

The Tradecraft of Homicide: How Organized Criminal Groups use Intelligence and Counterintelligence to Facilitate Acts of Lethal Violence

Carl Ursing

Carl.Ursing@mau.se

Malmö University

Tony Ingesson

Lund University

Research Article

Keywords: Organized crime, homicide, intelligence, counterintelligence, assassinations

Posted Date: September 9th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10889728/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Homicides committed by organized criminal groups (OCGs) are a high-risk form of criminal activity due to the potential for apprehension and subsequent law enforcement targeting. To facilitate homicides while reducing risk of police detection, OCGs use intelligence measures in homicide planning to locate the target and counterintelligence measures to anticipate, identify, and mitigate law enforcement surveillance. Drawing on 39 instances of homicide planning identified in Swedish police investigations between 2018 and 2024, including evidence from EncroChat, SkyECC, and ANOM, this article examines how OCGs plan homicides from an intelligence and counterintelligence perspective. Using crime-script analysis, each case is analyzed separately by deconstructing it into discrete variables representing the actors, tools, and knowledge involved. The cases are then recombined to identify recurring patterns. The findings show how OCGs employ both long- and short-term strategies to collect intelligence on targets while reducing the risk of law enforcement detection. They also show how OCGs' knowledge of law enforcement methods and surveillance capabilities can be used to anticipate and evade police detection. The study contributes to understanding OCGs as active participants in an intelligence and counterintelligence dynamic with law enforcement, bridging the gap between non-state actors and intelligence practices.

1. Introduction

Organized crime groups (OCGs) operate under conditions of persistent uncertainty (Kleemans & Henk G. van de Bun, 1999). Decisions concerning violence, resource allocation, and organizational security must be made despite incomplete information about law enforcement activities, rivals, and intended targets. The collection, interpretation, and protection of information therefore become essential organizational functions. This is particularly evident during the planning of homicides, where inaccurate information may result not only in operational failure but also in arrest or violent retaliation from other OCGs.

Aware of legal and operational risks (Swanström & Wenngren, 2017; Jacques et al. 2014). OCGs actively adopt their practices to reduce exposure. The ability to collect, manage, and protect information concerning identities, intentions, and activities is important to sustain criminal operations. Contemporary practices, including surveillance and the compartmentalization of violence through peripheral actors, illustrate how intelligence and counterintelligence have become integrated into the operational logic of organized crime (de Korte & Kleemans, 2022; Warburton, 2025).

Although similar information-management practices have been studied among other violent non-state actors, such as terrorist organizations and insurgent groups (Kenney, 2003; Mobley, 2012; Tantalakis, 2019), comparatively little attention has been paid to how OCGs systematically collect, process, and protect information when planning high-risk criminal acts. This gap is partly explained by the limited availability of data capturing the internal operational dynamics of organized crime (von Lampe, 2016). By conceptualizing homicide planning through the framework of intelligence and counterintelligence, the article extends existing research on organized crime.

To examine this question this study makes use of chat logs from EncroChat, Sky ECC, and ANOM, obtained through court proceedings and coded into multiple datasets [Reference redacted to preserve anonymity for peer-review]. The study draws on encrypted communications extracted from Swedish court cases between 2018 and 2024 in a research project that aims to advance empirical knowledge of organized crime in Sweden. The present study focuses specifically on intelligence and counterintelligence practices in homicide planning. Accordingly, the article addresses the following research question:

What types of intelligence and counterintelligence practices are present in the planning of homicides by organized criminal groups in Sweden?

2. Previous literature on the topic

Operational Conditions of Organized Crime in Sweden

Organized Crime in Sweden has changed over recent decades. From approximately 1990s until 2010, OCGs primarily consisted of international motorcycle clubs, such as Hells Angels, and ethnically organized constellations, such as the “Yugoslavian mafia” (Korsell & Larsson 2011; Rostami, 2016; Sausdal and Hannerz, 2025). By the 2010s, internal disputes and legal interventions had weakened and fragmented this structure, leading to more locally based and territorially oriented groups gaining influence (Angerbrandt et al. 2024; Johansen et al. 2026).

Contemporary OCGs are increasingly embedded in specific neighborhoods and local environments, allowing them to establish forms of territorial influence and informal social control (Gerell et al. 2021). Some OCGs have further developed organizational capacities related to local influence, extreme violence, and participation in larger narcotics markets through established transnational connections (Tollin et al. 2022). The evolution has taken place in the broader context of Sweden as a highly digitalized and institutionally transparent society, characterized by public registries, accessible personal information, and open governmental systems.

Contributing to societal transparency, it also facilitates an environment in which personal and organizational information can be accessed and repurposed for criminal intelligence gathering and operational planning. Similar observations are made by Mobley (Mobley, 2012) regarding violent non-state actors, where territorial embeddedness creates a geographically bounded setting, facilitating monitoring of movement, identifying unfamiliar individuals, and awareness of local activities. Such conditions can, in turn, facilitate both intelligence collection and counter-surveillance practices.

Simultaneously, competition over narcotics markets is shown to contribute to escalating levels of violence (Liem & Moeller, 2025). Combined, the dynamics have facilitated the most severe period of lethal inter-group conflict in Sweden’s recent history (Sturup et al. 2019) with firearm homicides increasing from approximately 20 victims annually in the early 2010s to nearly 50 in the early 2020s (Granath, 2024).

A Function-Oriented Perspective on Intelligence

Intelligence studies have traditionally conceptualized intelligence as a function of the state. Yet many of the activities associated with intelligence, such as collecting, analyzing, and protecting information, are also necessary for non-state actors operating under conditions of uncertainty.

OCGs continuously adapt to changing opportunities, law enforcement strategies, and operational constraints by mobilizing people and resources to shape favorable operational conditions (Swanström & Wenngren, 2017; Ayling, 2009). Adaptations depend on the ability to acquire, interpret and protect information relevant to criminal operations. Despite the apparent importance of intelligence and counterintelligence functions in OCG operations, research examining how violent non-state actors employ such practices remains limited.

Definitions of intelligence and counterintelligence vary across the literature (Rønn &

Høffding, 2013), reflecting differences between military, policing and security contexts (Warner, 2013). Historically, the field has been dominated by a state-centric perspective, premised on the notion that only states possess the institutional capacity and resources required to conduct effective intelligence and counterintelligence operations (Prunckun, 2019; Gentry, 2016).

In recent years, however, scholars have increasingly challenged this assumption by conceptualizing intelligence as a set of functions and practices that may be performed by a variety of actors. This is particularly evident in the study of terrorist organizations (Gaetano, 2009; Ilardi, 2009; Kheyre, 2022; Sinai, 2024) guerrilla and insurgent movements (Krause, 1996 Jackson, 2019; Strachan-Morris, 2019a; Strachan-Morris, 2019b) and hybrid or semi-state organizations such as Hizballah (Wege, 2012; Flamer, 2025), which have been shown to use capabilities in intelligence collection, counterintelligence and information management in the protection of clandestine operations.

The present article adopts this more function-oriented approach. Accordingly, intelligence is here defined as the process through which information is collected, processed, and transformed into actionable intelligence that supports operational decision-making (Gill & Phythian, 2018). Counterintelligence is defined as:

“The process, or constellation of activities, analysis, and decision-making, that a group engages in to prevent adversaries from acquiring accurate information about its actions, personnel, and plans”. (Mobley, 2012, p 8)

In practice, both intelligence and counterintelligence operate across two distinct time horizons: strategic and tactical (Dahl, 2013, p 2-3). The purpose and application of intelligence vary depending on which of the perspectives are adopted. Strategic intelligence provides broad, long-term assessments that inform organizational objectives and decision-making, whereas tactical intelligence focuses on short-term, actionable information that supports specific operations, events, or targets. Distinguishing between the temporal dimensions helps capture important nuances in how intelligence and counterintelligence measures are applied, providing additional evidence for understanding their purpose and function.

Intelligence Beyond the State

To sustain operations, criminal groups have to collect information and transform it into actionable intelligence that supports decision-making while simultaneously denying information to adversaries (Mobley & Ray, 2019; Harber, 2009; Kuloglu, 2016; Łabuz and Safjański, 2017). Members routinely collect, interpret and apply information to reduce uncertainty, improve operational decision-making and manage risk (Kenney, 1999).

The dynamic is further intensified by the need for OCGs to continuously engage in criminal activity to generate revenue (von Lampe, 2016; Morselli et al. 2007). Consequently, operational exposure cannot be avoided entirely, requiring groups to continuously balance profit generation against the risk of detection and apprehension. Because organized crime is an ongoing process rather than a series of isolated events, this balance remains dynamic. Changes in law enforcement practices may therefore also produce corresponding changes in criminal behavior and organizational adaptation.

Limited research linking organized crime to intelligence and counterintelligence practices has largely emerged from cartel-focused studies and similarly structured criminal organizations. For instance, Mobley and Ray's analysis of the Cali Cartel (2019) using news reports and various legal documents demonstrate the systematic use of counterintelligence practices, including detection of law enforcement, supported by human intelligence collected through civilian networks. Similarly, Krame et al. (2023) through extensive case investigations show how the adoption of drone technology enhances cartels' real-time surveillance and evasive capabilities during narcotics transportation. Together, these studies suggest that larger and more structurally complex criminal organizations may develop relatively sophisticated intelligence systems that, in some respects, approach the functional characteristics of state-like entities (Kenney, 2003).

However, the concentration of research on highly organized cartel environments introduces a potential bias in literature. The scale, resources, and organizational capacities of cartels may enable forms of intelligence and counterintelligence that are not easily replicated by smaller or less formalized OCGs. It raises questions about whether existing frameworks adequately capture intelligence practices in smaller or less formalized criminal organizations, an issue the article emphasizes.

Studying Intelligence Through Homicide Planning

Homicide represents one of the highest risk activities undertaken by OCGs. The severe legal consequences associated with homicide increase the need for both intelligence generation and counterintelligence measures. OCGs must therefore generate actionable intelligence regarding targets, routines, and vulnerabilities while simultaneously limiting exposure to law enforcement intervention. Recent European studies of OCG-related homicides through subcontracted violence provide empirical support for this assumption. Drawing on police and court documentation from London, Warburton (2025) identifies recurring risk-distancing strategies, including the use of intermediaries and compartmentalized

coordination to create plausible deniability and complicate police investigations. The study also demonstrates systematic efforts to generate actionable intelligence on targets through various forms of surveillance and monitoring. Similarly, de Korte and Kleemans (2022), in their crime-script analysis of contract killings in the Netherlands, document the use of encrypted communications, surveillance technologies, and subcontracted violence to create organizational distance between planners and perpetrators.

Materials

The study draws on material from a research project that aims to advance empirical knowledge of organized crime in Sweden [Reference redacted to preserve anonymity for peer-review]. The project is based on the systematic collection of court documents and police investigation records from 2018 to 2024, including encrypted communications obtained from EncroChat, Sky ECC, and ANOM. While EncroChat and SkyECC were commercial services later breached by European authorities, ANOM is a platform covertly operated by U.S. law enforcement to directly monitor criminal coordination. This means that the material provides a rare opportunity to examine the entire progression of a crime.

The material primarily concerns the organizational dynamics of OCGs operating in Sweden. OCGs are identified by the Swedish Police using the European Union's 11-point framework for organized crime classification (Korsell & Larsson, 2011). The framework requires the presence of at least six criteria, including four mandatory elements: collaboration between more than two individuals; activities conducted over a prolonged or indefinite period; suspected involvement in serious criminal offences; and the pursuit of profit and/or power (Polismyndigheten, 2025). The project material today consists of (n = 189 court cases) detailed OCG descriptions and direct message exchanges, corroborated by formal police investigations. Court cases represent prosecution and police establishing guilt in criminal cases through various investigative methods, often ranging from before the crime until its aftermath.

This means that the material provides a rare opportunity to examine the entire progression of a crime (i.e., planning, execution, and post-offence). By capturing interactions, the project addresses the empirical limitations of the field, enabling an in-depth analysis of how organized crime manifests in the everyday practices of its members (von Lampe, 2016).

Sample

The final analytical sample consists of 39 homicide planning events identified across 21 Swedish court cases. Cases were selected through a systematic three-stage sampling procedure from the project database (n = 189 court cases).

To create the sample, the material was sampled according to a three-step process: First, the project database (n = 189 court cases) was systematically screened using the keyword *homicide*. The search included completed homicides, attempted homicides, and conspiracy to commit homicide, yielding an

initial sample of 45 court cases containing homicide-related offences. Following De Korte and Kleemans (2022), the analytical focus is on the planning process rather than the criminal outcome. Consequently, attempted homicides and conspiracy offences were included, as they often reveal the same intelligence gathering, coordination, and operational decision-making processes as completed homicides. Secondly, each case was then reviewed to determine whether (1) the offenders belonged to an organized crime group as defined within the project database and (2) the homicide involved coordination between members of the same OCG. This criterion ensured that the analysis focused on organizational decision-making rather than violence committed by individuals acting independently. Finally, the remaining cases were assessed to determine whether the available court documents and police investigations contained evidence that homicide planning had progressed beyond the initial expression of intent. Cases were retained only when they contained evidence of coordinated preparatory activities, including resource acquisition, role allocation, or logistical planning. Cases consisting solely of vague threats or undeveloped discussions without subsequent operational planning were excluded (n = 6).

The resulting sample captures homicide planning that progressed beyond intention into coordinated organizational action, providing an empirical basis for analyzing intelligence and counterintelligence practices during the planning of homicides.

Method

To analyze intelligence and counterintelligence activities during homicide planning, this study employs Crime Script Analysis (CSA). Crime Script Analysis enables complex criminal events to be analyzed as a sequence of interconnected actions (Snaphaan, 2025), providing a framework for analyzing how activities are organized across different cases. Drawing from Script-Analysis in cognitive psychology, Cornish (1994) introduced the script-theoretic approach to criminology as a means of analyzing how, during different progressions of the criminal event, actors, activities, resources, and settings interact to facilitate the crime's continuation. By deconstructing crimes into their constituent stages and component parts, such an analysis provides a broad systematic insight into what goes into a crime and how it is facilitated (Cornish, 1994; Borrión, 2013). In an OCG context, Crime-Script also have added value, as such crimes typically involve multiple actors, specialized roles and extended periods of preparation.

As of today, crime scripting has been applied globally to analyze a wide range of complex crime types, including smuggling (Morgenthaler & Leclerc, 2023; Bish m.fl., 2024; Langlois et al. 2022) cybercrime (Choi et al. 2024; Madarie et al. 2024; Madarie et al. 2025), money-laundering (Snaphaan and van Ruitenburg, 2025; Gilmour, 2023; Wang, 2025; Levi and Soudijn, 2020), and subcontracted homicides (de Korte & Kleemans, 2022; Warburton, 2025).

However, an ongoing conceptual debate within the crime scripting literature concerns whether a standardized model should be applied across crime types (Tompson & Chainey, 2011) or whether scripts should remain flexible enough to accommodate the specific characteristics of different offences (Borrión, 2013). Although this debate remains unresolved, the principal aim of crime scripting is consistent: rather

than detailing single instances or the actions of individual offenders, crime scripts are analytical abstractions that capture recurring patterns across multiple cases (Cornish, 1994; Snaphaan, 2025). Accordingly, the scripts developed in this study are understood as analytical representations of recurring planning activities rather than fixed behavioral sequences.

Although approaches to script construction vary across studies, most crime scripts are built around a common set of analytical components: scenes, roles, activities, and props (Cornish, 1994). Scenes represent distinct stages in the criminal event, each organized around the achievement of a specific sub-goal, such as planning a homicide or disposing of evidence. Within each scene, roles refer to the actors who perform the actions required to advance the offence. Activities comprise the behaviors and decisions undertaken to achieve the objectives of each scene, while props denote the resources, tools, skills, and know-how employed throughout the criminal process (Snaphaan, 2025). Having established CSA as the analytical framework, the following section describes how the method was operationalized to the current study.

Operationalizing the current study

To operationalize the crime-script framework, 39 instances of homicide planning identified across 21 Swedish court cases were used. While majority of cases involve investigations and prosecutions related to planned or completed homicides, some also encompass associated offences, such as aggravated weapons offences. All cases contain police investigation materials that include encrypted communications recovered from the EncroChat, Sky ECC, and ANOM platforms, involving a total of 171 unique user accounts. The dataset originates from the project and consists of cases in which homicide planning progressed beyond the expression of intent into coordinated preparatory activity. The basic unit of coding was the planning activity. Individual chat messages, intercepted communications, and other case material were interpreted in context and coded according to the activity they documented rather than as isolated observations.

Among the various approaches to crime scripting, the study adopts the framework proposed by Tompson and Chainey (2011), which is particularly suited to the analysis of fragmented data, such as encrypted communications. The framework structures analysis around broad temporal scenes: Pre-Activity; Activity & Post-Activity while maintaining flexibility in interpreting incomplete or discontinuous sequences of events as shown in Table 1.

Act	Planning of Homicide Table. 1			
Scene	Preparation	Pre-Activity	Activity	Post-Activity
Content	Initiating the act	What happens before the main activity	The main activity	What happens to finalize the act?

The framework has previously been applied to the study of organized crime in contexts such as illegal waste management (Thompson & Chainey, 2011) and oil theft from pipelines in Mexico (Berbotto &

Chainey, 2021). In both studies, researchers drew on private-sector sources and OSINT, including news reports and internal documents, to systematically reconstruct the actors, tools, knowledge, and activities involved in the criminal events.

In practice, most measures deliberated were initiated during the pre-activity scene (*operational planning*) and are then used or altered throughout the rest of the planning process. This is where most observable intelligence and counterintelligence interactions occurred in the context of formulating the *how's* before acquiring necessary resources, displayed in Table 2.

Act	Planning of Homicide Table. 2			
Scene	Preparation	Pre-Activity	Activity	Post-Activity
Content	Initiating the act	Operational Planning	Acquisition of resources	Storage of Resources

During the pre-activity stage, orchestrators in the planning process deliberated over available options of carrying out the homicide, including the selection of personnel and equipment. Perceptions of risk shaped deliberations, encompassing both the acquisition of necessary resources and the management of those resources during and after the offence.

The analysis proceeded iteratively through repeated comparison of planning activities across all homicide planning events. Activities sharing the same operational purpose were progressively grouped into broader analytical categories. The categories emerged inductively through repeated comparison across cases before being interpreted using the function-oriented intelligence framework. For example, usage of different social-media platforms to find out information about the target are combined under the category “social media monitoring,” grouped to the shared function in locating and monitoring target. Lastly, to illustrate the findings, translated anonymized excerpts from the chat logs are included when deliberating the various categories.

3. Actionable knowledge on targets

To support the planning of a homicide, participants discuss a range of data collection methods during the pre-activity (operational planning) stage of the crime script. The methods selected are subsequently used throughout the planning process to generate, analyze, and share information among participants.

By identifying recurring patterns across the empirical material, four categories of measures were distinguished and are presented below in order of frequency displayed in Table 3.

Recurring patterns of Intelligence use across the empirical material Table. 3				
Method	Lookouts	Public registries	Social media	GPS-tags
Number (n) of cases (%)	(n:24) (62%)	(n:17) (44%)	(n:21) (56%).	(n:9) (23%)

The process is used to identify a target's movements, routines, and social environment. Multiple methods are often combined to enable triangulation. Based on insights, targets are mapped using various practices to assess when they may be isolated, unaware, or otherwise vulnerable.

Generally, Intelligence is primarily oriented toward immediate operational needs instead of continuous production, suggesting a predominantly tactical use of intelligence, closely tied to specific targets and events. Methods are selected through interactions among OCG members and implemented in different ways, varying between human, open source, and geospatial Intelligence. Usage extended beyond the initial operational planning stage, with repeated use throughout the crime-scripted homicide planning process to support the identification, continuous monitoring, and triangulated verification of intelligence.

Lookouts

The most frequently observed method of intelligence collection involves the use of lookouts tasked with monitoring targets, locations, and surrounding environments, 24 cases (62%) where one or several orchestrators explicitly stated to use lookouts to scout for the target. In the material, this is for example expressed as

"I have all my active ones out looking. They need to be found." (Göteborg tingsrätt, B 533-21, aktbilaga 360, p 27)

Individuals tasked as lookouts are typically younger or lower-ranking members of the OCG or individuals indirectly connected through affiliated subgroups. Personal information on lookouts is limited in the project material. In chat logs, lookouts are rarely identified by name and instead appear primarily through references to operational functions. Likewise, related police investigations provide little or no detail regarding who they are suspected to be, in the context of identity or background. Nevertheless, they appear to be mobile resources that can carry out surveillance tasks.

Lookout activities are generally positioned at the periphery of the broader homicide operation. Rather than participating directly in operational planning, lookouts primarily occupy street-level roles embedded within local social environments. Intelligence collection is thus often integrated into everyday activities rather than conducted as a separate or specialized task. Many appear to be tasked with lower-level criminal activities, such as local narcotics distribution, placing them in positions where they can observe movements, identify unfamiliar individuals and monitor relevant locations. Up-to-date knowledge of the criminal environment seems well established here, enabling them to provide in-depth information that otherwise would be hard to come by:

"Bro, the Askim kids say if you camp outside that guy Oliver there is a big chance that Terror and Henno will be there when they shoot him. They said all they are waiting for is a car so... We can camp there 3-4 days, if it doesn't work, then one of the Askim kids will call him out and get him out." (Göteborg tingsrätt, B 1343-21, aktbilaga 429, p 7)

Through this social embeddedness, lookouts provide OCGs with an extended observational capacity rooted in familiarity with local environments and social networks. Their effectiveness derives not only from numbers but from an ability to blend intelligence collection into routine interactions and activities. Consequently, lookouts contribute to a dispersed form of intelligence collection, where observations are continuously relayed upward within the organization.

The material further suggests that lookouts often operate with considerable autonomy. Instructions are typically minimal and limited to general directives such as monitoring locations, remaining vigilant or confirming sightings. The relative absence of detailed operational guidance indicates reliance on shared situational knowledge and familiarity with local contexts rather than formalized surveillance procedures.

In some cases, however, lookout functions become more explicitly task oriented. Individuals may be instructed to monitor specific addresses, entrances, or vehicles to provide real-time verification of a target's location or movements:

"Bro, do you know exactly which gate it is?"

"Yes"

"Good. Bro, now sit there and check" (Halmstad tingsrätt, B 1486-19, aktilaga 583, p 34)

Although the material provides limited direct evidence regarding how targets are initially identified by lookouts, the findings suggest that identification often relies on the circulation of information through communication channels not captured in the encrypted material, for instance, Telegram, Signal & WhatsApp. Consistent with the broader pattern of triangulation observed across cases, lookout observations are typically combined with other forms of intelligence collection, including social media monitoring, public registries, and direct communication between members:

"And yes, bro, I can spy on a guy, no problem. Do you have a picture, address, and stuff like that on him?" (Göteborg tingsrätt, B 9641-21, aktilaga 144, p 120)

Social Media

Social media platforms make up a central source of intelligence collection during homicide planning (n=21) (56 %). Across cases, OCGs systematically monitor platforms such as Instagram, Facebook, and Snapchat to collect information regarding targets' locations, routines, social relations and everyday activities that can then be shared in the planning process:

"Bro, can you look up a guy on Facebook and screen capture an image of him? Preferably from someone else's phone." (Helsingborg tingsrätt, B 108-22, aktilaga 32, p 1066)

By design, social media platforms encourage the public display of identity, lifestyle and social interaction, thereby generating substantial amounts of accessible behavioral information (Andrews et al. 2018). In criminal environments, where status signaling and public self-presentation may hold particular

importance, such platforms provide valuable operational intelligence regarding movements, associations, and patterns of activity (Fernández-Planells, et al. 2021). Monitoring social media, therefore, constitutes a comparatively low-risk and accessible form of surveillance. In many cases, intelligence collection begins with minimal initial information, such as a name, alias, or known associate. From there, extended social networks can be explored through friend lists and follower connections:

"[Picture of a person] One of the Turks with the bastard." "Send it with an arrow so it can be downloaded. What's his name"

"How do you do it brother? [The Target] is called Seko"

"Take the picture then swipe right to the arrow. Instead of the eye. You see it far down on the left"
(Södertörn tingsrätt, B 9452-22, aktbilaga 43, p 131)

The process enables the reconstruction of social environments and everyday routines, including frequented locations, vehicles, recurring contacts, and behavioral patterns. Furthermore, in practice intelligence is collected by multiple members in different roles of the OCG, either directly involved in the operation or tasked with specific collection activities, such as locating and monitoring relevant accounts. The material further indicates that social media monitoring is not confined to the preliminary stages of planning. Once initiated, monitoring often continues throughout the operation as members repeatedly update information in response to newly published content. This continuous flow of information is particularly valuable in cases where targets have mobile lifestyles, travel frequently or regularly changing locations. Likewise, it provides evidence of changes in the targets' behavior that contributes to the operational assessment:

"[The Target] has started filming only his feet on Snapchat and doesn't post as much" (Malmö tingsrätt, B 9477-21, aktbilaga 10, p 358)

Social media monitoring is also combined with other forms of intelligence collection. Information collected online is frequently cross-checked against physical observations, reports from lookouts and other sources of intelligence. Digital and physical surveillance measures are therefore used in parallel to triangulate information and increase confidence in operational assessments.

In some cases, social media platforms are also used more actively to influence or manipulate targets. False information may be communicated through fake accounts to generate distress, shape movement patterns or alter behavior in ways that create favorable operational conditions for the planned attack.

"Make a fake Instagram [...] Write exactly like this bro, to one of them from a fake account: 'Bro, we know each other, but don't want to involve myself in crime, don't want to get involved in this, but saw the whore "tjockisen" and another one behind the Norra Dragspelsgatan last night and they had a radio, the kind that the police have. They walked up from the back of the villas, the other one I didn't see he had a balaclava, but he might have been Swedish.' Write like this to someone's insta from a fake account bro they'll panic."
(Göteborg tingsrätt, B 1343-21, aktbilaga 223, p 166)

Attempts to manipulate targets indicate an increased sophistication in how to facilitate homicides, signaling increased operational competence (Mobley, 2012). On the other hand, it also directly increases the risk of the plan being uncovered if poorly executed, thus adding more risk while simultaneously facilitating the execution of the plan. Successfully influencing a target's behavior requires prior knowledge of their routines, preferences and likely responses, which in turn depends on intelligence collected through other methods. Thus, active manipulation is arguably both information-intensive and more exposed to failure or detection, indicating a breaking point of sophistication for some OCGs.

Public Registries

Under Sweden's Fundamental Law on Freedom of Expression, private actors may obtain so-called publication certificates, which grant constitutional protection to certain online databases (Mediemyndigheten, n.d.). As a result, the databases are exempt from key provisions of the General Data Protection Regulation (GDPR), particularly those regulating the processing and dissemination of personal data.

The legal framework enables commercially operated registries that provide extensive personal information, including residential addresses, telephone numbers, vehicle ownership, and in some cases, details about family members, associates, and cohabitants. These are used extensively by OCGs to map their targets (17) (44%):

"Isn't he the Syrian who owned the bar?"

"Ahh yeah that's him."

"But he's just a normal guy? What the hell does he have to do with Ali?"

"I don't know, I think I saw him bro, I'm not sure"

"But is the car Ali's or the Syrian's?"

"It's registered on the Syrian bro." (Örebro tingsrätt, B 5057-20, aktilaga 610, p 255)

Although justified in terms of transparency and freedom of expression, chat logs indicate that publicly accessible registries are systematically exploited in the planning of homicides to collect operational information on targets:

"[Sends image] BMW that's the rats' new car, and the Golf is his old. Both appear to be registered to someone in his family, as the car seems to be registered to someone in Vårby" (Södertörn tingsrätt, B 9452-22, aktilaga 43, p 116)

By combining information such as vehicle ownership, residential addresses and kinship ties, members can map not only the primary target but also their extended social and familial environments. It significantly enhances the capacity for spatially informed and temporally precise surveillance. The material suggests that registry-based intelligence collection primarily occurs in two forms. First, registries are used iteratively to expand limited initial information into broader operational knowledge. A name, vehicle registration number or known associate may serve as an entry point from which additional

information is extracted and cross-referenced across multiple databases. Through this process, members reconstruct relational ties, identify associated addresses, and connect individuals to vehicles or locations relevant to the operation:

“Within a week, [The Target] will be out of the hospital, then we go with a car and mow them down. [Registration Number]. Their registration on their BMW. Oh, and don't look it up from your phone”

“What do you want me to check?”

“Just saw it. I'll go and see if it's in the parking lot”

“[Sends image]” (Södertörn tingsrätt, B 20229-21, aktilaga 697, p 3)

Second, registries are used more situationally to verify information in real time. Members frequently cross-check observations made during surveillance activities, such as confirming vehicle ownership or identifying individuals connected to a specific address:”

“[Several license plate number] Check those. Parked outside [the Target's] father” (Göteborg tingsrätt, B 1343-21, aktilaga 223, p 23)

Like social media monitoring, the use of public registries contributes to the reconstruction of everyday routines and social relationships. In several cases, registry data revealed otherwise informal arrangements, including temporary living situations, romantic relationships, or recurring interpersonal contacts. Registry data, therefore, functions not only as static background information but also as a means of contextualizing and interpreting observations collected through other forms of intelligence collection. Importantly, the use of registries rarely appears centrally coordinated or formally instructed. Instead, registry searches are treated as routine and taken-for-granted practices embedded within broader intelligence collection activities. Knowledge regarding which databases to use and how to extract relevant information appears widely distributed among members.

GPS Trackers

GPS trackers are, in some instances, deployed to monitor vehicles associated with intended targets featured in 23% of the cases. The primary function is to enable near real-time tracking and the reconstruction of movement patterns over time. By generating continuous location data, GPS tracking contributes to the spatial and temporal identification of routines and operational vulnerabilities and provides real-time data on the target's whereabouts, in comparison to more situational observations:

“Is that Q7 his or does he drive a BMW? Never heard of the Q7. Who has that GPS?”

“The Yugoslav”

“Can they get over there and put it on he will leave soon” (Malmö tingsrätt, B 9477-21, aktilaga 26, p 562)

While similar types of devices are used across cases, acquisition patterns vary. GPS trackers are obtained through mainstream e-commerce platforms, local electronics retailers, and vendors specializing in surveillance equipment, similar to findings on contract killings in the Netherlands by de Korte & Kleemans (2022). Differences in procurement and types, however, appear to have a limited impact on operational use. Despite prominence in Swedish media portrayals (Larsson, 2019), where GPS use is often framed as indicative of technologically sophisticated or “spy-like” criminal operations, the empirical material points to a more limited and practical usage. Rather than functioning as indispensable or highly sophisticated tools, GPS trackers primarily serve as supplementary, although important, sources of intelligence collection. In most cases, the devices are used to confirm, refine, or extend intelligence already obtained through other forms of surveillance:

“He with family, but think he sleeps there from now and then” “Don't know if they are still together anymore but worth checking”

“Maybe GPS her car she might sleep with him”

“Okay bro” (Göteborg tingsrätt, B 1359-21, aktilaga 884, p 66)

Thus, usage is primarily facilitative rather than transformative, assisting in confirming or refining information obtained through other methods while enhancing situational awareness and a sense of operational control among orchestrators. Seldom, as observed in the chats, was the GPS used as a catalyst to initiate a homicide. If this came down to uncertainty of signal (for instance, if the GPS had been manipulated), or the perceived need to triangulate information is, however, difficult to ascertain.

The deployment of GPS trackers, however, introduces significant risks. Unlike other methods of intelligence collection (e.g., social media, public registries), GPS devices must be physically attached to a target's vehicle. Installation requires possible interaction with the target and increases the likelihood of exposure or detection. Consistent with patterns observed throughout the material, this is frequently delegated to younger or lower-ranking members:

“Bro, here's the plan, you're there around 2 o'clock, you go straight to check if the car is there and if it is, you GPS-tag it.” (Solna tingsrätt, B 10412-22, aktilaga 403, p 57)

The effectiveness of GPS tracking must also be understood in relation to the characteristics of the target population. In OCG contexts, targets are often embedded in criminal milieus, which may heighten their situational awareness and sensitivity to surveillance and counter-surveillance practices. In some cases, this awareness contributes to the use of counter-surveillance measures such as signal jammers or equipment intended to detect tracking devices. Consequently, the use of GPS trackers may paradoxically increase operational risk by introducing opportunities for detection that would not arise through less intrusive methods.

4. Counterintelligence and Risk Mitigation

To avoid detection and apprehension, OCGs rely on knowledge of policing practices as well as the legal and procedural frameworks that shape them. Counterintelligence in this context consists of a range of measures designed to limit exposure and divert police attention. The effectiveness of these measures depends on how accurately actors understand the ways in which the police collect and interpret information, as deficiencies in understanding can lead to misdiagnosis of threats (Ratcliffe, 2009; Clark, 2026, p 237-238).

Across cases, recurring counterintelligence methods were identified and condensed into four central practices, as shown in Table 4.

Recurring patterns of Counterintelligence use across the empirical material Table. 4				
Method	(Getaway)Vehicles, False License Plates & Signal Jammers	Systematic reporting on police surveillance and resources.	Manipulating evidence	Distractions
Number (n) of cases (%)	39 cases (100%)	27 (69%)	16 (41%).	7 (18%)

In contrast to intelligence collection, which is primarily tactical and case-specific, many counterintelligence practices operate at a more strategic level and extend beyond individual homicide events, while also being adapted to specific stages of the crime script. During homicide planning, specific measures are aligned with different stages of the event, including distancing actors from the offence, minimizing traceable connections, destroying forensic evidence and complicating identification (e.g., through the use of false license plates).

Collectively, these practices undermine police capacity to detect, attribute, and reconstruct criminal activity, both during the commission of the offence and in subsequent investigations.

(Getaway)Vehicles, False License Plates & Signal Jammers

All cases involve the planned use of vehicles to transport offenders in ways that minimize traceability. Various methods are employed to remove direct association with members of the OCG, allowing their use of vehicles to remain inconspicuous during both planning and execution. Vehicles play a significant role in the operation by enabling the rapid transport of the shooter to and from the crime scene, minimizing time

spent at the location and facilitating swift movement to a safe area. In most cases, both assembly points and target locations are situated in the same city, though often in different districts.

Used vehicles are almost exclusively cars, ranging from high-performance models (e.g., Audi RS variants) to more ordinary vehicles obtained through illicit markets, intermediaries, or other OCGs. From an operational perspective, vehicles are treated as disposable assets. In most instances, vehicles are intended to be destroyed, typically by burning, immediately after the homicide, further limiting forensic and investigative opportunities:

“Need vehicles, mopeds, motocross, stolen cars. Anything. Who sells?”

“Do you want to buy stolen cars??”

“Yes bro, or motocross or vespas or e-scooter. Just cheap ones you can use for action then dispose of.”
(Göteborg tingsrätt, B 533-21, aktilaga 360, p 115)

Considerable effort was dedicated to ensuring that vehicles did not attract attention in the period between acquisition and use. This often involved storing them in enclosed or semi-private locations, such as garages linked to fronts. However, mismatches between the vehicle type and its environment, for example, high-performance cars parked in low-visibility or economically deprived areas, could inadvertently increase suspicion, thus requiring some insight into different locations where parking is acceptable:

“Okay bro, write when I'm on the way back”

“Yes, my friend”

“I'll be on the way in 10”

“[voice call]”

“The car is in that parking lot. We need to move it again brother to a garage in Högsbo but we can do it tomorrow morning.”

“Alright bro.” (Göteborg tingsrätt, B 1359-21, aktilaga 884, p 76)

To further obscure identification, vehicles are frequently fitted with false license plates, with registration numbers not overlapping with what is registered on the car. The acquisition of false license plates appears varied. False license plates are obtained either through theft from other vehicles, bought from other criminal actors, or produced through contacts with access to relevant materials and equipment, such as metal workshops:

“Listen, if we don't find anything, he'll have the guy fix the license plates, don't steal them, fix the signs at a sheet metal workshop, it usually doesn't cost more than 1k, same color as the car and same model”
(Göteborg tingsrätt, B 1343-21, aktilaga 233, p 54)

In instances with license plates from outside Sweden, origin is particularly Eastern European countries (especially Poland). The reason this region is preferred is not distinguishable in the chat-logs nor the investigative material, but a suggestion in line with preventing investigative possibilities, reflects the increased difficulty of cross-border verification. The use of false plates, often installed shortly before the operation, is assumed to complicate efforts by the police to trace vehicles and link them to specific individuals:

“And bro, very, very important to remove the license plates before they drive the car 1 millimeter, bro. If there are Swedish plates on the car, let them just change them. And throw the Polish plates in the forest, and someone will come and take them.” (Örebro tingsrätt, B 5057-20, aktilaga 610, p 300)

Also linked to vehicles is how, in some instances, signal jammers are used to disrupt tracking technologies suspected of being fitted on some cars in the immediate vicinity of the operation. It seems to overlap with vehicles both bought or rented to facilitate earlier parts of the operation. Although references remain limited, such practices suggest an understanding that the police or rival groups may themselves employ tracking technologies during investigations or conflicts. Reasonably, making use of tracking technologies also contributes to awareness of technologically facilitated surveillance and how to counter it:

“Okay, sorry, writing to my friend to pick up the machine [counter-surveillance equipment] so you can check if he has installed a GPS. For the GPS that's in the car, that's just GPS [location]. If they're on to us now, they'll install a GSM so they can hear it too [sound-receiver]” (Solna tingsrätt, B 10412-22, aktilaga 403, p 33)

Systematic reporting on Police surveillance and resources.

In the material, OCG members in 27 cases (69%) demonstrate a high degree of situational awareness of police activity and the importance of limiting the information that the police can collect about them. Although intelligence collection on police activity is rarely described explicitly in the chat logs, complementary material in the context of narcotics dealing in the broader project dataset shows cases of relatively systematic monitoring practices. This includes the coordinated reporting of police presence, with participants documenting both marked and unmarked vehicles through detailed descriptions (e.g., license plates, colors, and models). Collectively, it contributes to an informal but functionally significant intelligence system concerning police deployment and surveillance patterns that shape operational conduct:

“There has been a lot of activity around the old town of Kortedala, I don't know if they have anything to do with it, but they stop every car there, and the cops have had checks there several times in a row now.” (Göteborg tingsrätt, B 1343-21, aktilaga 429, p 101)

Through repeated reporting and circulation of observations, members develop shared assessments regarding where police resources are concentrated, which locations may be under heightened scrutiny,

and which individuals may currently be subject to surveillance, resulting in heightened or lowered periods of activity, both individually and organizationally:

"But it is important that everyone is awake now and has eyes in the back of their heads, if you see or feel that you have the police on your ass, you postpone the task you have until you have ducked the surveillance." (Göteborg tingsrätt, B 1359-21, aktilaga 884, p 98)

The circulation of information, sometimes regarding specific police officers, further suggests that orchestrators hold operational value in identifying and recognizing detailed information. Counterintelligence practices, therefore, extend beyond generalized awareness of police activity toward more individualized assessments of investigative actors and surveillance capabilities:

"It's really weird. They only did the company, right? Not the apartments or anything. You should put a mic in Pelle's [police officer] home and car. Fucking whore. Do you know who the operation leader is? Fuck their mother bro, they're getting closer and closer."

"Mattias, I think his name was. We should pay them back, blow up some cop houses." (Helsingborg tingsrätt, B 108-22, aktilaga 35, p 195)¹

Members also routinely circulate warnings regarding "hot" individuals, vehicles or locations believed to be under active surveillance. Assessments are based both on direct observation and on inferences drawn from recent police interventions or changes in policing patterns. Such practices illustrate how collective interpretations of risk are continuously produced, negotiated, and operationalized in the OCGs:

"Park it in the free parking lot then and make sure no one else sees you park it there."

"Well, bro, it's fine, no one has seen me, but I understand what you mean."

"Bro, I have 24-7 surveillance on me, if you came to the club, just make sure no one else sees where you park it, so they don't put GPS. (Norrköping tingsrätt, B 308-20, protokollaga, p 112)

Further, material indicates identifiable organizational patterns in how this information is managed. Members occupying orchestrating roles or leadership roles frequently receive, interpret, and spread intelligence to participants. Operational responsibilities also appear shaped by perceptions of police visibility and exposure. Individuals believed to attract police attention due to prior police interactions or local recognition are, in some cases, assigned different operational tasks or partially excluded from sensitive activities.

Manipulating forensic evidence

The counterpart to intelligence collection on the target is the anticipation and mitigation of forensic detection after the offence. Identifying vulnerabilities during earlier phases of information collection,

OCGs appeared in 16 cases (41%) to anticipate forensic risks either through prior experience or by accessing public court records:

"Bro, we have had contact on Wickr so throw away your phone. Break it and throw it away. Same with the Encro. Break it and throw it away in different places. Or burn it." (Helsingborg tingsrätt, B 108-22, aktilaga 32, p 828)

In most cases, this includes the use of gloves, face, and head coverings, as well as disposable clothing to reduce both visual identification and the transfer of trace evidence, such as gunshot residue or DNA. Items requiring destruction or removal, including clothing, weapons and vehicles, are often handled by peripheral or auxiliary actors rather than by the primary perpetrators. This organizational separation contributes to operational distancing by limiting direct links between offenders and post-offence evidence management:

"When should we start camping?" "As soon as I've planned my escape route and someone who burns the clothes" (Göteborg tingsrätt, B 1343-21, aktilaga 429, p 137)

Destruction of items linking individuals to the crime is typically planned in advance, including decisions regarding responsibility as well as the location and method of disposal. Execution is usually carried out as soon as possible after the homicide, with selected individuals tasked to implement planned steps immediately following the event. Such urgency reflects an awareness that the period immediately after a crime is critical for forensic linkage and that rapid action can significantly reduce investigative opportunities:

"Okay, but those who torch [the evidence] should be in place, and someone who drives behind us and the goare [person who lures the target out]" (Örebro tingsrätt, B 5057-20, aktilaga 610, p 277)

Practices appear informed by accumulated knowledge of investigative procedures and forensic techniques, suggesting a degree of experiential learning and adaptation. Often aligned to established modes of effectively removing crucial evidence through steps of sequential mitigating actions, the standardization suggests reuse of established routines. The coordinated removal and destruction of evidence thus may indicate a structured approach to post-event risk mitigation that may extend beyond homicide to other forms of criminal activity:

"Okay brother, they're easy to find, it's really perfect there to burn the car, then after you go towards Linköping, drive past the Ingelstad exit and turn off at the 'Klocket' exit, then to Ektorp and home to 50, there take a quick shower, then just continue home" (Norrköping tingsrätt, B 308-20, protokollbilaga, p 168)

Similar methods appear regardless of items. Vehicles used during homicides are frequently intended to be destroyed shortly after the attack. Preparations for destruction include pre-positioning fuel in PET bottles placed in specific places. Smaller items, such as clothing, are similarly disposed of through

burning and, in some cases, then buried. Both typically take place in secluded environments located either in or outside urban areas, such as rural or wooded areas.

It is however not observed how the offenders dispose of weapons after usage. Evidence from chats suggests weapons are less obtainable and at the same time hard to get rid of in a safe way. Instead, it can only be assumed that these are cleaned and, in some cases, resold to other parts of Sweden, where it is harder to trace them back to the offending OCG.

Distractions

Distractions occurred in 7 cases (18%) and constitute an active form of counterintelligence where OCGs attempt to redirect police attention immediately prior to, or during, the execution of a homicide.

Unlike measures primarily aimed at concealment or avoidance, distractions seek to manipulate police deployment by creating incidents that demand immediate operational response:

“We'll blow it up at 6pm. Then all the police and surveillance will have their focus elsewhere.” (Helsingborg tingsrätt: B 108-22, File appendix: 32, p 348)

Distractions may take the form of gunfire in public locations or vehicle explosions, events that resemble serious violent incidents and are therefore likely to trigger rapid and substantial police responses. Rather than minimizing visibility, distractions exploit the response by overwhelming or redirecting police attention, creating temporary gaps in coverage that can be used operationally.

Responsibility for distraction activities is generally assigned either to members involved in the broader operational planning or to lower-ranking individuals tasked with carrying out the diversion without full knowledge of the wider operation:

“Bro, can you blow up a car in Hagelby at the same time to lure the cops there, it's really easy bro, it's like an XL-Banger. Just light the fuse then after 3 minutes it goes off, you'll have time to go home and roll one before it goes off.” (Norrköping tingsrätt, B 308-20, protokollbilaga, p 642)

It requires comparatively high levels of temporal coordination and role differentiation, as the effectiveness of the distraction depends on overlapping with the homicide itself. At the same time, involving additional actors and operational stages introduces further risks related to exposure, miscommunication or operational failure. Selected actors carry out the diversionary act, leave the scene quickly and are rarely identified or apprehended in the available material:

“Bro, can you have a clean car in the vicinity of Biltema [a store] you know when you drive up the main road, there is a parking lot on the side where the car is. While you pour gasoline and fuck up the stolen one, he starts the clean car”. (Helsingborg tingsrätt, B 108-22, aktbilaga 32, p 1004)

The material suggests that distraction tactics remain uncommon compared to other counterintelligence measures. The limited occurrence may reflect the additional organizational complexity, particularly when less resource-intensive measures are considered sufficient to reduce operational exposure. Supporting the interpretation, distractions are more commonly observed in high-profile crimes in Sweden, such as robberies targeting postal terminals, rather than in operations attributed to smaller or less structured OCGs. Use appears concentrated among OCGs with prior experience in complex operations, possibly indicating a more developed capacity for coordinating multi-layered crimes. Usage of distractions is thus not intended to eliminate risk, but to redistribute it:

“Bro, send him some bag with a cable that sticks out so he can place it in the parking lot, or something, so there will be a large police operation.” (Örebro tingsrätt, B 5057-20, aktilaga 610, p 279)

In this sense, distractions represent a shift from primarily defensive counterintelligence measures focused on concealment toward a more offensive form of operational manipulation intended to shape adversary behavior directly, as defined by Mobley (2012).

5. Discussion

Organized crime and the boundaries of intelligence studies

The findings suggest recurring information-driven practices to facilitate criminal operations and mitigate risk. These are interpreted as intelligence and counterintelligence activities and appear associated with the planning of homicides in Sweden, primarily oriented toward two interconnected objectives. First, intelligence activities appear to involve the identification of suitable opportunities for carrying out a homicide, including the selection of locations frequented by the intended target and the continuous monitoring of the target's movements to determine when such opportunities arise. Second, counterintelligence appears to focus on reducing indicators that could signal the impending commission of a homicide and on mitigating the potential generation of evidence before, during and after the event. Both practices seem to be informed by accumulated experiential knowledge derived from previous criminal activities, interactions with other OCGs and contemporary police practices aligned to more explicit use of intelligence, as well as by ongoing observation of law enforcement operations and interpretations of perceived police behaviors in relevant contexts.

Limited attention is given to OCGs within the subject field of intelligence studies, despite operating in environments characterized by continuous need for intelligence and counterintelligence. This absence is noteworthy, as the increasing reliance of contemporary policing on intelligence-led approaches (Europol, 2025, p 88) is potentially influencing the criminal environment. Although some methods may be recognized by practitioners, due to conceptual and theoretical boundaries, they are seldom conceptualized into broader intelligence frameworks. As a result, the information management practices of OCGs often remain analytically underdeveloped despite their operational significance.

In competitive and confrontational environments, operational decisions are made under conditions of uncertainty. The use of intelligence becomes particularly important in violent operations, where inaccurate or incomplete information may not only result in operational failure, but also expose organizational capabilities, intentions, and methods to rival OCGs or police intelligence. Decision-making through intelligence can according to Erik Dahl (2013, p 2-3)

be managed either through long-term continuous strategies (i.e., strategic intelligence) or short-term tactical (i.e., tactical intelligence). The findings of this study point to a predominantly tactical use of intelligence in which information collection is oriented toward immediate concerns such as target identification, vulnerability assessment, environmental awareness and the timing of the operation. Whereas arguments can be made that general surveillance takes place in a strategic setting, its deployment in the context of homicide has specific characteristics. In the case of counterintelligence, it refers primarily to what Mobley defines as a “defensive” approach with most measures aimed at preventing the leakage of information rather than to an “offensive” approach involving the manipulation of the police (2012, p 8-10).

How ‘intelligent’ is it?

In conducting intelligence and counterintelligence in homicides (i.e., high-stakes activities), OCG members combine fragmented observations from multiple sources, including local surveillance, social media monitoring, public registries, GPS tracking devices and reports from associates positioned within relevant physical and social environments. Information is progressively corroborated through triangulation, whereby observations are continuously cross-checked against other sources to establish sufficient operational certainty. At the same time, ongoing monitoring of police activity, the use of disposable vehicles and false license plates, distraction tactics, and efforts to manipulate forensic evidence collectively serve to reduce the risk of attribution and preserve operational plausible deniability. Rather than concentrating intelligence functions within centralized structures, information collection is dispersed across multiple OCG members in different roles whose contributions are narrow, localized and often fragmented. Intelligence work therefore emerges less through formalized ‘bureaucratic’ systems than through decentralized practices embedded in everyday criminal activity.

That being said, most of the measures are not comparable with more sophisticated intelligence operations. Intelligence work emerges less through centralized bureaucratic structures than through decentralized practices embedded in everyday criminal activity. Functions are not institutionalized through dedicated intelligence units comparable to those of state agencies. Instead, intelligence activities are distributed across actors occupying different social and organizational positions, allowing groups to maintain situational awareness while limiting visibility and exposure. Within this context, intelligence and counterintelligence practices appear comparatively informal and organizationally fluid. Participation is structured less around rigid specialization than around differential exposure to risk and visibility. Individuals perceived as more exposed to police attention or rival observation are often restricted from

direct proximity to targets, while actors with lower visibility or fewer established associations to ongoing conflicts can move more freely without attracting suspicion.

As a result, participants frequently possess only partial knowledge regarding the broader purpose of the activities in which they are involved. Such compartmentalization may reduce the risks associated with intentional or accidental information leakage while simultaneously increasing plausible deniability if individuals are apprehended by the police. Organizational security therefore appears to depend less on preserving secrecy, than on the uneven distribution of operational knowledge across loosely connected participants.

Despite this organizational fluidity, the implementation of intelligence and counterintelligence measures nevertheless appears predominantly hierarchical. Strategic direction and tasking are generally articulated through top-down interactions, while operational execution is delegated across organizational layers. The resulting structure combines centralized coordination with decentralized implementation, allowing OCGs to maintain operational control while limiting organizational exposure.

This perspective also carries implications for policing and intelligence analysis. Criminal environments are shaped not only by the activities of OCGs, but also by their continuous adaptation to policing methods, surveillance practices, and investigative strategies. Intelligence and counterintelligence practices may therefore evolve through repeated interaction with law enforcement, producing reciprocal processes of adaptation between state and non-state actors. Overlooking this dynamic, identified by Erving Goffman (1970) as 'Strategic Interaction', risks underestimating both the operational learning capacities of OCGs and the extent to which intelligence practices may emerge outside traditionally recognized intelligence institutions.

Collectively, findings support function-oriented understandings of intelligence in which intelligence is defined primarily by what activities accomplish rather than by the formal characteristics of the institutions performing them. From this perspective, OCGs may engage in intelligence and counterintelligence practices despite lacking formal intelligence organizations, professional analytic units or bureaucratically institutionalized collection systems. Overlooking such dynamics risks underestimating both the operational learning capacities of OCGs and the extent to which intelligence practices may emerge outside traditionally recognized intelligence institutions.

Declarations

Ethical considerations:

All data in the study was handled in accordance with approved ethical guidelines by the Swedish Ethical Review Authority on [Information redacted to preserve anonymity for peer-review]. Any personal information is pseudonymized. This process is performed by relevant government authorities before it is provided to the project. In the case of information derived from court documents, all personal information

(such as Personal Number, Sex, Residence and Family associations) has been removed and is not included in the study.

Conflict of Interest:

No conflict of interest is present in the study.

Funding:

[Information on funding redacted to preserve anonymity for peer-review]

Author Contribution

C.U was responsible for design of the research, collection of data and data analysis as well as drafting the manuscript, including the tables/figures T.I: Contributed to the data analysis and revisions of the text and table/figures.Both authors have reviewed the manuscript and agreed to be held accountable for the work.

Data Availability

The dataset can not be shared to to Ethical Guidelines of Project.

Court Documents

Göteborg tingsrätt: B 1343-21

Göteborg tingsrätt: B 1359-21

Göteborg tingsrätt: B 9641-21

Göteborg tingsrätt: B 533-21

Halmstad tingsrätt: B 1486-19

Helsingborg tingsrätt: B 108-22

Malmö tingsrätt: B 9477-21

Norrköping tingsrätt: 308-20

Solna tingsrätt: B 10412-22

Södertörn tingsrätt: B 9452-22

References

1. Alonso Berbotto A, Chainey S (2021) Theft of oil from pipelines: an examination of its crime commission in Mexico using crime script analysis. *Global Crime* 22(4):265–287. <https://doi.org/10.1080/17440572.2021.1925552>
2. Ayling J (2009) Criminal organizations and resilience. *Int J Law Crime Justice* 37(4):182–196. <https://doi.org/10.1016/j.ijlcj.2009.10.003>
3. Angerbrandt H, Dufort M, Dudas V (2024) Ökningen av skjutvapenvåld i Sverige. *Brottsförebyggande rådet*, Stockholm
4. Bish, A., Borrion, H., Cockbain, E., & Toubaline, S. (2025). Anatomy of a route: Script analysis of irregular migration, smuggling and harms on the Central Mediterranean route to Europe. *Criminology & Criminal Justice*, 25(1), 59-80.
5. Borrion H (2013) Quality assurance in crime scripting. *Crime Sci* 2:6. <https://doi.org/10.1186/2193-7680-2-6>
6. Choi SW, Lee J, Choi Y-J (2024) Unveiling the patterns of romance scams in South Korea: insights and implications. *Int J Cyber Behav Psychol Learn* 14(1):1–15. <https://doi.org/10.4018/IJCBPL.357152>
7. Clark, R. M. (2026). *Intelligence analysis: A target-centric approach* (8th ed.). CQ Press.
8. Cornish DB (1994) The procedural analysis of offending and its relevance for situational prevention. In: Clarke RV (ed) *Crime prevention studies*, vol 3. Criminal Justice Press, Monsey, NY, pp 151–196
9. Dahl EJ (2013) *Intelligence and surprise attack: failure and success from Pearl Harbor to 9/11 and beyond*. Georgetown University Press, Washington, DC
10. de Korte LR, Kleemans ER (2022) Contract killings: a crime script analysis. *Trends Organ Crim* 25(1):130–143. <https://doi.org/10.1007/s12117-021-09411-4>
11. Fernández-Planells A, Orduña-Malea E, Feixa Pàmpols C (2021) Gangs and social media: a systematic literature review and an identification of future challenges, risks and recommendations. *New Media Soc* 23(7):2099–2124. <https://doi.org/10.1177/1461444821994490>
12. Flamer, N. (2025). Hizballah's Intelligence Collection Leading Up to and During the 2006 War With Israel: How a VNSA Conducts Operative Intelligence. *Terrorism and Political Violence*, 0(0), 1–17. <https://doi.org/10.1080/09546553.2025.2508799>
13. Gentry JA, Spencer DE (2010) Colombia's FARC: a portrait of insurgent intelligence. *Intell Natl Secur* 25(4):453–478. <https://doi.org/10.1080/02684527.2010.537024>
14. Gentry, J. A. (2016). Toward a Theory of Non-State Actors' Intelligence. *Intelligence and National Security*, 31(4), 465–489. <https://doi.org/10.1080/02684527.2015.1062320>

15. Gerell M, Sturup J, Magnusson M-M, Nilvall K, Khoshnood A, Rostami A (2021) Open drug markets, vulnerable neighbourhoods and gun violence in two Swedish cities. *J Polic Intell Counter Terror* 16(3):223–244. <https://doi.org/10.1080/18335330.2021.1889019>
16. Gilmour N (2023), "Crime scripting the criminal activities of money laundering – holistically". *Journal of Money Laundering Control*, Vol. 26 No. 3 pp. 594–608. <https://doi.org/10.1108/JMLC-09-2020-0109>
17. Gill P, Phythian M (2018) *Intelligence in an insecure world*, 3rd edn. Polity, Cambridge
18. Goffman E (1970) *Strategic interaction*. University of Pennsylvania Press, Philadelphia
19. Granath S (2024) Firearm and criminal milieu homicide in Sweden. *J Contemp Crim Justice* 40(3):493–510. <https://doi.org/10.1177/10439862241249010>
20. Harber JR (2009) Unconventional spies: the counterintelligence threat from non-state actors. *Int J Intell CounterIntell* 22(2):221–236. <https://doi.org/10.1080/08850600802698200>
21. Ilardi GJ (2009) Al-Qaeda's counterintelligence doctrine: the pursuit of operational certainty and control. *Int J Intell CounterIntell* 22(2):246–274. <https://doi.org/10.1080/08850600802698226>
22. Ilardi, G. J. (2009). The 9/11 Attacks—A Study of Al Qaeda's Use of Intelligence and Counterintelligence. *Studies in Conflict & Terrorism*, 32(3), 171–187. <https://doi.org/10.1080/10576100802670803>
23. Jacques S, Wright R, Allen A (2014) Drug dealers, retaliation, and deterrence. *Int J Drug Policy* 25(4):656–662. <https://doi.org/10.1016/j.drugpo.2014.03.001>
24. Johansen ML-E, Hedlund A, Tutenges S (2026) Nordic policy responses to gang-related crime 2009–2025: policy developments and future challenges in Denmark, Sweden and Norway. *Eur J Crim Policy Res* 32(2):503–522. <https://doi.org/10.1007/s10610-026-09662-3>
25. Kenney M (1999) When criminals out-smart the state: understanding the learning capacity of Colombian drug trafficking organizations. *Transnational Organized Crime* 5(1):97–119
26. Kenney MC (2003) Intelligence games: comparing the intelligence capabilities of law enforcement agencies and drug trafficking enterprises. *Int J Intell CounterIntell* 16(2):212–243. <https://doi.org/10.1080/08850600390198733>
27. Kleemans ER, van de Bunt HG (1999) The social embeddedness of organized crime. *Transnational Organized Crime* 5(1):19–36
28. Korsell L, Larsson P (2011) Organized crime the Nordic way. *Crime Justice* 40(1):519–554. <https://doi.org/10.1086/660917>
29. Krame G, Vivoda V, Davies A (2023) Narco drones: tracing the evolution of cartel aerial tactics in Mexico's low-intensity conflicts. *Small Wars Insurg* 34(6):1095–1129. <https://doi.org/10.1080/09592318.2023.2226382>
30. Krause LB (1996) Insurgent intelligence: the guerrilla grapevine. *Int J Intell CounterIntell* 9(3):291–311. <https://doi.org/10.1080/08850609608435319>
31. Kuloglu, G. (2016). Organized Crime Intelligence Management and a Model Proposal. *American Intelligence Journal*, 33(2), 115–125. <https://www.jstor.org/stable/26497096>

32. Łabuz, P., & Safjański, T. (2017). Counter-detection activities of criminal organizations aimed at reducing the effectiveness of surveillance conducted as part of operational activities. *Issues of Forensic Science*, 298, 62. <https://doi.org/10.34836/pk.2017.298.3>
33. Langlois, F., Rhumorbarbe, D., Werner, D., Florquin, N., Caneppele, S., & Rossy, Q. (2022). International weapons trafficking from the United States of America: a crime script analysis of the means of transportation. *Global Crime*, 23(3), 284–305. <https://doi.org/10.1080/17440572.2022.2067847>
34. Levi, M., & Soudijn, M. (2020). Understanding the Laundering of Organized Crime Money. *Crime and Justice*, 49, 579–632. <https://www.jstor.org/stable/48785549>
35. Liem M, Moeller K (2025) Revisiting Goldstein's drugs-violence nexus: expanding the framework for the globalized era. *Int Criminol* 5(1):71–83. <https://doi.org/10.1007/s43576-025-00160-w>
36. Madarie, R., Weulen Kranenbarg, M. & de Poot, C., (2024) Introducing object-oriented modelling to cybercrime scripting: visualisation for improved analysis. *Crime Sci* **13**, 27. <https://doi.org/10.1186/s40163-024-00227-5>
37. Madarie, R., Weulen Kranenbarg, M., & de Poot, C. (2025). Examining the cyclical nature of crimes: A looped crime script of data theft from organizational networks. *Computers in Human Behavior Reports*, 17, 100548. <https://doi.org/10.1016/j.chbr.2024.100548>
38. Magnusson M-M, Gerell M (2026) The geography of drug markets, drug crime and systemic gang violence—open drug scenes in Sweden. *Int J Drug Policy* 148:105119. <https://doi.org/10.1016/j.drugpo.2025.105119>
39. Mediemyndigheten (2026) Utgivningsbevis och databaser. <https://mediemyndigheten.se/ansokan-och-registrering/utgivningsbevis-och-databaser/>. Accessed 12 April 2026
40. Mobley BW (2012) Terrorism and counterintelligence: how terrorist groups elude detection. Columbia University Press, New York
41. Mobley BW, Ray T (2019) The Cali Cartel and counterintelligence. *Int J Intell CounterIntell* 32(1):30–53. <https://doi.org/10.1080/08850607.2018.1522218>
42. Morgenthaler E, Leclerc B (2023) Crime script analysis of drug importation into Australia facilitated by the dark net. *Global Crime* 24(3):169–194. <https://doi.org/10.1080/17440572.2023.2212592>
43. Morselli C, Giguère C, Petit K (2007) The efficiency/security trade-off in criminal networks. *Soc Networks* 29(1):143–153. <https://doi.org/10.1016/j.socnet.2006.05.001>
44. Polismyndigheten (2025) Myndighetsgemensam lägesbild: organiserad brottslighet 2025. Polismyndigheten, Stockholm
45. Prunckun H (2019) Counterintelligence theory and practice, 2nd edn. Rowman & Littlefield, Lanham, MD
46. Ratcliffe J (ed) (2009) Strategic thinking in criminal intelligence, 2nd edn. Federation Press, Sydney
47. Rostami A (2016) Criminal organizing: studies in the sociology of organized crime. Dissertation, Stockholm University
48. Rønn KV, Høffding S (2013) The epistemic status of intelligence: an epistemological contribution to the understanding of intelligence. *Intell Natl Secur* 28(5):694–716.

<https://doi.org/10.1080/02684527.2012.701438>

49. Sausdal D, Hannerz E (2025) Gängkriminalitet: från gatan till sociala medier. Liber, Stockholm
50. Sinai, J. (2024). Jihadi Intelligence and Counterintelligence. *Perspectives on Terrorism*, 18(4), 210–212.
51. Snaphaan T (2025) Connecting the dots: utilising crime scripting to leverage multimodal data and innovative techniques in a meaningful manner. *Methodol Innov* 18(2):101–113.
<https://doi.org/10.1177/20597991251336070>
52. Snaphaan, T., van Ruitenburg, T. (2025) Financial Crime Scripting: an Analytical Method to Generate, Organise and Systematise Knowledge on the Financial Aspects of Profit-Driven Crime. *Eur J Crim Policy Res* **31**, 695–715. <https://doi.org/10.1007/s10610-023-09571-9>
53. Strachan-Morris, D. (2019a). Developing theory on the use of intelligence by non-state actors: five case studies on insurgent intelligence. *Intelligence and National Security*, 34(7), 980–984.
<https://doi.org/10.1080/02684527.2019.1672034>
54. Strachan-Morris, D. (2019b). The use of intelligence by insurgent groups: The North Vietnamese in the Second Indochina War as a case study. *Intelligence and National Security*, 34(7), 985–998.
<https://doi.org/10.1080/02684527.2019.1668714>
55. Sturup J, Rostami A, Mondani H, Gerell M, Sarnecki J, Edling C (2019) Increased gun violence among young males in Sweden: a descriptive national survey and international comparison. *Eur J Crim Policy Res* 25(4):365–378. <https://doi.org/10.1007/s10610-018-9387-0>
56. Swanström N, Wenngren C (2017) Organized crime in foreign policy. *Oxford Research Encyclopedia of Politics*. <https://doi.org/10.1093/acrefore/9780190228637.013.375>
57. Tantalakis E (2019) Insurgents' intelligence network and practices during the Greek Civil War. *Intelligence National Security* 34(7):1045–1063. <https://doi.org/10.1080/02684527.2019.1668718>
58. Tompson L, Chainey S (2011) Profiling illegal waste activity: using crime scripts as a data collection and analytical strategy. *Eur J Crim Policy Res* 17(3):179–201. <https://doi.org/10.1007/s10610-011-9146-y>
59. Tollin K, Hammar L, Jonsson A (2022) Illegal drug markets in Sweden: a study of smuggling, street dealing, internet sales and buyers. *Brottsförebyggande rådet*, Stockholm
60. von Lampe K (2016) *Organized crime: analyzing illegal activities, criminal structures and extra-legal governance*. SAGE, Los Angeles
61. Wang, F. (2025). A Crime Script Analysis of Pao Fen Operations and the Construction of Prevention Strategies. *Crime & Delinquency*, 0(0).
62. Warburton J (2025) Subcontracted violence amongst London's drug gangs. *Global Crime* 26(3–4):173–191. <https://doi.org/10.1080/17440572.2025.2499448>
63. Warner M (2013) The past and future of the intelligence cycle. In: Phythian M (ed) *Understanding the intelligence cycle*. Routledge, London, pp 9–20
64. Wege CA (2012) Hizballah's counterintelligence apparatus. *Int J Intell CounterIntell* 25(4):771–785.
<https://doi.org/10.1080/08850607.2012.705185>

Footnotes

1. In the original quote, the word "snuthus" is used, which can be interpreted to mean both "police-station" and the private residences of police officers.