well as logistics and command staff.

- Disposition: The spatial, temporal, and functional arrangement of these elements—essentially, "where" and "how" forces are deployed or maneuvered. This could involve mapping troop concentrations, supply depots, or patrol patterns to reveal operational priorities and vulnerabilities.
- Capabilities: The "what can they do" dimension—an assessment of equipment, training, doctrine, morale, logistics, and recent operational performance, which collectively determine the subject organization's ability to act.

Translating OOB to law enforcement presents both opportunities and challenges. While the analytical logic is transferable, policing contexts require reinterpreting each component (Ratcliffe, 2008; Ratcliffe, 2016). A parallel doctrinal model, intelligence preparation of the battlespace, has evolved through adaptation by police tactical groups, offering a tested framework for enhancing analytic rigor in applied settings (Boyd, 2020).

- Composition: Instead of military units, analysts map the leadership, membership, facilitators, and support networks of organized crime groups. For instance, an OOB assessment might distinguish between core leadership, regional managers, financial operatives, and street-level associates.
- Disposition: Here, attention shifts to geographic reach (e.g., city neighborhoods, border crossings, transnational networks), operational nodes (warehouses, safehouses), and patterns of criminal activity or mobility, such as trafficking routes or hotspot locations.
- Capabilities: In policing, this encompasses criminal expertise (such as drug production or cybercrime), access to resources (weapons, technology, and vehicles), the ability to corrupt or coerce, financial strength, and resilience to law enforcement pressure.

Nevertheless, this adaptation is not without difficulty. Law enforcement agencies rarely possess the same level of intelligence resources or operational access as the military, and criminal organizations often operate with greater flexibility and secrecy than conventional armed forces. However, OOB offers the logic for imposing structure and clarity on difficult-to-investigate criminal environments (Ratcliffe, 2016; Brodeur, 2010).

ANALYTICAL APPROACH

This paper uses a conceptual and comparative analytical approach to assess whether the logic of Order of Battle analysis can be translated from military intelligence to civilian organized-crime intelligence in a way that is analytically useful, institutionally realistic, and ethically defensible. The analysis proceeds in three steps.

First, the paper identifies the core components of traditional OOB analysis—composition, disposition, and capabilities—and treats them as portable analytical categories rather than as military operational concepts. Second, it compares these categories with common law-enforcement intelligence practices, including narrative intelligence summaries, social network analysis, crime mapping, and risk assessment tools. The comparison is organized around six criteria: structure, scope, comparability, capacity for updating, clarity of communication, and strategic insight.

These criteria were selected because they reflect recurring weaknesses identified in the intelligence-led policing and organized crime literature: fragmentation, retrospective bias, inconsistent terminology, uneven cross-jurisdictional transferability, and difficulty translating intelligence into decision support. Third, the paper applies the adapted framework to a hypothetical organized crime example to demonstrate how information could be organized, where intelligence gaps might become apparent, and how the framework could support strategic assessment.

The tables in this paper should be read as conceptual demonstrations rather than as empirical findings. They do not measure the effectiveness of OOB in operational practice. Instead, they make explicit the reasoning by which OOB may offer a more standardized and comparative framework for assessing organized crime. Empirical validation, including tests of inter-analyst reliability, operational usefulness, and effects on decision-making, remains a task for future research.

COMPARATIVE ANALYSIS

Current law enforcement assessments of organized crime are frequently supported by narrative intelligence reports, social network maps, and crime heatmaps. These methods can provide valuable operational insights, but they may also offer only partial perspectives, potentially limiting their usefulness for comprehensive, long-term strategic planning (van der Hulst, 2009; Chainey & Ratcliffe, 2013).

Narrative intelligence summaries synthesize available information into descriptive accounts of criminal organizations, often drawing on case files, surveillance logs, and informant interviews (Frost & Morris, 1983). While they offer flexibility, their unstructured format leads to wide variation in detail and may omit information about the group's underlying structure or long-term trends (Parks & Peterson, 2000). For example, a summary might focus on recent drug seizures linked to a syndicate but fail to analyze how its leadership adapts to enforcement efforts (UNODC, 2010).

Social network diagrams visually depict relationships between suspects, facilitators, and associates, highlighting key nodes or potential brokers within a criminal group (Prunckun, 2019). These diagrams help clarify interpersonal connections, although incomplete or outdated data often restricts their analysis. Additionally, they rarely consider organizational skills, logistical capabilities, or geographic distribution (Sparrow, 1991). For example, a

network diagram might show links among suspects in different cities but not illustrate how the network supports coordinated trafficking activities.

Crime heatmaps compile and display incident data across time and space, helping agencies identify hotspots and allocate patrol or investigative resources (Weisburd & Telep, 2014). However, heatmaps typically do not distinguish between organized crime and individual actors, nor do they provide insight into organizational resilience or decision-making processes. A heatmap may indicate an increase in burglaries in a district without revealing whether a specific group is responsible or whether the pattern is coincidental (Chainey & Ratcliffe, 2013; Townsley, 2008; UNODC, 2010).

Collectively, these methods produce useful but often fragmented intelligence. Focusing on incidents and known actors can obscure patterns, such as how groups innovate or recover after enforcement actions (Levi & Maguire, 2004; Sheptycki, 2004; Maguire & John, 2006; UNODC, 2010).

In contrast, the Order of Battle framework provides analysts with a structure for classifying intelligence by composition (who and how many), disposition (where and how organized), and capabilities (what they can do and how effectively). This enables the development of a more comprehensive, comparative understanding of organized crime (Heuer & Pherson, 2014; Brodeur, 2010; van der Hulst, 2009). Table 1 presents a generic OOB template showing how analysts could organize information about any complex organized crime group.

Table 1: Generic OOB Template for Organized Crime Assessment

OOB Category	Attributes	Example Data (Hypothetical)
Composition	Core members, leadership, facilitators	20 core members, 3-tier hierarchy, external financier, corrupt official
Disposition	Geographic activity, operational nodes, mobility	Operating in three cities, with border crossings at two sites, and regular movement of shipments every ten days
Capabilities	Expertise, weaponry, technology, resilience	Advanced concealment techniques, encrypted phones, access to automatic weapons, and adaptability to prior enforcement action

Table 2 compares approaches using the six criteria outlined in the preceding section on the analytical approach: structure, scope, comparability, update capacity, communication clarity, and strategic insight. OOB-based assessments, shown side by side in Table 2, offer a formal structure, consistency, and transparency that help agencies benchmark criminal groups, monitor organizational changes, and communicate actionable intelligence more effectively (Brodeur, 2010).

Table 2: Comparison of Typical Law Enforcement Assessment Methods vs. OOB-Based Assessment

Aspect	Typical Assessment	OOB-Based Assessment
Structure	Informal, variable	Formalized, standardized
Scope	Focused on incidents or individuals	Encompasses group structure, reach, and capability
Comparability	Limited (case-specific, idiosyncratic)	High (repeatable, transferable)
Update/Iteration	Inconsistent, ad hoc	Systematic, modular
Communication	Analyst-dependent, may lack clarity	Transparent, evidence-based
Strategic Insight	Fragmented, retrospective	Integrated, prospective

ILLUSTRATIVE APPLICATION

This section is illustrative. It does not present an operational intelligence assessment, nor does it rely on privileged law enforcement information. It should not be read as a current assessment of the Sinaloa Cartel. The example is used only to demonstrate how the adapted OOB framework could organize information about a complex criminal organization. For that reason, the details are deliberately presented at a high level and treated as hypothetical, even when they reflect themes commonly discussed in open-source literature on transnational organized crime.

Step 1: Intelligence Gathering

The assessment begins by gathering data from various sources, including open-source intelligence (media reports, court documents), law enforcement records, financial investigations, intercepted communications, and field intelligence. Since the Sinaloa Cartel operates across multiple continents and employs various tactics, intelligence gathering would need to account for regional differences, shifting alliances, and the use of proxy actors (Calderón et al., 2015; UNODC, 2010; Felbab-Brown, 2017).

Step 2: Structured Analysis Using OOB

Information is then classified into OOB's three analytical pillars:

- Composition: This involves mapping the internal structure of the cartel, identifying not only its central leadership but also regional managers, specialist facilitators (such as financial coordinators or logistics experts), enforcement teams, and external associates (including corrupt officials and business partners) (Calderón et al., 2015; Paoli, 2014; UNODC, 2010).

- Disposition: Analysts map the group's physical and operational presence, including key strongholds in Sinaloa, major trafficking routes, international transit points, and the use of hidden infrastructure such as tunnels, airstrips, and maritime channels. They track the movement of personnel and resources, showing the cartel's efforts to avoid law enforcement and adapt to market or security pressures (Felbab-Brown, 2017; Grillo, 2021; UNODC, 2010).
- Capabilities: The assessment evaluates the cartel's operational sophistication, including drug production capacity, access to weapons and technology, expertise in money laundering, and the ability to maintain continuity despite leadership losses or territory disputes. Analysts also consider the cartel's resilience, including its track record of adapting to interdictions and shifting trafficking routes (Calderón et al., 2015; Paoli, 2014; Grillo, 2021).

Step 3: OOB Assessment Table

Unlike Table 1, which provides a generic template, Table 3 illustrates how the same categories might be populated in a specific notional case.

Table 3: Illustrative OOB Application to a Hypothetical Sinaloa Cartel Assessment

OOB Category	**Attributes**	**Example Data (Hypothetical)**
Composition	Leadership, core members, facilitators	Multiple senior leadership figures, decentralized command arrangements, regional managers, logistical coordinators, finance specialists, corrupt facilitators, enforcement personnel, and local affiliates.
Disposition	Geographic activity, operational nodes, movement patterns	Primary bases in Sinaloa, major operational presence throughout Mexico, significant transnational reach into the United States, Central America, and Europe; key transit corridors and border crossings; frequent use of clandestine airstrips, tunnels, and maritime routes.
Capabilities	Expertise, weaponry, technology, resilience	Advanced drug manufacturing and distribution expertise, access to military-grade weaponry, use of encrypted communications, capacity for large-scale money laundering, history of rapid leadership succession, demonstrated ability to adapt to law enforcement interdiction and territorial loss.

The OOB approach reveals important features of the Sinaloa Cartel's structure and operations that more traditional intelligence methods may overlook. By mapping relationships among leaders, facilitators, and regional cells, OOB highlights vulnerabilities, such as reliance on specific facilitators or choke points in trafficking networks. The geographic mapping of disposition reveals routes and nodes most at risk of interdiction. The capabilities assessment

helps anticipate how the organization might respond to enforcement actions, such as changing routes or quickly appointing new leaders (Morselli, 2009).

Unlike narrative summaries or network diagrams, OOB's framework emphasizes identifying knowledge gaps, allowing law enforcement to focus future collection efforts. At the same time, its clear presentation helps decision-makers understand what is known and what remains uncertain. Ultimately, OOB enhances the accuracy of resource allocation, targeting, and disruption efforts against complex, adaptive threats (Maguire & John, 2006).

DISCUSSION

Although some law enforcement intelligence practices already reflect aspects of OOB-style assessment, particularly in their attention to group structure, geographic activity, and operational capability, these practices have not commonly been formalized as a standardized OOB methodology. The lack of widespread training, analytical standards, and consistent implementation has therefore prevented the realization of this approach's benefits. Applying Order of Battle analysis can directly address weaknesses in current organized crime intelligence, especially the absence of standardized methods, reliance on outdated data, fragmented strategic views, and ongoing difficulties in delivering actionable insights to decision-makers (Heuer & Pherson, 2014; Carter & Carter, 2009; Brodeur, 2010; Levi & Maguire, 2004).

The paper's contribution is to narrow and standardize a specific component of military intelligence analysis for assessing organized crime. Boyd (2020) demonstrates the broader relevance of Intelligence Preparation of the Battlespace for tactical policing; this paper builds on that insight by shifting the focus from tactical intelligence support to the strategic assessment of organized crime groups. Its distinctive claim is that the OOB categories of composition, disposition, and capabilities can provide a repeatable structure for comparing criminal organizations across cases, jurisdictions, and time. The contribution is not the wholesale transfer of IPB into policing, but the selective adaptation of OOB as a disciplined analytic template for intelligence-led policing.

This distinction is also important because military-derived frameworks can understandably raise concerns about the militarisation of police. Those concerns should be taken seriously, but they do not defeat the argument advanced here. The adaptation proposed in this paper is not a call for police to adopt a military posture toward communities, nor does it imply that organized crime problems should be treated as combat problems. Instead, OOB is used to structure analysis: identifying relevant actors, mapping operational presence, assessing capabilities, and clarifying intelligence gaps. The framework must be subordinated to civilian policing principles, including necessity, proportionality, legality, accountability, and respect for civil liberties. Properly constrained, OOB can strengthen analytic discipline without importing militarised policing practices.

As demonstrated by the Sinaloa Cartel case study, OOB's principal strength is its structured analytic approach. By categorizing intelligence into sections that address

composition, disposition, and capabilities, OOB supports more consistent analytical outputs across investigations and jurisdictions. Unlike narrative reports, network diagrams, or crime heatmaps, which are often informal or specific to individual cases, OOB enables dependable and repeatable comparisons, supporting a broader analysis of organized crime trends and organizational shifts over time (Frost & Morris, 1983; Maguire & John, 2006; Paoli, 2014; Brodeur, 2010).

Furthermore, the structured nature of OOB supports the systematic identification of intelligence gaps. By analyzing a group's internal structure, geographic scope, and operational capabilities, analysts are better positioned to identify missing information, such as unknown regional facilitators, uncharted trafficking routes, or unclear leadership hierarchies. This gap analysis enhances analytical accuracy, aids targeted intelligence collection, and supports strategic operational planning (Heuer & Pherson, 2014; Brodeur, 2010; Paoli, 2014).

Transparency is another key benefit of OOB, as it improves communication with senior decision-makers, oversight bodies, and partner agencies. Traditional intelligence products often lack clarity and accessibility due to their technical complexity or ad hoc nature. In contrast, OOB assessments document sources, analytical criteria, and underlying assumptions, making intelligence processes transparent, accountable, and defensible. Decision-makers can directly connect assessments to specific data points, reducing ambiguity and enhancing the quality and legitimacy of strategic decisions (Ratcliffe, 2016; Sheptycki, 2004; Parks & Peterson, 2000).

Finally, OOB moves beyond retrospective analysis to offer a forward-looking framework. By systematically assessing the organizational capabilities and operational patterns of criminal groups, analysts can predict emerging threats, prioritize strategic responses, and implement proactive law enforcement strategies. This future-oriented ability improves the accuracy of operational planning, enabling police agencies to target key nodes, reinforce vulnerable areas, and allocate resources effectively based on solid, structured evidence (Brodeur, 2010; Maguire & John, 2006; UNODC, 2010).

Having argued these points, the absence of field validation is a limitation of the article rather than an omission in its design. This paper establishes the conceptual basis for adapting OOB to organized crime intelligence; empirical testing of its reliability and operational effects is a separate research task.

POLICY AND PRACTICE IMPLICATIONS

To integrate the OOB framework into policing, law enforcement agencies will need to incorporate it into existing training programs, operational standards, and interagency practices.

First, agencies should develop and implement dedicated OOB modules within their intelligence training curricula at both introductory and advanced levels. Leveraging established methodologies from military intelligence and counterterrorism, these modules

should use scenario-based exercises, structured simulations, and practical debriefings to build analytical proficiency. Formal operational doctrines should clearly outline OOB standards, explicitly defining composition, disposition, and capabilities, and establish ongoing certification processes to maintain consistency and accuracy among analysts (Carter & Carter, 2009; Brodeur, 2010; Lum & Koper, 2017; Ratcliffe, 2016).

Law enforcement agencies should base such training and doctrine development on structured analytic frameworks recognized within the intelligence community. Integrating these structured analytical methods ensures not only rigorous standardization and methodological consistency but also enhances analysts' ability to communicate findings and collaborate effectively across jurisdictions (INTERPOL, 2022).

Second, by adopting OOB as a common analytic framework and standardizing OOB-based reporting across joint task forces, fusion centers, and international collaborations, agencies can communicate more effectively, facilitating shared understanding and coordinated actions against organized crime. Drawing on successful counterterrorism practices, agencies should establish formal interagency agreements that require standardized OOB intelligence products, complemented by regular joint training exercises to reinforce shared analytic norms and build trust across jurisdictions (INTERPOL, 2022; Europol, 2021).

Third, the effectiveness of OOB should be evaluated through pilot studies and ongoing research programs. Law enforcement agencies or specialized task forces could initially pilot OOB methodologies in controlled contexts, such as analyses of regional drug trafficking networks, to evaluate the consistency of analytics, operational impacts, and the effectiveness of resource allocation. Partnerships with universities, criminological institutes, or oversight entities can enhance methodological rigor, ensuring that evaluations provide transparent, empirical evidence to support the broader adoption of the OOB framework (Lum & Koper, 2017).

Lastly, ethical standards and civil liberties considerations should be integral to any implementation of OOB in policing. Because the framework is adapted from military intelligence, agencies must ensure that its use remains within civilian legal and institutional boundaries. OOB assessments should not encourage threat inflation, guilt-by-association, excessive surveillance, or the treatment of communities as hostile environments. Instead, protocols should require evidentiary thresholds, source evaluation, data protection, classification standards, retention schedules, audit trails, and robust access controls. Independent oversight bodies or internal review committees should regularly assess whether OOB products comply with legal, ethical, privacy, and anti-discrimination standards. Embedding these safeguards into OOB practice would help ensure that the framework improves analytical clarity without contributing to militarised policing or undermining community trust.

REFERENCES

Bouchard, M., & Morselli, C. (2014). Opportunistic structures of organized crime. In L. Paoli (Ed.), *The Oxford handbook of organized crime* (pp. 288–302). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199730445.013.015

Bowen, R. J., Halpin, J. A., Russell, P. T., & Staniforth, B. J. (1975). *Tactical order of battle: A state-of-the-art survey* (Technical Paper 265). U.S. Army Research Institute for the Behavioral and Social Sciences.

Boyd, D. (2020). *Intelligence support for tactical policing: Intelligence preparation of the battlespace* [Doctoral dissertation, Charles Sturt University]. Charles Sturt University Research Output. https://researchoutput.csu.edu.au/en/publications/intelligence-support-for-tactical-policing-intelligence-preparati/

Bright, D., & Deegan, S. J. (2021). *The organisational structure, social networks and criminal activities of outlaw motorcycle gangs: Literature review* (Trends & Issues in Crime and Criminal Justice No. 621). Australian Institute of Criminology. https://doi.org/10.52922/ti04961

Brodeur, J.-P. (2010). *The policing web*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199740598.001.0001

Calderón, G., Robles, G., Díaz-Cayeros, A., & Magaloni, B. (2015). The beheading of criminal organizations and the dynamics of violence in Mexico. *Journal of Conflict Resolution, 59*(8), 1455–1485. https://doi.org/10.1177/0022002715587053

Carter, D. L. (2004). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies*. U.S. Department of Justice, Office of Community Oriented Policing Services.

Carter, D. L., & Carter, J. G. (2009). Intelligence-led policing: Conceptual and functional considerations for public policy. *Criminal Justice Policy Review, 20*(3), 310–325. https://doi.org/10.1177/0887403408327381

Chainey, S., & Ratcliffe, J. H. (2013). *GIS and crime mapping* (2nd ed.). Wiley.

Coates, E. N., & McCourt, A. W. (1976). *A questionnaire-based analysis of order-of-battle elements* (Technical Paper 271). U.S. Army Research Institute for the Behavioral and Social Sciences.

Decker, S. H., & Curry, G. D. (2002). Gangs, gang homicides, and gang loyalty: Organized crimes or disorganized criminals? *Journal of Criminal Justice, 30*(4), 343–352. https://doi.org/10.1016/S0047-2352(02)00134-4

European Union Agency for Fundamental Rights. (2017). *Data protection in the police sector: A comparative study*. Publications Office of the European Union.

Europol. (2021). *European Union serious and organised crime threat assessment (SOCTA) 2021*. European Union Agency for Law Enforcement Cooperation.

Felbab-Brown, V. (2017). *Los Zetas Inc.: Criminal corporations, energy, and civil war in Mexico*. Yale University Press.

Freedman, L. (1994). *The evolution of nuclear strategy* (2nd ed.). St. Martin's Press.

Frost, C. C., & Morris, J. (1983). *Police intelligence reports*. Palmer Enterprises.

Grillo, I. (2021). *Blood gun money: How America arms gangs and cartels*. Bloomsbury.

Heuer, R. J., & Pherson, R. H. (2014). *Structured analytic techniques for intelligence analysis* (2nd ed.). CQ Press.

Innes, M. (2014). *Signal crimes: Social reactions to crime, disorder, and control*. Oxford University Press.

International Association of Chiefs of Police. (2021). *Law enforcement use of surveillance and intelligence gathering technologies: Ethical issues and policy considerations*. IACP Policy Center.

INTERPOL. (2022). *Global crime trend summary report*. https://www.interpol.int/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

Johnson, K. D. (1991a). *Intelligence preparation of the urban battlefield*. U.S. Army Command and General Staff College. https://apps.dtic.mil/sti/pdfs/ADA234196.pdf

Johnson, K. D. (1991b). *Intelligence preparation of the theater*. U.S. Army Command and General Staff College. https://apps.dtic.mil/sti/pdfs/ADA251783.pdf

Kilcullen, D. (2013). *Out of the mountains: The coming age of the urban guerrilla*. Oxford University Press.

Levi, M., & Maguire, M. (2004). Reducing and preventing organized crime: An evidence-based critique. *Crime, Law and Social Change, 41*(5), 397–469. https://doi.org/10.1023/B:CRIS.0000039600.88691.af

Lum, C., & Koper, C. S. (2017). *Evidence-based policing: Translating research into practice*. Oxford University Press.

Maguire, M., & John, T. (2006). Intelligence-led policing, managerialism and community engagement: Competing priorities and the role of the National Intelligence Model in the UK. *Policing and Society, 16*(1), 67–85. https://doi.org/10.1080/10439460500399791

Morselli, C. (2009). *Inside criminal networks*. Springer. https://doi.org/10.1007/978-0-387-09526-4

Paoli, L. (2002). The paradoxes of organized crime. *Crime, Law and Social Change, 37*(1), 51–97. https://doi.org/10.1023/A:1013355122531

Paoli, L. (Ed.). (2014). *The Oxford handbook of organized crime*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199730445.001.0001

Parks, D., & Peterson, M. B. (2000). Intelligence reports. In M. B. Peterson, B. Morehouse, & R. Wright (Eds.), *Intelligence 2000: Revising the basic elements* (pp. 121–133). International Association of Law Enforcement Intelligence Analysts.

Pherson, K. H., & Pherson, R. H. (2020). *Critical thinking for strategic intelligence* (3rd ed.). CQ Press.

Prunckun, H. (2019). *Methods of Inquiry for Intelligence Analysis* (3rd ed.). Rowman & Littlefield.

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Willan.

Ratcliffe, J. H. (2016). *Intelligence-led policing* (2nd ed.). Routledge. https://doi.org/10.4324/9781315717579

Shelley, L. I. (2014). *Dirty entanglements: Corruption, crime, and terrorism*. Cambridge University Press. https://doi.org/10.1017/CBO9781139059039

Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology, 1*(3), 307–332. https://doi.org/10.1177/1477370804044005

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks, 13*(3), 251–274. https://doi.org/10.1016/0378-8733(91)90008-H

Stelfox, P. (2007). Professionalizing criminal investigation. In T. Newburn, T. Williamson, & A. Wright (Eds.), *Handbook of criminal investigation*. Willan.

Townsley, M. (2008). Visualising space-time patterns in crime: The hotspot plot. *Crime Patterns and Analysis, 1*(1), 61–74.

United Nations Office on Drugs and Crime. (2010). *The globalization of crime: A transnational organized crime threat assessment*. United Nations.

U.S. Department of the Army. (1994). *FM 34-130: Intelligence preparation of the battlefield*. https://www.marines.mil/Portals/1/Publications/FM%2034-130.pdf

van der Hulst, R. C. (2009). Introduction to social network analysis (SNA) as an investigative tool. *Trends in Organized Crime, 12*(2), 101–121. https://doi.org/10.1007/s12117-008-9057-6

Weisburd, D., & Telep, C. W. (2014). Hot spots policing: What we know and what we need to know. *Journal of Contemporary Criminal Justice, 30*(2), 200–220. https://doi.org/10.1177/1043986214525083

Williams, P. (2001). Transnational criminal networks. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 61–97). RAND Corporation. https://www.rand.org/pubs/monograph_reports/MR1382.html

Wright, D., & Kreissl, R. (Eds.). (2014). *Surveillance in Europe*. Routledge. https://doi.org/10.4324/9781315851365

Xu, J., & Chen, H. (2005). Criminal network analysis and visualization. *Communications of the ACM, 48*(6), 100–107. https://doi.org/10.1145/1064830.1064834

ABOUT THE AUTHOR

Dr. Henry W. Prunckun, BSc, MSocSc, MPhil, PhD, Adjunct Associate Research Professor, Australian Graduate School of Policing and Security, Charles Sturt University, Sydney