MASTER THESIS | MASTER‘S THESIS

Titel | Title

Geocriminality: Hybrid Threats and the Strategic Role of Organised Crime

verfasst von | submitted by

Sonja Mayr, BEd MEd

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Advanced International Studies (M.A.I.S.)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 992 940
Universitätslehrgang lt. Studienblatt | Degree programme as it appears on the student record sheet:	Internationale Studien | International Studies
Betreut von | Supervisor:	Priv.Doz. Robert Schuett, Ph.D.

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

Abstract

This thesis investigates why states employ elements of organised crime as instruments of conflict, a phenomenon conceptualised as geocriminality. As the contemporary security environment is in a stage of transformation from conventional warfare towards grey zone competition, states increasingly rely on indirect and deniable methods of coercion that operate below the threshold of armed conflict. While hybrid threat research and organised crime scholarship have developed largely in parallel, the strategic logic behind the instrumentalisation of criminal networks by states remains undertheorised. This thesis addresses that gap by developing a mechanism-based explanatory framework. Methodologically, the study adopts a qualitative, small-N case study design combining extensive literature research with process tracing across two illustrative cases: North Korea and Iran. The analysis proceeds in three layers: establishing a conceptual and theoretical framework drawing on realism, the English School, game theory, and the principal-agent theory; identifying the strategic logic and incentive structures that make organised crime attractive to states; and empirically testing the proposed mechanisms through case study analysis. Five core mechanisms are identified in order to explain why states turn to organised crime as a strategic tool: plausible deniability and strategic ambiguity, escalation control through threshold management, outsourcing to pre-existing illicit capacity, exploitation of illicit infrastructures, and iterative disruption leading to cascading destabilisation. The findings demonstrate that geocriminality is a rational strategic choice particularly for states facing sanctions, diplomatic isolation, military asymmetry, or resource constraints. North Korea exhibits an institutionalised form of geocriminality centred on regime survival, while Iran employs a more flexible pattern oriented towards influence projection and asymmetric competition. The thesis contributes to bridging criminology and security studies, reframing organised crime not merely as a law enforcement concern but as a fundamental strategic security issue with profound implications for the international order.

Keywords: geocriminality; hybrid threats; organised crime; grey zone conflict; state-crime nexus

Abstrakt

Ziel der vorliegenden Masterarbeit ist es zu untersuchen, warum Staaten Elemente organisierter Kriminalität als Instrumente der Konfliktführung einsetzen, ein Phänomen, welches als Geokriminalität konzeptualisiert wird. Im Kontext des sich kontinuierlich wandelnden Sicherheitsumfeld, das sich tendenziell von konventioneller Kriegsführung hin zur Konkurrenz in der Grauzone bewegt, greifen Staaten zunehmend auf indirekte und abstreitbare Formen der Einflussnahme zurück, die unterhalb der Schwelle bewaffneter Konflikte operieren. Während die bisherige Forschung hinsichtlich hybriden Bedrohungen und organisierter Kriminalität weitgehend separat verlief, wurde die strategische Logik hinter der Instrumentalisierung krimineller Netzwerke durch Staaten bislang theoretisch unzureichend beleuchtet. Diese Arbeit verschriftlicht das Bestreben diese Lücke durch die Entwicklung eines mechanismenbasierten Erklärungsrahmens zu schließen. Methodisch kommt ein qualitatives Small-N-Fallstudiendesign zur Anwendung, das umfassende Literaturrecherche mit Prozessverfolgung (Process Tracing) im Rahmen zweier illustrativer Fallstudien – Nordkorea und Iran – verbindet. Die Analyse gliedert sich demnach in drei Ebenen: die Erarbeitung eines konzeptionellen und theoretischen Rahmens auf Grundlage des Realismus, der Englischen Schule, der Spieltheorie und der Prinzipal-Agent-Theorie; die Identifikation der strategischen Logik und Anreizstrukturen; sowie die empirische Überprüfung der Mechanismen durch die Fallstudienanalyse. Diesbezüglich werden fünf Kernmechanismen identifiziert: glaubhafte Abstreitbarkeit und strategische Ambiguität, Eskalationskontrolle durch Schwellenmanagement, Auslagerung an bestehende illegale Kapazitäten, Ausbeutung illegaler Infrastrukturen sowie iterative Destabilisierung mit kaskadierenden Effekten. Die Ergebnisse zeigen, dass Geokriminalität eine rationale strategische Wahl darstellt, insbesondere für Staaten, die mit Sanktionen, diplomatischer Isolation, militärischer Asymmetrie oder Ressourcenknappheit konfrontiert sind. Nordkorea weist eine institutionalisierte Form der Geokriminalität auf, die auf Regimeüberleben abzielt, während der Iran ein flexibleres Muster verfolgt, das auf Einflussprojektion und asymmetrische Konkurrenz ausgerichtet ist. Die Arbeit leistet einen Beitrag zur Überbrückung von Kriminologie und Sicherheitsforschung und verortet organisierte Kriminalität nicht nur als Problem der Strafverfolgung, sondern als strategische Sicherheitsfrage mit weitreichenden Implikationen für die internationale Ordnung.

Schlüsselwörter: Geokriminalität; hybride Bedrohungen; organisierte Kriminalität; Grauzonenkonflikt; Staat-Kriminalität-Nexus

Acknowledgements

My most heartfelt thanks go to my family and my friends for supporting and guiding me throughout this journey.

Thank you for everything!

On my honour as a student of the Diplomatische Akademie Wien, I submit this work in good faith and pledge that I have neither given nor received unauthorised assistance on it.

Table of Contents

1. INTRODUCTION 1
   1.1. Research Background and Problem 1
   1.2. Research Question and Argument 2
   1.3. Objectives, Scope, and Structure 4
2. RESEARCH DESIGN AND METHODOLOGICAL APPROACH 6
   2.1. First Analytical Layer: Creating a Conceptual and Theoretical Framework 6
   2.2. Second Analytical Layer: Tracing The 'WHY' – States' Strategic Logic 7
   2.3. Third Analytical Layer: Case Studies, Analysis, and Discussion 9
3. CONCEPTUAL AND THEORETICAL FRAMEWORK 11
   3.1. Conceptual Framework 11
   3.2. Theoretical Perspectives 16
4. THE 'WHY' – STATES' STRATEGIC LOGIC 21
   4.1. Strategic Context: Actors, Relationships, and Interaction 21
   4.2. Incentive Structure and Structural Conditions 25
   4.3. From Incentives to Action: The Mechanism Framework 38
5. CASE STUDY ANALYSIS 40
   5.1. Case Study: North Korea 40
   5.2. Case Study: Iran 48
   5.3. Discussion 57
6. CONCLUSION 61

BIBLIOGRAPHY 64

ANNEX 77

Annex 1: Glossary 77

1. INTRODUCTION

1.1. Research Background and Problem

Since the end of the Cold War we have lived in a comparatively peaceful world; but the transformation of the security environment is well underway. While the post-Cold War period was largely characterised by expectations of liberal peace and cooperative multilateralism with the advent of a multipolar order and expanding interconnectedness due to globalisation, contemporary international politics increasingly reflects renewed geopolitical rivalry and strategic competition. While conflict has anything but disappeared, it has inherently shifted in its form. The times, when military, hard power was the most pivotal deciding factor in conflict, may have passed, and non-military, soft power contest has added considerably to the various actors' toolbox. Instead of large-scale conventional warfare between major powers, states increasingly rely on indirect and deniable methods of coercion; and the rise of multi-domain competition has blurred the distinction between war and peace. Strategic actors deliberately operate below the threshold of armed conflict and act within this penumbra between war and peace – the grey zone – in order to avoid escalation, retaliation, and legal consequences. This transformation has heightened the relevance of non-state actors in the strategic landscape.

Importantly, the growing interconnectedness has not gone unnoticed by organised crime actors (cf. Calcagni, 2010, p. 73). As Clarke and Williams (2024) elucidate, "globalization had a profound impact on organized crime, creating new opportunities for criminal organizations to extend their reach and capabilities, facilitating the expansion of illicit economies" (p. 192). Transnational organised crime has transformed from territorially bounded groups into globally networked, technologically sophisticated actors, which operate across cyber domains, financial systems, supply chains, and increasingly also in political spheres. As illicit markets globalise, criminal infrastructures become embedded in global logistics, financial systems, and digital networks. These infrastructures can produce macro-level effects: financial disruption, supply chain manipulation, institutional erosion, and societal destabilisation. Organised crime has thus evolved from a rather local to a global threat, which crucially "is becoming a profound threat to democratic governance. By infiltrating public institutions, manipulating procurement processes and eroding the rule of law through corruption and fear, criminal networks can undermine the legitimacy of the state. Public trust erodes, resources are diverted and inequality deepens – fuelling social fragmentation" (ART, 2025, p. 3).

In this context, Giannopoulos et al. (2021, p. 15) points out the transformation of the concept of security, which now encompasses not merely the military sphere, but includes a myriad of domains, such as the individual, society, and humanity as a whole. With regard to the possible erosion of state legitimacy through organised crime, state security therefore cannot only be threatened by a malignant state through military capabilities, but also by non-state actors, such

as organised criminal networks. State actors are increasingly aware of developments within the threat landscape, not only with regard to their own security, but also concerning the security gaps of their adversaries. Hence, non-state threat actors, which generally pursue their own objectives, not always act independently, as such an actor may be turned into an agent. But what happens, when states utilise organised crime to execute their political agenda? And why would a state be incentivised to do so?

The convergence of hybrid threat tools and organised crime is paramount in this context. Generally, the concept of hybrid threats captures coordinated activities that combine state and non-state tools to achieve strategic objectives below the threshold of conventional warfare. Many such activities, including cyberattacks, economic sabotage, and disinformation, overlap with practices commonly associated with criminal actors. Organised crime therefore occupies a structural position within hybrid conflict environments. However, these phenomena have largely been examined separately. While research on hybrid threats mainly focuses on military, intelligence, and geopolitical instruments, organised crime research remains rooted in criminology and legal studies. As a result, limited attention has been paid to organised crime as a strategic tool of statecraft.

The core research problem concerns states' instrumentalisation of organised crime, in short, *geocriminality*. While existing scholarship acknowledges the existence of the state-crime nexus, proxy warfare, and hybrid conflict, what remains underexplored is the intersection depicting organised crime as a deliberately tolerated, enabled, or exploited proxy instrument within hybrid strategies. In other words, the strategic logic behind what makes organised crime an attractive tool for states remains insufficiently theorised. This thesis sets out to address this gap by developing a mechanism-based account of organised crime as an instrument of hybrid conflict and state strategy.

1.2. Research Question and Argument

Research Question

This thesis aims to investigate the following: *Why do states employ elements of organised crime as instruments of conflict?* This question seeks to explain strategic incentives for states to employ elements of organised crime as instruments of conflict and thereby frequently as proxies rather than prove direct coordination between state and criminal non-state actors. Posing a 'Why' question allows for focusing on the strategic logic behind states' engagement in geocriminality rather than on the empirical verification of covert state-criminal relationships. This thesis will therefore be framed as an explanatory study of incentives and mechanisms, rather than as an investigative effort to prove state responsibility or direct control.

States do not need to covertly or overtly hire or collaborate with non-state actors who commit an organised crime in order to employ elements of organised crime as instruments of conflict. Rather, states can also passively benefit from organised crime targeting another state. Hereinafter, organised crime is construed as a hybrid threat to states' security. It is of interest to explore why states may be incentivised to use hybrid threats in the form of organised crime

in the context of conflict and power competition instead of relying on conventional military, economic, and political means. It is further pivotal to acknowledge that this thesis does not attempt to demonstrate direct command-and-control relationships. Rather, it focuses on strategic logic, opportunity structures, and mechanism-based explanation, examining inter alia alignment, permissiveness, and benefit instead of formal proof of orchestration.

Argument

The central claim put forward in this thesis is: *Organised crime constitutes a hybrid proxy instrument for states, which is capable of generating coercive, deniable, and strategically relevant effects below the threshold of armed conflict.*

The argument will develop along the following lines: the central hypothesis postulates that organised crime constitutes a hybrid threat to state security, as both state-led and autonomous non-state actors – whether operating as proxies and or pursuing independent profit motives – can generate coercive, deniable, and strategically significant effects below the threshold of armed conflict. It is further suggested that the engagement in geocriminality as a strategic tool is favoured over conventional political, military, or economic instruments, as the former is harder to attribute, entails a lower risk of retaliation, is comparatively inexpensive and easy to deploy, and can produce disproportionate levels of disruption and harm.

As organised crime provides states with several key advantages, five core mechanisms underpin this argument. *(1) Plausible deniability and strategic ambiguity* arises, as delegating activities to criminal actors obscures attribution and diffuses accountability. *(2) Escalation control through threshold management* keeps operations below legal and military thresholds, enabling sustained pressure without triggering collective defence or retaliation. *(3) Outsourcing to pre-existing illicit capacity* reduces financial and political costs by leveraging criminal networks' existing logistics, infrastructure, and expertise. *(4) Exploitation of illicit infrastructures* provides access to smuggling routes, shell companies, money laundering systems, and sanctions evasion networks. Finally, (*5) iterative disruption and cascading destabilisation* gradually erodes institutional trust, economic stability, and governance capacity as cumulative criminal effects produce disproportionate strategic impact.

Additionally, geocriminality provides a variety of tactical advantages for states, while the use of conventional, kinetic as well as non-kinetic instruments of power may generate certain disadvantages, which renders their employment unattractive. For instance, military force risks escalation, economic sanctions are traceable and politically costly, and diplomatic coercion lacks deniability. The emerging image suggests that organised crime offers a lower-risk alternative in competitive environments. The broader implication, hence, is that geocriminality erodes international order gradually, undermining sovereignty without openly violating it while simultaneously challenging traditional distinctions between crime and conflict as well as war and peace.

1.3. Objectives, Scope, and Structure

Objectives and Significance

The primary objective of this thesis is to address the question of why states employ elements of organised crime as instruments of conflict. Academically, the objectives are manifold, but limited in their weight due to the scope of the present work. Shortly, the aims are bridging the gap between criminology and security studies and providing a theoretical explanation rather than descriptive case accounts. Theoretically, this thesis sets out to contribute to the development of a mechanism-based framework explaining state incentives. Another endeavour is to clarify how the employment of elements of organised crime fits within below-threshold coercion and integrate a realist cost-benefit logic within hybrid threat theory.

The significance of investigating the research question lies in its policy relevance by reframing organised crime as a strategic security issue. It highlights the limits of purely law enforcement responses and points out the necessity of improved attribution mechanisms, hybrid resilience strategies, international coordination, and legal reforms regarding state responsibility. The central problem is a gap in existing scholarship: while literature on hybrid threats and proxy warfare increasingly recognises the role of non-state actors, the strategic logic behind the use of organised criminal networks as proxies remains under-theorised. This thesis addresses this gap by explaining why organised crime constitutes a particularly attractive instrument for states seeking to compete and coerce below the threshold of armed conflict.

Scope and Limitations

Outlining the scope of this thesis, the focus is clearly placed on organised crime in situations where it generates strategic security effects. The emphasis is placed on below-threshold competition, rather than open warfare. Some limitations include the methodology – a qualitative, small-N, explanatory approach based on the analysis of two illustrative case studies has been chosen as the modus operandi, which entails the reliance on open-source, qualitative material. Additionally, this thesis neither does nor seeks to provide conclusive proof of state orchestration and therefore cannot establish intent beyond plausible inference. Data on geocriminality is scarce and sources, particularly those stemming from organised criminal networks, are opaque (cf. Petta Gomes da Costa, 2018, p. 11). Moreover, not all organised criminal activity constitutes a hybrid threat. The present thesis considers organised crime as a hybrid threat and thus a tool to be employed merely in instances when it produces macro-level strategic effects, intersects with geopolitical competition, and aligns with state incentives.

Structural Outline

To conclude, the structure of this thesis is outlined as follows: Chapter 2 presents the qualitative, theory-guided case study design, focusing on recurring patterns between states and organised criminal networks. It identifies key mechanisms such as plausible deniability, reduced escalation risks, lower costs, access to illicit infrastructures, and exploitation of legal gaps. Chapter 3 develops the conceptual and theoretical framework, clarifying key terms and engaging selectively with contested concepts such as hybrid threats and grey zones. As

Vladimir Bankov (2024) emphasises, “conceptual perfectionism is unbeneficial” (p. 17). Accordingly, a minimal, operational definition of hybrid threats is adopted. The chapter also introduces the main theoretical lenses, including realism, the English School, and hybrid threat theory. Chapter 4 outlines the strategic logic that underpins the engagement in geocriminality, conceptualising organised crime as a potential instrument in below-the-threshold strategies. Chapter 5 applies this framework to selected case studies, providing a case study analysis as well as the assessment and discussion of cross-case patterns and broader implications. Chapter 6 concludes by summarising the elucidations of Chapters 2 to 5, addresses the research gap, and outlines avenues for future research.

2. RESEARCH DESIGN AND METHODOLOGICAL APPROACH

Methodologically, this thesis adopts an explanatory qualitative approach that combines literature research with a qualitative case study analysis.[1] The aim is to analyse organised crime as a hybrid threat and assess the incentives states have to engage in geocriminality. The methodology is deliberately non-positivist: rather than relying on statistical correlations between variables like regime type, state capacity, or sanctions exposure and the presence of state-sponsored organised crime, this thesis explores states' incentives on the basis of a conceptual and theoretical framework and by tracing the concrete causal mechanisms that link state decisions to the instrumentalisation of organised crime. Causal mechanisms are the processes that explain how and why one thing produces another. They reveal the intermediate actions, actors, and conditions that link a cause to its effect (cf. Ylikoski, 2019, p. 16).

The central research question is a 'why' question: *Why do states employ elements of organised crime as instruments of conflict?* This 'Why' investigates a) what the reasons behind states' strategic logic in this context are and b) how states are incentivised to do so. Rather than seeking direct proof for command-and-control relationships, this behaviour is explained by identifying the competitive advantages that states may derive from engaging in geocriminality. The purpose of this method is to provide a feasible causal explanation for a 'why' question: it uncovers the processes through which states translate incentives into the concrete instrumentalisation of organised crime, integrates theory, and supports policy-relevant conclusions. The approach taken proceeds in three analytical layers: the first two layers rely on extensive literature research, while the third consists of an empirical qualitative case study analysis. These layers simultaneously function as the core structural elements of the present thesis.

2.1. First Analytical Layer: Creating a Conceptual and Theoretical Framework

At the conceptual and theoretical level, this thesis establishes the analytical foundation by defining its core building blocks and situating them within relevant theoretical perspectives. It first develops a coherent conceptual framework by clarifying the key terms that structure the analysis, namely *hybrid threats*, *organised crime*, and *geocriminality.*[2] Building on these definitions, this thesis then links these elements within established theoretical approaches in international relations and security studies. In particular, *Realism* provides a framework for

[1] "We define a case study to be a method of obtaining a "case" or a number of "cases" through an empirical examination of a real-world phenomenon within its naturally occurring context, without directly manipulating either the phenomenon or the context" (Kaarbo & Beasley, 1999, p. 372).
[2] These terms among others will be thoroughly defined in subsection *3.1. Conceptual Framework*.

understanding state behaviour as driven by strategic utility, power considerations, and cost-benefit calculations, while *Hybrid Threat Theory* highlights the growing importance of ambiguous and non-linear instruments of conflict. By bringing these perspectives together, this layer (Chapter 3) demonstrates that the engagement in geocriminality is theoretically consistent with existing expectations about state behaviour. It establishes the plausibility within existing theoretical framework of such practices and derives initial expectations regarding the strategic incentives that may motivate states to engage in geocriminality.

2.2. Second Analytical Layer: Tracing The 'WHY' – States' Strategic Logic

Building on the conceptual and theoretical framework, the second analytical layer (Chapter 4) explains *why* states employ elements of organised crime by identifying the causal mechanisms that link structural incentives to concrete forms of action. Rather than simply assuming intentional control or direct command relationships, the analysis focuses on how states are incentivised to utilise organised crime within specific strategic contexts. Answering a 'why' question requires more than identifying abstract motivations. Incentives alone do not constitute causal explanations unless it can be shown how they translate into behaviour and produce observable effects. For this reason, the analysis adopts a mechanism-based approach, in which each explanation specifies not only the underlying incentive, but also the actions through which it is operationalised and the resulting outcomes (cf. McGinley, 2014, p. 377). This allows this thesis to move from speculative reasoning about state intentions to a structured account of how and why organised crime is instrumentalised. Hence, each causal mechanism is conceptualised as a process consisting of three elements:

(1) an underlying incentive,
(2) the actions through which this incentive is operationalised, and
(3) the resulting strategic outcome.

This structure connects abstract theoretical expectations to observable practices and provides the analytical basis for process tracing in the case study analysis (Chapter 5). Five core mechanisms are identified:

1. Plausible deniability and strategic ambiguity

This mechanism is driven by the incentive to avoid attribution and limit political and legal accountability, particularly in contexts where direct involvement would entail diplomatic, legal, or military consequences. States enact this incentive by delegating activities to organised crime actors and deliberately obscuring links between state and non-state entities. The outcome is strategic ambiguity: attribution becomes difficult, response options are delayed or constrained, and states are able to act while minimising the risk of retaliation. As Bryjka suggests, "the essence of war by proxy is […] maintaining 'plausible deniability'" (p. 191).

2. Escalation control through threshold management

The underlying incentive here is to exert pressure on adversaries while avoiding escalation into open conflict. This is realised through activities that remain below legal and military thresholds, including indirect and hence deniable operations conducted by criminal networks. By relying on actors whose conduct does not clearly meet the criteria of armed attack or use of force, states create legal ambiguity. The outcome is controlled coercion: states can apply sustained, incremental pressure without triggering collective defence mechanisms or provoking immediate military retaliation.

3. Outsourcing to pre-existing illicit capacity (cost efficiency)

This mechanism is driven by the incentive to minimise financial and political costs, such as the expenses associated with training and maintaining specialised units, or risking diplomatic fallout from direct state involvement. States do this by outsourcing tasks to organised crime groups that already possess the necessary infrastructure, expertise, and logistics. Rather than developing capabilities internally, states leverage existing criminal capacities. The outcome is cost-efficient and flexible operations with reduced institutional exposure, allowing states to pursue strategic objectives without large-scale mobilisation or formal commitment.

4. Exploitation of illicit infrastructures (sanctions evasion)

This mechanism is based on the incentive to circumvent economic and legal constraints, first and foremost, sanctions regimes. States translate this into action by leveraging existing criminal infrastructures such as smuggling routes, shell companies, corruption networks, and money laundering systems. These systems enable the movement of goods and capital outside traceable channels. The outcome is enhanced operational flexibility: states can sustain economic activity and evade external restrictions.

5. Iterative disruption and cascading destabilisation

The underlying incentive is to weaken adversaries over time without engaging in direct confrontation. This mechanism operates through the cumulative effects of criminal activities such as corruption, coercion, and illicit finance, which gradually erode institutional trust and governance capacity. Over time, these micro-level disruptions accumulate into broader systemic effects. The outcome is cascading destabilisation: economic, political, and social systems become increasingly fragile, often less through actual institutional breakdown than through shifts in public perception. This aligns with the broader observation that hybrid threats "aim to create cascading effects and exploit interconnections" (Aho et al., 2023, p. 10).

MECHANISM	CORE INCENTIVE (WHY?)	OPERATIONAL LOGIC (HOW?)	STRATEGIC OUTCOME (WHAT?)
PLAUSIBLE DENIABILITY & STRATEGIC AMBIGUITY	Avoid attribution; minimise legal and political accountability	Delegation to organised crime actors; indirect support; concealment of links	Reduced attribution; delayed or constrained responses; lower risk of retaliation
ESCALATION CONTROL	Exert pressure without triggering open conflict	Use of fragmented, deniable activities below legal/military thresholds	Incremental coercion without escalation; avoidance of direct military response
OUTSOURCING TO ILLICIT CAPACITY	Minimise financial, operational, and political costs	Reliance on criminal actors with existing expertise and logistics	Cost-efficient operations; reduced institutional exposure
EXPLOITATION OF ILLICIT INFRASTRUCTURES	Circumvent legal, economic, and regulatory constraints	Use of smuggling routes, financial networks, corruption structures	Sanctions evasion; sustained covert operations; increased flexibility
ITERATIVE DISRUPTION & CASCADING DESTABILISATION	Weaken adversaries without direct confrontation	Repeated criminal activities (corruption, coercion, illicit finance)	Gradual erosion of trust, governance, and systemic stability

Table 1: Core mechanisms of states' strategic logic

Overall, these mechanisms explain how states translate structural pressures into indirect and deniable forms of conflict behaviour. While analytically distinct, they often reinforce one another in practice. Conceptualising them as mechanisms allows the analysis to move beyond descriptive claims about strategic advantages and instead provide a structured causal explanation of state behaviour.

2.3. Third Analytical Layer: Case Studies, Analysis, and Discussion

The third analytical layer (Chapter 5) applies the mechanism-based framework to case studies to examine how the identified incentives are translated into concrete action. Building on the previous layer, the analysis uses process tracing to assess whether the proposed causal mechanisms are observable in practice (cf. Kaarbo & Beasley, 1999, p. 386). Rather than seeking definitive proof of command-and-control relationships, the focus lies on identifying sequences of incentives, actions, and outcomes that align with the mechanisms outlined above.

Methodologically, this thesis adopts a small-N qualitative case study design. The selected cases – North Korea and Iran – share common features but vary significantly in geopolitical context. This variation allows the analysis to assess which mechanisms operate consistently and which are contingent on specific strategic environments. For each case, process tracing is used to reconstruct the causal chain linking structural incentives to the use of criminal networks for strategic purposes. Across cases, a structured comparison is employed to identify similarities and differences in how these mechanisms manifest.

To account for varying degrees of state involvement, the analysis adopts a graduated understanding of geocriminal engagement, ranging from indirect alignment to more integrated relationships between state and criminal actors (cf. Singh, 2024). The aim is to demonstrate systematic correspondence between state incentives and criminal activities. Given the covert and ambiguous nature of the phenomenon, direct evidence is often limited. This thesis therefore prioritises explanatory coherence over definitive attribution. It seeks to show how organised crime can function as a strategic instrument by tracing the mechanisms, rather than by conclusively proving intentional state control.

3. CONCEPTUAL AND THEORETICAL FRAMEWORK

The analytical foundation of this thesis is based on a conceptual framework and its situation within established theoretical perspectives. This chapter therefore functions as the first analytical layer the subsequent layers will build on.

3.1. Conceptual Framework

The conceptual framework establishes the core concepts and building blocks of the present work, providing definitions and explanations for how these key concepts interrelate. It is therefore of interest to revisit the constituents of the research question: *Why do states employ elements of organised crime as instruments of conflict?*

Essentially, this question frames organised crime as a hybrid threat that can be instrumentalised by states for strategic purposes. The three most central elements of interest hence are *hybrid threats* including the actors that can perform them, *organised crime* in its various shapes and forms, and last but not least organised crime use as *instruments of conflict*. The conceptual framework draws on existing literature to define and delimit the key concepts relevant to the analysis, while the subsequent section situates them within broader theoretical perspectives.

Hybrid Threats and Hybrid Threat Actors

International Relations (IR) in its most basic definition involves interactions – of the positive as well as the negative sort – between a variety of actors. While states remain central actors within the international system, intra-state behaviour plays out across a myriad of dimensions. Shehu (2024) identifies political economic security, legal, cultural and social, as well as technological dimensions of international relations. Analysing such interactions becomes increasingly layered when non-state actors are involved, particularly when they operate transnationally and outside legal frameworks. Simultaneously, not only the type of threat actors has diversified, but also the types of threats have done so, both in theory and in practice.

In this context, the concept of *hybrid threats*, referring to a multi-domain approach, has emerged as a neologism in the vocabulary of strategists, analysts, and scholars. Generally, 'hybrid threat' has evolved into an umbrella term encompassing a wide range of coordinated activities, reflected by the definitional multiplicity found in literature. Despite this definitional plurality, there is broad agreement that hybrid threats are characterised by the combination of various means and multifaceted activities, targeting both military and civilian domains (cf. Bankov, 2024, p. 16; Cilluffo & Clark, 2014, p. 48; Hoffman, 2007, p. 29). For instance, NATO defines hybrid threats as the combination of "military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of

irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt [...] to destabilise and undermine societies" (NATO, 2026) – a highly laden definition, too broad for some (cf. Wigell et al., 2021, p. 11), not including enough aspects according to others. Similarly, the Council of the European Union (2025) defines hybrid threats as follows:

Definition	"Hybrid threats usually refer to coordinated harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined. These means may include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force. Hybrid tactics are used by both state and non-state actors and are growing in complexity and sophistication. In addition to the security risk, they pose a threat to democracy, targeting its core values and aiming to fracture society and undermine political decision-making. Hybrid campaigns are designed in a way that makes detecting and defending against them difficult. They are devised to remain below the threshold which could constitute or be perceived as an act of war" (Council of the European Union, 2025).

A central characteristic of hybrid threats is therefore their strategic intent: actions only constitute hybrid threats when they are deliberately employed to undermine or manipulate a target. Importantly, such activities might not be illegal per se (cf. Giannopoulos et al., 2021, p. 9), but may also take the form of foreign policy tools "such as the use of disinformation, economic coercion, or election meddling for political influence" (Wigell, 2019, p. 258). It is furthermore worth noting that hybrid threats refer to activities that deliberately remain below the threshold of armed conflict and may never escalate into open war or armed conflict. Generally, war or armed conflict is associated with kinetic military force, physical destruction, loss of life, or effects comparable to conventional military attacks. Hybrid threats deliberately avoid crossing these thresholds, while still achieving strategic objectives.

As Sari (2026) highlights, below-the-threshold competition entails a variety of characteristics such as the creation of ambiguity, the fostering of deniability of involvement as well as responsibility, the possible aim of generating non-kinetic results such as the erosion of trust, and the decrease in the likelihood of retaliation. "This might include the gradual build-up of capacity, persistent activities meant to achieve strategic gains over time or small-scale engagements of limited intensity that, when taken by themselves, do not merit a robust response by the target" (p. 31). These features closely align with the concept of the *grey zone*, where the lines between peace and war are blurred (cf. Mazarr, 2015, p. 58). The grey zone describes "a space between states, and/or their proxies, in which states engage in strategic competition with each other, and in which their activities are aimed to either weaken or coerce the opponent. These activities do not amount to classical (military) war, nor do they amount to peace" (De Castro, 2025, p. 7).

Within this environment, scholarship exhibits broad consensus that hybrid threat activities can stem from state as well as non-state actors (cf. Normark, 2019, p. 2; Voyger, 2021). Importantly,

in order to carry out hybrid threat activities, states may decide to instrumentalise non-state actors, turning them into proxies in the pursuit of strategic objectives. As such, proxy use constitutes a key operational feature of hybrid threats, particularly in the grey zone context. This is where the connection to organised crime becomes particularly relevant. Organised crime shares several characteristics with hybrid threats: organised criminal networks utilise a variety of means, they operate transnationally and outside legal frameworks, and do so with malign intent. When instrumentalised by states, these characteristics enable organised crime to get integrate into hybrid threat strategies.

Organised Crime in the Security Context

Organised crime refers to criminal activities carried out by organised criminal networks or organised criminal groups. For reasons of simplicity, this thesis does not differentiate between networks and groups and uses both terms interchangeably. Organised criminal groups are defined by the United Nations Convention against Transnational Organized Crime (UNTOC) as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences […] in order to obtain, directly or indirectly, a financial or other material benefit" (United Nations Office on Drugs and Crime [UNODC], 2004, Annex I, p. 5).

Monetary gain is frequently highlighted as the main driver of organised crime (cf. United Nations Office on Drugs and Crime [UNODC], n.d.). As De Boer and Bosetti (2015) argue, "the tendency is to emphasize a profit motive, provoking questions as to whether serious illicit activities perpetrated for non-economic reasons (i.e. social status, ideology) can constitute organized crime" (p. 3). While this thesis acknowledges that organised criminal actors may also be driven by non-economic motives, there appears to be broad consensus that the majority of organised crime is primarily aimed at generating financial gain. Accordingly, this thesis adopts the following definition:

Definition	Organised crime refers to "the organised criminal acts of non-state actors committed with economic motives against nations across national borders" (Liyanage, 2022).

This definition highlights three core characteristics of organised crime:

(1) the central role of non-state actors,
(2) the predominance of economic motivations, and
(3) the transnational nature of activities directed against states (Liyanage, 2022).

Organised crime encompasses a wide range of activities. Europol (2017, p. 57) identifies a variety of key crime areas, such as cybercrime, drug trafficking, trafficking in human beings, migrant smuggling, firearms trafficking, fraud, intellectual property crime, environmental crime, and currency counterfeiting. These activities are increasingly interconnected. As Luyten (2024, p. 7) remarks, digitalisation and technological developments contribute to the convergence of different forms of criminal activity, particularly in the fields of cybercrime,

financial crime, and fraud. Such developments not only complicate law enforcement but also amplify the broader societal impact of organised crime. Criminal proceeds undermine legitimate financial systems, distort market dynamics, and fuel corruption, which in turn facilitates further criminal activity. As a result, organised crime is increasingly framed as a security threat, rather than solely a law enforcement issue. The European Union, for instance, identifies organised crime as "a key threat to […] internal security" (European Parliament, 2024, p. 2). This shift in perspective reflects the recognition that organised crime can have systemic effects on governance, economic stability, and societal resilience.

Importantly, there is a significant overlap between organised crime and the activities typically associated with hybrid threats. Many of the activities attributed to hybrid threats, such as cyber operations, economic coercion, or covert influence, can also be carried out by organised criminal networks. As such, organised crime can itself constitute a form of hybrid threat. As Lamb (2021) argues, "in several respects, organized crime is similar in nature and intent to hybrid warfare. Both seek to operate from the shadows, both create counter cultures, and have sophisticated organizational structures which make identifying key players and their real intent extremely difficult" (p. 4). This overlap is crucial for the present analysis. While organised crime is traditionally conceptualised as a non-state phenomenon driven by profit, its characteristics – covert operation, transnational reach, and access to illicit infrastructures – make it particularly suitable for use within hybrid threat environments. This raises the question of how organised crime can move beyond being an independent threat actor to becoming an instrument within broader strategic dynamics.

Geocriminality: When Organised Crime Is Used as a Hybrid Threat

As Schuett & Schramm (2025) state, "today's criminal syndicates are not just crisis profiteers; they increasingly operate on behalf of states. In doing so, they blur the lines between internal and external threats. The concept of geocriminality – where crime functions as a tool of geopolitical ambition – is no longer theoretical". The previous sections have demonstrated that threats emanating from organised crime activities conducted by non-state actors overlap significantly with hybrid threats typically associated with state actors. As Europol (2025) highlights, hybrid threats "encompass a range of criminal activities and tactics, such as sabotage of critical infrastructure through digital or physical means, information theft, disinformation campaigns, cyber-attacks, migrant smuggling, certain types of drugs trafficking and other forms of crime" (p. 14). In this sense, organised crime activities can directly contribute to hybrid threat dynamics. For instance, in the realm of economic coercion and sabotage, hybrid actions may include targeted economic pressure, manipulation of supply chains, and financial disruption via criminal networks (cf. Aukia & Ingibergsson, 2023). Such disruption can take the form of large-scale fraud, ransomware operations, money laundering, or sanctions evasion through illicit trade, falsified shipping documents, and front companies.

The present thesis therefore assumes, in line with existing literature, that organised crime conducted by non-state actors can constitute a hybrid threat when its activities extend beyond individual targets and affect state security at a broader level. At the same time, hybrid threats

are also employed by states against adversaries, which highlights a convergence between state-driven strategies and criminal activities. This overlap reveals the strategic potential of organised crime as part of the hybrid threat toolkit, making it available for instrumentalisation by states; and this strategic potential has long been recognised by states. Organised criminal groups have a long history, and the use of criminal activity for state purposes is equally longstanding. Historical examples such as the Opium Wars illustrate early forms of state-backed criminal commerce (cf. Derks, 2012, p. 684; Short, 2022, p. 115). What is relatively new, however, is the conceptualisation of this phenomenon. The term geocriminality captures this dynamic:

Definition	Geocriminality can be described as the "state-led instrumentalization of organized crime and criminal actors abroad to achieve foreign and domestic policy priorities" (Thorley, 2025).

Importantly, geocriminality shifts the analytical perspective. While traditional approaches frequently focus on organised crime infiltrating the state, for instance, through corruption or collusion, the concept of geocriminality reverses this relationship (cf. Bagley et al., 2019, p. 3). Here, the state is the primary actor that instrumentalises organised crime for strategic purposes. This does not exclude individual-level collusion; as Decoeur (2018) claims, "state officials may engage in organized criminal activities to generate personal profit, or to further the state's objectives" (p. 17). However, geocriminality emphasises the strategic use of organised crime as part of broader state behaviour.

In this regard, organised crime can be understood as a proxy instrument. As Thorley (2025) observes, "various state actors are directing criminal proxies abroad to carry out assassinations, disinformation campaigns, cyber attacks and sabotage, to gather intelligence and move money, gold or sanctioned goods". This aligns with broader understandings of proxy use in international relations, where actors are supported directly or indirectly in pursuit of strategic interests (cf. D'Cunha et al., 2025). As Cockayne (2016) further argues, criminal groups may form strategic alliances with states, positioning themselves within a broader "market for government" (p. 282). In the context of this thesis, a proxy is understood as an actor that is not formally part of a state's institutional apparatus but whose actions serve – intentionally or unintentionally – the strategic interests of a state. It is of utter importance to stress that such relationships do not require direct command or full control. They may also exist where a state tolerates, enables, or passively benefits from the activities of organised criminal networks.

Geocriminality is not limited to major powers or highly capable states. As Behalal (2025) illustrates with the example of Rwanda's involvement in the M23 crisis, even smaller or medium-sized states can instrumentalise elements of organised crime as tools of conflict. More relevant than state size is the form that geocriminality takes. Thorley (2026) distinguishes between episodic and systemic geocriminality. The "'episodic' form refers to the state instrumentalisation of crime for distinct tasks while the 'systemic' form is a longer term configuration where criminals are tolerated and in some cases actively supported by the state

so long as the criminals' activities generate sufficient benefit for the state" (p. 2). Episodic geocriminality tends to be more visible and easier to operationalise, whereas systemic geocriminality involves sustained and less direct forms of influence, shaping "criminal behaviour towards state ends" (Thorley, 2026, p. 6) over time.

All in all, the concept of geocriminality provides a framework for understanding how organised crime can move beyond being an independent non-state threat actor to becoming an instrument of state strategy within hybrid threat environments. This conceptual framework, however, does not yet explain why states choose to employ organised crime in this way. Addressing this question requires an analysis of the underlying incentives and causal mechanisms, which is developed in Chapter 4. Before doing so, the following section establishes the theoretical perspectives that underpin this analysis.

3.2. Theoretical Perspectives

The analysis of organised crime as a hybrid threat to state security is informed by a critical security studies perspective that draws on realist assumptions about state interests while simultaneously recognising blurred boundaries between state and non-state actors, proxy dynamics, and the strategic role of organised criminal actors in contemporary security environments. Rather than adhering to a single theoretical tradition, this thesis adopts a pluralist approach that combines insights from Realism, the English School, Game Theory, as well as Principal-Agent Theory. These perspectives – albeit introduced briefly, as over-theorisation is to be avoided – provide the theoretical foundation for connecting these concepts.

Realism

Realism provides an important genesis for understanding state behaviour. Classical and neorealist approaches conceptualise international relations as a realm of competition between self-interested, rationally acting states. A bedrock assumption of realism is that international politics is axiomatically anarchic and that states constitute the primary actors seeking survival within the international system (cf. Jordan, 2020, p. 7; Lemke, 2025, p. 195). The pursuit of survival is dependent on ensuring security, which "refers to the measures and actions taken by a government to protect its sovereignty, territorial integrity, and the safety of its citizens from external threats and internal disturbances" (Fiveable, 2024). Security, in turn, relies on a state's capacity to defend itself and is closely linked to the power it possesses.

In an anarchic world, states threaten one another, as all seek survival and power, which for Mearsheimer (2001) is "the currency of great-power politics" (p. 12). As Fisher-Onar (2023, p. 104) points out, realists frequently describe states as "billiard balls," interacting as independent actors within structural constraints. This metaphor is particularly illustrative of offensive realism, which emphasises constant rivalry, power maximisation, and the ultimate pursuit of hegemony as the best guarantee of survival (cf. Mearsheimer, 2001, p. 2). In short, states compete with other states for survival and power and constantly perceive one another as potential threats. This dynamic creates a security dilemma and incentivises states to select strategies that maximise their own advantages or minimise disadvantages rather than

prioritising cooperation (cf. Karstedt, 2014, p. 306). As De Castro (2025, pp. 6-7) illustrates, this includes not only open warfare but also activities below the threshold of armed conflict. In this sense, realist logic is directly applicable to hybrid conflict environments.

From a realist perspective, geocriminality can be understood as an extreme form of self-help. Due to the lack of an overarching authority and the assumption that states pursue power maximisation, they cannot fully trust one another and must rely on all means that are at their disposal (cf. Jordan, 2020, p. 6). Power can be "defined as the sum of all resources available to a nation in the pursuit of national objectives" (The Lightning Press, n.d.). As states remain "ceaselessly vigilant for opportunities to maximize power and/or security" (Lemke, 2025, p. 195), the instrumentalisation of organised crime can represent such an opportunity.

Hence, through this lens, the use of organised crime as an instrument of conflict reflects a cost-benefit calculation where the costs of other strategies such as employing conventional tools are simply outweighed by the benefits of employing a proxy. As Mearsheimer (2001, pp. 21, 31, 415) argues, states seek to exploit opportunities where benefits outweigh costs, while uncertainty about other states' intentions encourages risk-spreading strategies, including covert instruments. Moreover, even when states have aggressive intentions, they may lack the capability to act directly, making indirect tools more attractive. Using organised crime thus expands the strategic toolkit available to states when it comes to power competition with other players in the geopolitical arena and thereby furthers states' capacity in conflict.

These assumptions are highly relevant for explaining why states might tolerate, exploit, or benefit from organised crime in hybrid conflict settings. Realism is particularly well suited to explaining the cost-benefit calculations and incentive structures that underpin such behaviour. At the same time, a purely realist lens is insufficient. Traditional realist approaches frequently marginalise the role played by non-state actors or treat them as epiphenomenal. While liberal approaches emphasise their importance and since realism "basically declares non-state actors outside its area of responsibility" (Stengel & Baumann, 2017), this thesis conceptualises organised crime actors not as independent drivers, but as agents or tools to be instrumentalised. In this sense, state primacy remains intact while acknowledging that non-state actors can exert meaningful influence on security dynamics. Moreover, a narrow focus on material power risks overlooking the social and legal dimensions in which organised crime operates, particularly in the grey zone where state authority, illegality, and transnational networks intersect.

The English School

To complement the realist perspective, this thesis also draws on the English School of International Relations. The English School shifts the analytical focus from the international system to international society, emphasising shared rules, norms, and institutions, as well as the tension between order and justice. While, similar to realism, it recognises anarchy, it differs in how states respond to it (cf. Lemke, 2025, p. 193). Rather than focusing solely on power maximisation, it highlights the emergence of an international society structured by shared

institutions such as sovereignty, international law, and the balance of power. Youde (2018) provides an insightful explanation of what this international society entails:

> "International society contains two key imperatives: order and justice. The members of international society desire both order and justice, but there exists a possible tension between them which colours the relationship among those members. Pluralism and solidarism provide two different understandings of the relative priority international society should place on the rights of sovereign states as opposed to the value of promoting particular rights even when they impinge upon absolute state sovereignty" (p. 16).

The international society is sustained by primary institutions such as sovereignty, war, international law, and the balance of power. The realist self-interested cost-benefit calculation is hence tipped in favour of mutual benefit within the international society. While state-centrism remains a core feature, the English School allows analytical space for non-state actors (cf. Lemke, 2025, pp. 201-203; Schuett & Williams, 2024, p. 226; Youde, 2018, p. 22).

Within this framework, organised crime occupies a particularly relevant position. It operates transnationally, challenges the distinction between internal and external security, and blurs the line between legitimate and illegitimate uses of force. Hybrid threats, including those involving organised crime, operate in the grey zone below the threshold of open conflict, thereby challenging the core institutions of international society such as sovereignty, non-intervention, and the state's monopoly on legitimate violence. Organised crime particularly contributes to this dynamic by exploiting weak governance structures and engaging in activities such as smuggling, cybercrime, or illicit financial flows that can be leveraged for strategic purposes.

Simultaneously, the English School emphasises that states operate within a normative order (cf. Schuett & Trenta, 2025). States are not purely power-maximising actors, nor are they fully constrained by international norms; rather, they operate within a society of states in which maintaining order and legitimacy is as important as pursuing strategic advantages. As Troy (2018) points out, "establishing common rules of conduct (for example, international law), international norms, and institutions (for example, the non-intervention principle) is a foundational and persistent feature of the international society" (p. 92). This creates a structural tension: states seek to influence, destabilise, or coerce others, but must avoid openly violating the norms that sustain the system. Instrumentalising organised crime offers a way to manage this tension. Relying on geocriminality allows states to act in ways that would otherwise constitute clear violations of international norms, without formally breaching those norms. In this sense, organised crime becomes a tool of statecraft.

The distinction between pluralist and solidarist perspectives further sharpens the analysis. From a pluralist lens, order and stability take precedence over justice. States may tolerate the use of organised crime as a proxy as long as escalation is avoided and core norms are not openly violated. Deniability preserves order and ambiguity prevents the breakdown of diplomatic relations. By contrast, a solidarist reading emphasises justice, human rights, and the rule of law. From this perspective, the use of criminal proxies undermines legal norms, human security, and collective trust, and is therefore harmful to the international society.

In sum, an English School perspective highlights that organised crime is embedded within the evolving structure of international society. It functions as a hybrid actor that mediates between state interests and systemic constraints, enabling states to navigate the tension between power and legitimacy. Geocriminality thus reflects not a breakdown of international society, but rather its adaptation to new forms of competition and governance in a complex, interconnected world.

Game Theory

One of the most widely used approaches to analysing strategic decision-making is Game Theory. Although initially intended to explain individual decision-making, it has long been applied in international relations to analyse state behaviour (cf. O'Neill, 1994, p. 1002). Within this framework, states are conceptualised as rational actors whose decisions are both independent and interdependent. As Jervis (1988) explains, "Game theory and Realism are generally compatible – both are structural, strategic, and rational" (p. 318). Game Theory analyses how actors choose between strategies based on expected outcomes, assuming that they act in their own best interests (cf. Chen, 2022, pp. 200-201; Kelly, 2003, p. 2). A key illustration is the Prisoner's Dilemma:

> "When two individuals are interacting, and their behaviors reward them in ways that depend on both their own actions and the actions of the other individual, one scenario that can occur is the "prisoner's dilemma." Four outcomes are possible in a prisoner's dilemma: mutual cooperation (both parties cooperate), mutual defection (both parties' defect), a sucker's payoff (received by an individual who cooperates when the other player defects), and a temptation payoff (received by an individual who defects when the other player cooperates)" (Chassay, 2019, p. 6260).

As Chassay (2019) elucidates, the temptation payoff – acting in the lines of self-interest – represents the most advantageous outcome. Applied to geocriminality, this implies that states may choose to employ organised crime if doing so provides them with a competitive advantage. The fear of receiving the sucker's payoff incentivises defection, while the desire for the temptation payoff encourages exploitation. In this sense, the use of organised crime can be understood as a strategic choice within a broader set of available options. This suggests that state A, aiming to maximise its benefits, may choose to employ organised crime, while state B would get the sucker's payoff by adhering to international rules and norms. The Game Theory therefore shows states do not simply choose war versus peace, they choose from a toolkit of strategies. Depending on what they deem strategically more beneficial, they may "substitute one foreign policy tool for another" (Salehyan, 2009, p. 2). Using organised crime as a tool represents such a strategy, expanding the toolkit and enabling more flexible engagement.

The Principal-Agent Theory

The Principal-Agent Theory provides further insights into how states operationalise such strategic choices. The principal refers to the patron, in other words, the delegating actor (the state), while the agent represents the actor carrying out tasks on the principal's behalf. In the context of geocriminality, organised crime groups function as agents. In line with the Game

Theory, the Principal-Agent Theory suggests that a principal / state actor delegates a task to a non-state agent to further its own objectives and maximise benefits while minimising costs, which is particularly useful "when the principal lacks task-specific knowledge and expertise" (Salehyan, 2009, p. 3) and especially fruitful when interests between principal and agent align (cf. Bryjka, 2020, p. 198).

At the same time, delegation complicates attribution and weakens deterrence, as "the defender is confronted with an increasing number of potential suspects" (Cilluffo & Clark, 2014, p. 50). Importantly, these relationships are not always hierarchical. As Jokinen et al. (2022, pp. 10-11) remark, actors may cooperate informally or act in parallel and relationships may evolve with time. This flexibility is particularly relevant in the context of geocriminality. States may not require full control over organised crime actors, but may tolerate, enable, or benefit from their actions. When employing organised crime, states must therefore weigh the costs and benefits of delegation, including issues of control, reliability, and potential risks.

Synthesis

All in all, these theoretical perspectives provide a comprehensive framework for analysing organised crime as a hybrid threat. Realism explains why states pursue power and may adopt indirect strategies. The English School highlights the normative constraints shaping such behaviour. Game Theory explains strategic choice among available options, while the Principal-Agent Theory clarifies how these choices are operationalised. Together, they demonstrate that geocriminality is embedded within broader patterns of strategic behaviour.

4. THE 'WHY' – STATES' STRATEGIC LOGIC

> "Obviously, we can't expect, in something that touches the behaviour of human beings, mathematical precision. We can, however, demand analytical rigour, conceptual clarity and tight reasoning that will allow us to find certain solutions to complex problems" (Jarillo, 2003, p. 2).

As J. Carlos Jarillo (2003) illustrates so aptly, strategic logic is something engrained in humans from childhood on. Something so inherently shaped by humans cannot be predicted with 100% precision or clarity. When referring to states' strategic logic, the state is seen as an actor that makes decisions based on structured reasoning; however, these decisions are ultimately made by decision-makers and state officials, shaped by their experiences, systemic constraints, and beliefs. States' reasoning builds on the calculated alignment of political goals with available resources and ways of action to ensure, in a realist sentiment of cost-benefit calculations, the attainment of the best possible outcome in any situation where strategic choices are to be made.

Generally, a state's strategic logic in the context of conflict is therefore the reasoning that underlies the choice of a particular instrument that provides "the capacity to produce effects that are more advantageous than would otherwise have been the case" (Freedman, 2014, pp. 18-19). With regard to geocriminality, analysing the underlying 'why' requires going beyond incentives and examining the strategic logic behind them. The mere existence of an incentive does not automatically translate into action. It is thus of utter importance to consider the different constituents involved in geocriminality: who is involved, what these actors seek to attain, how they aim to attain their objectives, and what their benefit is from a selected strategy.

4.1. Strategic Context: Actors, Relationships, and Interaction

When dissecting the research question into its constituent parts, one logical step is to identify who the actors involved in the interaction under scrutiny – the instrumentalisation of organised crime as a strategic tool – are. In general, three main actors can be identified: the primary actor, the state that employs organised crime; the agent, the organised criminal element, which may be an organised crime group involved in trafficking, weapons smuggling or cybercrime, to name a few; and lastly, the target, which is the state or society which the hostile act is directed against. In debates surrounding neologisms such as geocriminality and the degree of novelty attributed to 'hybrid threats', it is easy to overlook that neither the actors, nor their agents or targets, nor the underlying strategic logic are new. History reveals a multiplicity of instances in which states relied on what is now termed geocriminality to improve their standing on the geopolitical stage in the quest of furthering their strategic objectives. This historical continuity

suggests that the strategic logic underpinning the instrumentalisation of organised crime has been present since the earliest recorded forms of interstate interaction.

Historical Continuity and the Prevalence of Geocriminality

Generally, when states seek to exert influence over one another in order to enhance their position in the international system, they pursue certain foreign policy goals through employing a variety of tools. These tools have traditionally been conceptualised along the DIME framework, distinguishing the four key areas of diplomatic, information, military, and economic power (cf. Kan, 2019). As the Council on Foreign Relations (2022) observes, "each tool has its advantages and disadvantages. The trick to foreign policy-making is figuring out how to manage those tradeoffs by selecting the best combination of tools for any given situation". Ever since the emergence of the first states, divergent foreign policy goals have constituted a cause for friction, prompting states to select those instruments from their foreign policy toolbox that are the most advantageous for achieving their objectives. Simultaneously, the strategic use of organised crime has long been one such instrument and is therefore not a phenomenon limited to the 20th or 21st century.

Rather, throughout centuries, the actors and their agents have remained largely unchanged, while the domains they target and the tools they employ have evolved, diversified and adapted to an increasingly interconnected world. Globalisation and digitalisation in particular introduced new avenues for illicit activity and, consequently, for its strategic use. This is emphasised also by Jokinen et al. (2022), who state that "the employment of non-state actors (NSA) by state actors (SA) to gain levers of influence for foreign and security policy objectives is as old as the existence of states. [...] Innovations in fields such as information technology and financial services have enhanced the power of non-state actors [...] making them even more potent proxies, partners and rivals to states" (p. 4).

Illustrative examples of this historical continuity of geocriminality can be found as early as the 16th to 18th centuries during the apex of colonial expansion. For instance, the imperial efforts of many European powers such as the British Empire (cf. Clarke & Williams, 2024, p. 190) saw the collusion of states with pirates, creating a mutually beneficial and lucrative win-win arrangement in which criminal activity served as a political lever against rivals. Chambliss (1989) highlights this dynamic in the case of the French Empire whose leadership apparatus "instructed the governors of its islands to allow pirate ships safe portage in exchange for a share of the stolen merchandise. Thus, the state became complicitous in the most horrific sprees of criminality in history" (p. 186). Further examples can be found in more recent history. For instance, the U.S. government allegedly employed mafia groups in Southern Italy during World War II and in the aftermath of the war cooperated with Yakuza criminal gangs in Japan in other to further its political and security objectives (cf. Chabat, 2019, p. 16). Similarly, Grabosky (2013, p. 21) suggests U.S. involvement with criminal actors through the CIA in the context of the Cuban Missile Crisis and assassination attempts on Fidel Castro.

These examples underscore that geocriminality is not a novel phenomenon but, contrarily, has been prevalent throughout time. While the environment in which it occurs has shifted through major developments such as globalisation and digitalisation, the underlying strategic logic has remained constant. As Waugh and Yousuf (2022) emphasise, "crime [...] can be understood as part of a criminal governance strategy that is associated with the political, social and/or economic interests of state and non-state actors" (p. 2). The reference pointing to differing interests highlights the importance of examining the specific roles and characteristics of the actors involved in geocriminality. Hence, before exploring the incentives that drive states' engagement in geocriminality, it is of utmost necessity to further elaborate on the particularities of the three identified actors: the state (actor), organised crime (agent), and the target.

The State: Actor / Principal / Patron

As established in the theoretical foundation of the present thesis, particularly within a realist framework states constitute the primary actors in the analysis of geocriminality. In line with the Principal-Agent Theory, the state takes on the role of the principal, delegating tasks to an agent and acting as the patron ruling over the proxy. A variety of factors influence whether a state is prone to engage in geocriminality. Among these, regime type is particularly relevant. As Shehu (2024) puts forward, "the political system of a country, whether democratic or authoritarian also influences it foreign policy choices and interactions with other states in international relations" (p. 86). In democratic systems, checks and balances, such as freedom of expression, independent media, and the rule of law, make engagement in illicit activities more difficult and politically costly. Public opinion and institutional oversight may constrain governments from employing malign strategies. By contrast, authoritarian systems frequently face fewer internal constraints. As Giannopoulos et al. (2021) observe, "in authoritarian states, the media can seldom express criticism towards the government unless the government has vetted that criticism" (p. 17). The relative absence of checks and balances may therefore increase the likelihood that such regimes engage in geocriminality (cf. Lebrun, 2023, p. 5). This observation is supported by Liyanage (2022) and Löjdquist (2021, p. ix), who suggest a correlation between authoritarian governance and engagement in geocriminality.

Particularly interesting are the elucidations of Martin Thorley, who is often credited with developing the concept of geocriminality. According to Thorley (2025), "geocriminality is more likely to occur when a state is strong at home but isolated abroad. In authoritarian states, those in power are typically subject only to limited forms of scrutiny and accountability, and state actors are better able to utilize criminal networks without facing widespread criticism, loss of legitimacy or legal consequences". This not only echoes the previously mentioned observations regarding the greater proneness of authoritarian regimes to engage in geocriminality, but also highlights how limited accountability and international constraints such as diplomatic isolation or sanctions create incentives for covert strategies (cf. Giannopoulos, 2021, p. 16). States facing strategic constraints, including (military) power asymmetries or economic restrictions, may therefore be particularly prone to employ organised crime. Thus, while engaging in geocriminality may provide appealing avenues of action for

different regime types alike, authoritarian regimes are more likely to be the aggressor, whereas democracies, are more likely to be the target of such malign activities. Additionally of interest to mention is that this phenomenon is not limited to great powers. While the vast amount of literature focuses on major powers such as Russia or China[3], it is pivotal to take into consideration that smaller and medium-sized states such as North Korea may also rely on geocriminality, particularly as they often lack conventional means of influence in comparison to the big players. As Rauta (2025) emphasises, the sponsorship of an agent is "a strategy employed by a spectrum of state actors, ranging from great powers seeking to avoid direct conflict to weak powers aiming to gain an asymmetric advantage" (p. 7).

Hence, size is not the deciding factor when analysing the potential actors involved in geocriminality. Aspects such as regime type, level of (military and economic) power, and the presence of strategic constrains are more relevant in determining whether a state engages in geocriminality. The state – regardless of size – remains the principal actor of geocriminality and thus the hybrid threat initiator. Interestingly, however, the Hybrid Threat "concept originated from actions engaged in by weaker non-state actors to challenge stronger parties through the use of smart tactics" (Giannopoulos et al., 2021, p. 22). When scrutinising the actors involved in geocriminality, it is therefore integral to also illustrate the role played by the non-state actors which are employed as proxies by state actors.

Organised Crime: Agent / Instrument

The non-state actor involved in this interaction, also referred to as the agent or instrument, consists of organised criminal actors employed by the state actor from which the hybrid threat emanates. It is pivotal to refrain from reducing these actors to passive tools, as these entities are often highly powerful actors with significant financial resources and capabilities (cf. Monaghan & Prideaux, 2016, p. 61). As Muggah (2023) states, "criminal actors generate at least $9 trillion in earnings every year [...]. Not surprisingly, organized crime is also detrimental to peace and security. In some cases, armed criminal groups fighting with State actors or with one another generate exceedingly high levels of violence and casualty rates far exceeding those occurring in some war zones" (p. 569).

Despite the aforementioned characteristic of organised crime being focused strongly on a monetary goal, these actors possess extensive networks and influence across multiple domains. In this regard, aside from financial motivations, organised crime actors may also pursue political objectives. As Schuett & Schramm (2025) observe, they "operate with strategic intent and geopolitical consequence". Similarly, Petta Gomes da Costa (2018, pp. 19-20) argues that organised criminal actors' political ambition may function to further their goal of maximising monetary profits, but it may also be ideologically driven. In the context of geocriminality, organised crime actors transition from independent hybrid threat actors who act with strategic intent based on financial and/or political motives to agents of the state. However, they remain active entities with their separate interests and strategic calculations.

[3] Inter alia, Aukia and Kubica (2023) suggest links between Russia and China and state-crime collusion.

The Target

The third component of this interaction is the target. While the profile of the target state may vary, it can tendentially be characterised as the inverse of the actor state. Democracies, in particular, are frequently identified as more vulnerable to hybrid threats and, by extension, to geocriminality (cf. Akiyama et al., 2019, p. 5). This vulnerability and targetability by malign activity stems from a variety of structural features that are detrimental to democratic systems such as open societies, free markets, and the rule of law, which can be exploited by criminal networks (cf. Aho et al., 2023, p. 5). As Jokinen et al. (2022) point out, "democratic societies with open market economies face particular challenges in maintaining a proper balance between making countermeasures effective and safe guarding the norms and values underpinning their model of political organization" (p. 5), which is a danger also highlighted by several European ministries (cf. German Federal Ministry of the Interior and Community, n.d.).

Having strong checks and balances may decrease the vulnerability of a democratic state to be targeted or when they are targeted. At the same time, weak governance structures may further increase vulnerability. As Locke (2012) highlights, "roughly half of all illicit transactions in the world are taking place in countries experiencing a range of weak enforcement mechanisms, low levels of economic well-being, insufficient government capacity, and significant societal divisions. In these contexts, transnational criminal networks further erode state legitimacy by incentivizing corruption" (p. 1). Hence, a state might be vulnerable to being targeted in the context of geocriminality either due to its openness or due to structural weakness.

The Triangle of Interaction

The strategic context is thus a triangular one where the state engaging in geocriminality has a relationship marked by one-sided instrumentalisation with the agent (organised crime), where the relationship between the agent and the target is marked by the execution of malign action, and where the antagonistic state and the target have a relationship marked by strategic competition. In a next step, it is therefore of interest to consider the incentive structure that presents itself to actor and agent alike by considering the advantages as well as disadvantages for each connected to their engagement in geocriminality.

4.2. Incentive Structure and Structural Conditions

What are the conditions that lead to engagement in geocriminality following the cost-benefit calculations of both state and non-state actors? The incentives which states' strategic logic is based on are manifold. Before exploring the specific incentives for the state and the organised criminal actor as well as analysing the constraints and risks which fundamentally shape the decision-making of all actors involved in geocriminality, it is of particular importance to examine why covert action is chosen over overt and direct use of state capabilities.

4.2.1. Why Indirect and Covert Action?

Contemporary times are marked by "a return to great power competition" (Ball, 2018). Within this context of renewed power rivalry, the instruments that states strategically select from their foreign policy toolbox can be ascribed to different types of action, ranging from conventional tools and direct, overt action to the use of irregular means and indirect, covert action. Hybrid threats carried out by non-state actors such as malign activities stemming from organised criminal actors "may be backed covertly or overtly by states" (Schroefl & Kaufman, 2014, p. 867). It is therefore crucial not to automatically equate hybridity with covertness. Even in its most extreme form, hybrid warfare, the "overt use of armed forces […] in addition to a mix of other means" (Pawlak, 2015) remains possible.

Geocriminality, however, can be characterised as predominantly covert and indirect. It entails the outsourcing of action to criminal proxies, which allows the state to maintain internal control while simultaneously disassociating itself from the malign act. This raises a central question: why does states' strategic logic in certain structural contexts favour indirect and covert action over overt and conventional means? The answer to this conundrum lies in the recognition that states do not freely choose from their toolbox of instruments; rather, they are constrained. These constraints, be they political, economic, legal, and/or strategic, push states towards indirect and covert forms of action. As inter alia Chambers & Beehner (2020, p. 118) and Salehyan (2009) highlight, direct warfare is connected to a myriad of costs and risks for the state, which renders overt military engagement unattractive in many contexts.

> "To understand the choice to delegate, it is important to discuss the costs and benefits of direct warfare. [...] War is a costly strategy, [...] as the state burns resources and lives are lost. In addition to these direct costs, initiating a violent conflict can invite international condemnation and foreign sanctions, invite the intervention of the state's allies, and be opposed by domestic audiences who are averse to casualties [...]. Finally, invading a foreign territory requires costly intelligence gathering about terrain, infrastructure, appropriate targets, and the local population, both to mount an effective assault and to hold onto captured ground" (Salehyan, 2009, p. 11).

In contrast, indirect and covert approaches offer a wide range of core advantages. At the lower end of the conflict spectrum, states can pursue their interests "without handing [their rivals] a casus belli" (Sari, 2026, p. 31). By concealing their sponsorship within the patron-proxy relationship, states deny their adversaries a clear justification for military retaliation. Hybrid strategies are thus designed to achieve gradual gains while avoiding repercussions: they "combine a wide range of non-violent means […] to undermine […] targets […] without triggering decisive responses" (Monaghan, 2019, p. 87). As Sari (2026) further points out, "Clausewitz himself recognized that wars take place at different levels of intensity" (p. 29), where not all hostile acts involve combat and where actors increasingly rely on non-kinetic means.

This strategic environment is characterised by features such as ambiguity, incrementalism, and multidomain engagement. As Redhead (2025) illustrates, states can operate "in relative

comfort," (p. 112) confident that their actions will not provoke strong countermeasures or major disadvantages to their position within the international system. Covert action, defined as "a foreign policy tool leaders use to secretly influence foreign state and non-state actors, conditions and events [...] while concealing sponsorship" (Long, 2025, p. 91), allows states to disavow any allegations of involvement (cf. Normark, 2019, p. 3). This ambiguity is a central benefit of covert action, as it complicates attribution and delays or constrains responses by target states. Cost considerations further reinforce the attractiveness of covert action. Compared to military operations, which frequently entail financial encumbrances for the belligerents, covert strategies are often cheaper, more flexible, and easier to retract from if unsuccessful. In addition, Bryjka (2020, p. 194) emphasises that proxy-based approaches allow states to maintain deniability of responsibility for casualties, which means that they avoid the risk of negatively impacting public opinion domestically as well circumvent international opposition.

It is moreover pivotal to note that indirect and covert actions allow states to operate within the so-called grey zone, below the threshold of open conflict. Similar to covert action, hybrid threats are characterised by their ability to "avoid crossing red lines that might otherwise provoke a robust response" (Sari, 2026, p. 35). As Monaghan (2019) argues, such strategies seek to achieve objectives "while avoiding reprisal through exploiting the gray zone between peace and war" (p. 86). This blurring of boundaries is a defining feature of contemporary conflict, where the distinction between war and peace as well as between civilian and military domains becomes increasingly ambiguous (cf. Sullivan & Jones, 2024, p. 16; Mazarr, 2015, p. 62). Within this grey zone, states can exploit legal ambiguities, test thresholds, and impose costs on adversaries without triggering escalation. As Jordan (2020, p. 2) illustrates, such strategies are designed to avoid military escalation while enabling weaker actors to challenge stronger ones. Covert actions may also form part of broader grey zone strategies, which rely on "coercive behaviors […] designed to achieve strategic objectives below the threshold of open conflict" (Khoshnood, 2025, p. 1435). In this sense, hybrid threats and geocriminality represent tools that allow states to engage in continuous competition without crossing into open warfare.

Ultimately, the disadvantages of overt action, ranging from high costs to escalation risks and political consequences, stand in stark contrast to the advantages of indirect and covert approaches. By remaining within the grey zone through employing covert action, states can impose costs, test responses, avoid retaliation, and maintain plausible deniability. From a strategic perspective, this aligns closely with realist cost-benefit calculations. States are thus able to 'attack' one another below the threshold of war, weakening adversaries without triggering the legal and military consequences associated with open conflict. Simultaneously, these indirect strategies do not exclude escalation. Rather, they may prepare the ground for it in the long-run while achieving short-term gains. As Wigell (2019, p. 256) suggests, non-kinetic actions have the power to decisively weaken a target state and have the potential to lay the foundation for progressing towards conventional war. Similarly, organised crime can be used "to pave the way for more conventional military operations" (Galeotti, 2022, p. 118). In contemporary conflict, actors therefore increasingly combine conventional and irregular means

"to achieve maximum effect" (Nilsson, 2021, p. 2). As the benefits of indirect, covert action over conventional and overt means are evident, it is of interest to elucidate why the engagement in geocriminality seems to present itself as a particularly fruitful avenue and advantageous covert action to states. Why are states incentivised to employ elements of organised crime as instruments of conflict?

4.2.2. Incentives for the State (Actor)

The previous subchapter illustrated the general advantages of covert action and situated geocriminality within this domain. Building on this, the question arises why states would select geocriminality specifically as a foreign policy instrument. The advantages that present themselves to states in this context are manifold. In the following, a distinction is made between strategic, operational, and structural advantages, as well as strategic effects. It is crucial to acknowledge however that these categories are inherently interconnected and often reinforce one another. Strategic advantages such as plausible deniability and attribution ambiguity illustrate why geocriminality is politically attractive. Operational advantages, including cost efficiency and access to infrastructure, demonstrate its practical feasibility. Structural advantages such as legal gaps and opportunities for sanctions evasion expand the range of actions available to states without entailing clear legal repercussions. Finally, strategic effects such as the erosion of trust within a target state reflect the outcomes that malign actors aim to achieve. The interplay between these advantages in combination with structural constraints such as power asymmetries and risks creates strong incentives for states to instrumentalise organised crime.

Strategic advantages

One of the most central incentives states derive from employing elements of organised crime is the maintenance of plausible deniability. As Long (2025, p. 90) highlights, such deniability may in fact be implausible in practice, as indicators of state involvement may exist; however, due to the scarcity of conclusive proof, deniability persists. This allows states to pursue strategic objectives through illicit means while formally denying involvement and avoiding disadvantageous counterreactions. As Häggström (2021) mentions, "plausible deniability makes it very difficult to determine who the antagonist is in such an environment" (p. 132). The resulting ambiguity complicates the implementation of targeted countermeasures and reduces both external and internal political risks. As Chambers & Beehner (2020) argue, it decreases "domestic political risk as well as the risk of intervention by adversaries of the external sponsor" (p. 119). Covertly employing elements of organised crime to carry out illicit activities is therefore an attractive instrument of conflict for states wanting to obscure their involvement in malign conduct, allowing them to separate themselves from the actions carried out by organised criminal actors. In short, the use of organised crime enables states to distance themselves from malign activities while still benefiting from their outcomes. This raises an important conceptual question: if the state's involvement cannot be proven, does the situation still constitute a state-to-state conflict or merely a confrontation between a target and a non-state actor?

In this regard, Clausewitz's understanding of war as "a continuation of political intercourse, carried on with other means" (Clausewitz, 1976, p. 87) remains instructive. While war constitutes the apex of conflict, even in the absence of overt military force, geocriminality can be understood as such an 'other means', enabling states to pursue political objectives below the threshold of open conflict. In the context of geocriminality and maintaining plausible deniability, if a state's political goal is for instance to destabilise a neighbour or bypass international sanctions without triggering a full-scale war and therefore remaining below the threshold within the grey zone, employing elements of organised crime becomes such an 'other means' within states' strategic logic. It allows the state to pursue political objectives such as territorial influence or economic survival through non-traditional, illegal channels. While it can be argued that Clausewitz's theory does not pertain to geocriminality due to the general absence of (state-performed) kinetic violence, albeit armed criminal groups employed by states can demonstrate highly violent conduct, others such as Clark (2006, p. 425) suggest that Clausewitz's framework remains applicable even when regimes rely on criminal activity to achieve strategic aims. Similarly, de Liedekerke & Toelen (2022, p. 15) argue that Clausewitz deliberately refrained from defining a fixed level of violence required for war, allowing his theory to extend to contemporary hybrid forms of conflict.

Closely connected to plausible deniability, attribution is rendered more difficult when states are acting covertly through employing elements of organised crime, as "it's always a challenge of attribution to [...] figure out who [...] the state actors and who [...] the non-state actors" (Lopez, 2021) are. This lack of evidence limits both legal attribution and political response. Normark (2019) emphasises that employing organised crime "makes it more difficult for the targeted states to detect the harmful activity and […] attribute the harmful operation to the foreign state behind the event" (p. 3). The difficulty of conclusive attribution due to a lack of evidence therefore hinders the avenues for legal persecution as well as for ascribing a certain actor with responsibility for the action. As Redhead (2025) further explains, "the line is difficult to draw clearly, as it is perfectly possible for non-state actors to act in ways apparently consistent with a state's objectives without any direction or encouragement whatsoever" (p. 75). Hence, even when patterns of alignment between state objectives and non-state actions can be identified, conclusive proof remains elusive. Obfuscating attribution through maintaining uncertainty about the initiator of a threat is thus a benefit states may derive from engaging in geocriminality that would not be an avenue in the case of an overt approach.

This uncertainty resonates with Clausewitz's notion of war taking place "in a fog of greater or lesser uncertainty" (Clausewitz, 1976, p. 101). Geocriminality amplifies this uncertainty, placing target states in a position where attribution is both politically contested and evidentially difficult. While attribution may still occur as a political act, the absence of legal proof complicates justification of retaliation. Particularly malign states that are weaker than their target state benefit from rendering attribution more difficult, as elements of organised crime may expand the capacity of a state actor. Chinese philosopher and general Sun Tzu already stated in the context of planning strategically that "when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy

believe we are far away; when far away, we must make him believe we are near" (Sun Tzu, 2017, p. 4). However, despite a lack of evidence, attribution may still happen, as it is also political and not purely factual. Geocriminality thus does not make attribution impossible but makes it more difficult for a target state to justify retaliatory measures without being able to legally proof state responsibility.

A further strategic advantage states may achieve from geocriminality closely connected to those of plausible deniability and attribution ambiguity therefore is that of escalation control and reduced retaliation. Motivated by risk aversion, the cost of retaliation poses a constraint for states with malign intent and limits their course of actions. As detecting hybrid threats such as the one emanating from geocriminality as well as identifying the actual malign actor behind the activity is complex, retaliatory measures are equally difficult to justify (cf. Hybrid CoE, n.d.; O'Neill, 1994, p. 1009). With retaliation not being a viable option, the target state is left increasingly exposed and does not have the legal capacity to take proper countermeasures. Employing elements of organised crime as instruments of conflict hence functions as a form of escalation control for the aggressor state. As Chambers & Beehner (2020) illustrate, future conflicts are increasingly likely to play out in the grey zone between war and peace and below the threshold of open warfare. Importantly, non-violent or indirect strategies enable states to pursue objectives "while limiting the danger […] and prevent escalation to a broader 'shooting war'" (p. 119). In this sense, geocriminality functions as a tool for controlled coercion within the grey zone and play directly into the operational advantage of cost efficiency.

Operational advantages

Beyond these strategic considerations, geocriminality offers significant operational advantages, first and foremost, cost efficiency. Conventional warfare is not only politically costly but also increasingly expensive in material terms. By contrast, employing organised crime actors is a particularly attractive avenue for malign state actors, as it is comparatively inexpensive and avoids the financial encumbrances associated with large-scale military operations (cf. Galeotti, 2022, p. 11; Karlén & Rauta, 2021, p. 2058). Additionally, engaging in geocriminality not only offers the option to save costs concerning kinetic tools, but also carries the potential to reduce costs that would have otherwise flown into acquiring resources such as expertise or capabilities necessary to carry out certain malign activities. Outsourcing and delegation thus further enhances efficiency. As Salehyan (2009, p. 10) explains, states may lack the resources to carry out operations themselves and therefore rely on agents with specialised capabilities. Organised crime actors provide precisely such capabilities, allowing states to externalise operational tasks while benefiting from existing expertise and infrastructure. This reflects a broader strategic logic reminiscent of Sun Tzu's principle of subduing the enemy without direct confrontation (cf. Sun Tzu, 2017, p. 11).

Closely related is the advantage of access to infrastructure and resources. Organised criminal networks possess established logistical systems, local knowledge, and operational reach. These resources can present themselves in the form of expertise, for instance, if a state hires a hacker group to carry out a cyber-attack or the infrastructure provided by drug smuggling networks.

Cooperating with and instrumentalising elements of organised crime therefore gains the malign state "a partner that may possess greater local information and popular legitimacy" (Karlén & Rauta, 2021, p. 2053). Rather than investing financial resources as well as time into building up such networks, acting as a sponsor enables states to use established infrastructures that are controlled by organised criminal actors and delegate tasks to agents which are better equipped to achieve the strategic objectives of the state. Long (2025) describes such agents as "potent force multiplier[s]," (p. 89) offering logistics, intermediaries, and expendable operational capacity. Similarly, Normark (2019) highlights that "exploiting criminal organizations could entail utilizing established smuggling networks, the ability to provide forged documents, financial crime schemes, or simply the ability to threaten, intimidate, pressure or harm strategically important individuals" (p. 4). This infrastructure is particularly valuable in illicit domains such as money laundering, cybercrime, or smuggling where states would otherwise need to invest significant resources in developing comparable capabilities. By leveraging these existing systems, states can act more efficiently and with greater reach (cf. Burtin, 2024; Clarke & Williams, 2024, p. 200). As these infrastructures penetrate civil society and may abuse licit businesses to hide illicit activities, geocriminality poses a particularly harmful covert means that is difficult to detect and even more difficult to avert or take countermeasures against.

Flexibility and adaptability constitute further operational advantages. Organised crime is inherently dynamic, capable of rapidly adjusting routes, methods, and targets. As De Castro (2025) mentions, "organized crime is flexible […] Its trafficking tactics are innovated steps ahead of the reaction capacity of law enforcement" (p. 5). The threat posed by the adaptability of organised criminal actors is explicated also by Long (2025), who points out that "the relative anonymity of criminal actors, combined with their ability to traverse state boundaries and blend into societies, makes them attractive to states wishing to hide their coercive interferences" (p. 90). A report published by Europol (2017) similarly emphasises that criminal groups "quickly adapt to exploit new victims [and] evade countermeasures" (p. 13). This versatility enhances the effectiveness of geocriminality while further complicating detection and attribution.

Structural advantages

Structural conditions also provide important incentives for states' engagement in geocriminality. Particularly pivotal among these are legal gaps in international law concerning state responsibility and attribution – the legal grey zone. International legal frameworks generally assume that states combat rather than engage in organised crime. States are expected to be the primary adversary of organised crime and disrupt criminal activity, which may be a reason for the persisting gaps in law enforcement when it comes to states' involvement in organised crime. As Decoeur (2018) observes, "no treaty […] expressly prohibit[s] states […] from participating in or facilitating organized crime" (p. 54). This absence of a general prohibition on state participation in organised crime within international law reflects a broader perception of states as enforcers of law rather than as perpetrators (cf. Keene, 2018, p. 11; Petta Gomes da Costa, 2018, p. 25; UNODC, 2004, Art. 1).

Moreover, states almost universally hold the power to delineate legal norms, exercising control over "what gets defined as a crime" (Brandt, 2023, p. 432). Instruments such as the United Nations Convention against Transnational Organized Crime (UNTOC), which has 194 UN members as parties to the treaty, thus including states which are allegedly involved in geocriminal activities, require states to combat organised crime (cf. United Nations, n.d.). Yet, these legal instruments do not effectively prevent states from engaging in such activities. Betti (2024) observes that "countries with a high level of involvement of state-embedded actors in criminal activities are likely to continue to be involved in the various mechanisms for monitoring the implementation of treaties aimed at combating organized crime (e.g. the Conference of the Parties to the UNTOC), and even to participate in negotiations on developing new criminal justice instruments. However, their engagement is unlikely to be directed towards advancing the goals set out in these treaties". Hence, state participation in these frameworks may amount to diplomatic affectation rather than genuine commitment.

Another legal gap, which poses a structural advantage for states with regard to the engagement in geocriminality, lies in the definitional unclarity concerning whether the use of organised crime falls under use of force, as prohibited by the United Nations Charter. The prohibition of the use of force, enshrined in Article 2(4) of the UN Charter, stipulates that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state" (United Nations, 1945). However, many hybrid activities, including geocriminality, fall outside this definition, as states may use criminal networks to avoid being classified as using 'force' while still undermining their adversaries. As Sari (2026) elucidates, the concept of force "refers to armed force [...] Many hybrid threats […] fall outside the scope of the rule" (p. 35). In this context, for a state to trigger the safety measures of Article 51 – "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs" (United Nations, 1945) – is equally difficult to attain, as criminal activity often stays below the threshold of an 'armed attack', which gives malign states the capacity to avoid retaliation legally through outsourcing. This creates a gap between Article 2(4) and Article 51, allowing states to act aggressively without triggering the right to self-defence (cf. Sari, 2026, p. 37). In short, geocriminality renders retaliation hard to justify and involvement hard to prove.

Similarly, the principle of non-intervention, which prohibits coercive interference in the *domaine réservé* of a state, is difficult to apply. In general, state involvement in organised crime does not necessarily constitute unlawful intervention unless coercion can be clearly demonstrated (cf. Decoeur, 2018, pp. 67-68; Kriener, 2023). Furthermore, while organised groups act unlawfully under criminal law, states using organised crime to their own benefit raises distinct issues of state responsibility. Under the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA; International Law Commission [ILC], 2001), conduct under customary international law is attributable to a state when it is carried out by actors "acting on the instructions of, or under the direction or control of, that State" (ILC, 2001, Art. 8). Additionally, according to Article 2, a state act can only be considered as internationally wrongful when it is attributable to a state (cf. ILC, 2001, Art. 2). In practice, however, such

attribution is rarely attainable (cf. Singh, 2024). As Decoeur (2018) highlights, the main "challenge inherent in the exercise of ascertaining the existence of customary rules is particularly acute with respect to state conduct that often occurs covertly and therefore rarely attracts international attention. If a state takes issue with another state's involvement in organized crime, such matters are probably discussed through diplomatic backchannels and not on the record" (pp. 60-61). As "state practice and opinio juris are largely insufficient to support the proposition that customary international law prohibits the participation of state organs or agents in organized crime" (Decoeur, 2018, p. 63) and attribution is complex due to legal gaps regarding state responsibility, breaches of the principles of sovereignty, and non-intervention, the advantages states derive from engaging in geocriminality in the legal sphere are manifold.

Beyond the legal domain, economic incentives such as sanctions evasion also play a crucial role. States facing economic and political isolation may turn to organised crime to circumvent restrictions. The logic of sanctions evasion appears to be relatively straightforward: malign states who have been placed under a sanctions regime suffer from the economic consequences of previous actions (cf. Moiseienko, 2024, p. 18). Particularly states that are isolated politically (e.g., through the cutting of diplomatic ties) and economically (e.g., through the imposture of sanctions regimes) may strive to forge alliances or a sponsor-agent relationship with organised criminal actors, as "alliances are the primary tool for external power maximization. If states cannot develop sufficient resources domestically, their survival is best enhanced if they can add the resources of other states to their own" (Lemke, 2025, p. 195). Activities such as smuggling or shadow financial systems allow states to bypass sanctions and sustain economic activity.

A further structural advantage situated within the economic sphere is the prospect of financial gain. As Caparini (2022, p. 10) argues, the misuse of a states' authority for economic benefit is an important element of the state-organised crime nexus. While organised criminal actors are usually attributed with pursuing monetary gains, states – particularly when their economies have been weakened by sanctions regimes – can also harbour interest in financial gains. As such, engaging in geocriminality appears to offer an ideal alliance partner to achieve such goals. Particularly in constrained economic environments, states may benefit directly from illicit activities. As Schuett & Trenta (2025) point out, "many of these ventures are both disruptive (for the enemy) and profitable for those involved. Both states and criminal groups stand to gain from the collaboration and not only in financial terms".

Strategic Effects

Finally, the anticipated strategic effects of geocriminality also function as incentives. For instance, a common goal of hybrid threat actors is the destabilisation of a target state (cf. Bundesministerium der Verteidigung, 2025; Karlén & Rauta, 2021, p. 2056). Organised crime provides a useful tool for this venture, as it can force states to divert resources towards internal security, thereby exposing vulnerabilities, rendering the target more easily attackable in other domains, and blocking resources that may otherwise have been used for the build-up of defensive capabilities or to deploy countermeasures. As De Castro (2025) explains, "organized

crime [...] causes states, through their security forces, to commit enormous amounts of public resources, people and effort to mitigate or combat it, weakening them in the process" (p. 6). Beyond immediate disruption, geocriminality can generate also broader systemic effects, including the erosion of public trust and institutional legitimacy (cf. cf. ART, 2025, p. 7). As Locke (2012, p. 2) argues, building citizen confidence is a long-term process that can be deliberately undermined. Hybrid activities "are designed to create fear […] and sow distrust towards authorities" (Hybrid CoE, n.d.), targeting the core of democratic systems.

From a Clausewitzian perspective, such effects strike at the centre of gravity of a state, the fundamental sources of a states' strength being inter alia public trust, institutional stability, and economic resilience. By flooding a rival's streets with drugs or infiltrating their banking system with laundered money, the state attacks the opponent's core stability in a way a tank cannot. If legit businesses become involved in illicit activities or cyberattacks on the population can neither be prevented nor attributed to an aggressor, the convergence of exposed vulnerability and aggressor impunity critically erodes trust in core institutions which in turn harms internal cohesion, support for the government, and the trust in defence capabilities (cf. Galeotti, 2022, p. 118; Jordan, 2020, p.12). By exploiting vulnerabilities within society, geocriminality allows states to weaken adversaries in ways that conventional military means cannot. These effects are often cumulative and interconnected, producing cascading consequences that extend beyond the immediate impact of individual actions. In this sense, geocriminality represents not only a tool of coercion but a strategy of long-term destabilisation.

4.2.3. Incentives for Organised Crime (Agent)

Geocriminality requires two constituent parts in order to be performed: the actor and the agent. It is therefore crucial to take into consideration the reasons why organised criminal actors are incentivised to act as agents for the state. As Europol (2025) observes, "hybrid threat actors and criminal actors cooperate for mutual benefit, leveraging each other's resources […] to achieve their objectives" (p. 15). Despite the variety of ways in which organised criminal actors may benefit from such cooperation, two key motivators have been identified for the purpose of the present thesis and are elaborated upon in this subchapter. Before delving into these motivators, it is important to acknowledge that organised criminal actors, even when employed as agents or instruments of the state, are not mere puppets but retain agency instead. They may pursue their own interests in addition to those of the state, further contributing to the opacity surrounding geocriminality (cf. Rauta, 2025, p. 13). Organised crime itself operates on the basis of a conglomerate of incentives. Due to the elusiveness of the actors involved and the lack of reliable information on state-crime cooperation, it is difficult to pinpoint the exact motivations underlying specific actions. Nevertheless, the following two motivators may be identified as recurring incentives for organised criminal actors to engage in geocriminality.

Protection from Law Enforcement

The first key benefit organised criminal actors derive from engaging in geocriminality is the reduced risk of prosecution and extradition. States have an interest in ensuring protection from law enforcement for organised criminal actors that operate in their favour. As long as the

organised criminal actor complies with its role as an agent and maintains a mutually beneficial relationship with the state, it may expect to be shielded, at least to some extent, from investigations and legal consequences. Ensuring the continuity and feasibility of their own criminal activities is at the forefront of organised criminal actors' interests. Traditionally, corruption of state officials has been one way to achieve this, as it hinders "law enforcement, which allows them to get benefits from criminal activities. In these cases, there is an exchange of money for protection" (Chabat, 2019, p. 17). This form of protection also facilitates access to information and networks that allow criminal actors to sustain and expand their operations. Achieving protection from law enforcement through corruption "increases criminal profits and is less likely to attract the same attention and punishment as attempts to influence public officials through intimidation or actual violence" (UNODC, 2017, pp. 56-57).

Engagement in geocriminality may constitute an alternative and potentially more advantageous means of achieving such protection. Rather than relying on bribery, organised criminal actors may receive political shielding in exchange for providing services aligned with state interests. In this sense, protection is not 'free', but exchanged within a principal-agent relationship; it may simply be more lucrative to engage in geocriminality than to carry out activities without having the state as a sponsor. Becoming an agent of the state thus allows organised crime actors to operate under an umbrella of implicit state protection, enabling them to continue and expand their activities with reduced risk[4]. Closely connected to this is the benefit of increased political leverage. Through engagement in geocriminality, organised criminal actors may not only evade law enforcement but also expand their influence, power, and capabilities (cf. Rauta, 2025, p. 17). Reduced risk of prosecution may allow them to increase territorial control, strengthen coercive capacity, and gain leverage over rivals and local populations, particularly where and when state backing is present.

Economic and Material Benefits

The second key incentive for organised criminal actors to engage in geocriminality lies in economic and material gains (cf. ART, 2025, p. 6). As Luyten (2024) highlights, organised criminal actors "have only one goal in mind: making profits" (p. 3). Engaging in geocriminality can be understood as choosing a modus operandi that facilitates the achievement of this objective. By being employed as instruments of the state, organised criminal actors may gain enhanced access to smuggling routes, illicit markets, and additional resources such as weapons, intelligence, logistics, and forged documents. Their capacity to generate economic and material benefits increases, as states may provide greater leeway for criminal activities as long as these do not conflict with state objectives. In turn, organised criminal actors are able to expand their operations and improve their ability to carry out both state-directed and independent activities.

While organised crime is often primarily defined by its pursuit of financial gain, this economic power frequently translates into influence in other domains. Similar to large corporations,

[4] Authors such as Vanda Felbab-Brown (cf. Felbab-Brown (2023) and Felbab-Brown (2025)) suggest this behaviour to be applicable to alleged China-based organised crime.

organised criminal actors seek to create and maintain a favourable operating environment. Engagement in geocriminality may provide precisely such a beneficial environment, enabling them to operate with fewer constraints and greater security. At the same time, financial motivation does not exclude other drivers. As Cockayne (2016, p. 22) argues, while economic explanations suggest that criminal engagement in politics is a strategy to protect financial profit, this perspective alone is insufficient. Individual actors within these organisations are often motivated not only by profit, but also by the pursuit of power. Thus, while economic gain may constitute the primary incentive, it is frequently intertwined with other motivations, including the desire for influence, protection, and, in some cases, political or ideological alignment.

4.2.4. Constraints and Risks

"Delegation is undoubtedly risky for both sponsor and proxy, but more often than not, it is a mutually beneficial trade-off" (Rauta, 2025, p. 6). Despite the mutual benefits that state actors and organised criminal actors derive from engaging in geocriminality, constraints and risks must be taken into careful consideration, as they play a significant role in the cost-benefit calculations that underpin the decision to enter into such sponsor-proxy relationships. In general, states must consider a variety of factors when selecting a criminal network as a proxy. These selection criteria are based on "a combination of objective factors (i.e. the scope of common interests) and subjective factors (e.g. credibility, availability of alternatives, reputation, leaders' intentions, precision of obligations, specific strengths, etc.)" (Bryjka, 2020, p. 197). A range of such factors may pose constraints on states and in some cases also on the organised criminal actors involved.

Public Opinion and Scrutiny

States in which public opinion holds significant influence and where the population has the capacity to challenge or even remove the government must be particularly cautious when considering engagement in geocriminality. This constraint is especially relevant for democratic systems, where media scrutiny, political opposition, and institutional checks and balances are stronger than in authoritarian regimes. The presence of these mechanisms renders geocriminality a less likely instrument to be selected from the foreign policy toolbox. Public scrutiny and institutional oversight in particular discourage states from employing organised crime for strategic purposes (cf. Thorley, 2025; Chambliss, 1989, p. 204). While external pressures such as sanctions or diplomatic isolation may incentivise engagement in geocriminality, "it appears that the deeper form of state-crime activity associated with geocriminality […] comes about when regimes […] face only limited constraints domestically […]. The type of state relationship with crime signified by geocriminality could potentially be of great damage to state legitimacy were it widely known and discussed in the domestic arena. For this reason, the presence in the domestic realm of a broadly free media, independent judiciary and meaningful political opposition are all inhibitors of geocriminality" (Thorley, 2026, p. 5). Hence, the risk of reputational damage and loss of legitimacy constitutes an important constraint, particularly in open societies.

Lack and Loss of Control

Another significant risk that states must incorporate into their strategic considerations is the potential loss of control over their own foreign policy autonomy, which goes hand in hand with a lack of control over the agent. The state-crime relationship implied by geocriminality should not be understood as one in which the organised criminal actor is merely a passive proxy over which the state exercises full and uncontested control. Rather, this relationship is highly dynamic. As Rauta (2025) emphasises, "proxies actively shape the relationship with their sponsors, attracting, competing over, and sometimes even abandoning sponsors. Some proxy relationships are superficial and transactional, while others are forged in identity, ideological, or religious bonds" (p. 13). As a result, outsourcing foreign policy actions entails a degree of loss of autonomy for the state as well as limited control over the agent's behaviour. States may find it difficult to monitor, direct, or penalise the actions of their agents, particularly when interests diverge (cf. Salehyan, 2009, p. 3; Karlén & Rauta, 2021, p. 2053). This potential loss of control represents a fundamental drawback of geocriminality as a strategic instrument.

Unpredictability

Innately interwoven with the issue of control is the inherent unpredictability of organised criminal actors. By engaging in geocriminality, states align themselves with actors that operate in highly opaque environments and whose internal dynamics are often unreliable. The true intentions and trustworthiness of an organised criminal actor are complex to assess, as "criminal organizations are constantly susceptible to betrayal, defection and fragmentation. [...] The profit motive can radically undermine discipline and internal cohesion" (Cockayne, 2016, p. 40). This volatility makes it difficult for states to reliably anticipate the behaviour of their proxies. Moreover, organised criminal actors may become unreliable if their own risks increase, for instance, if their operational autonomy is threatened (cf. Karlén & Rauta, 2021, p. 2053). Hence, in such cases where they must fear restrictions in their agency, organised criminal actors may prioritise their own survival over compliance with state objectives.

Additionally, organised criminal actors "pursue their own goals independent of states. These goals might well go hand in hand with (some) states' policy aims, but they can equally conflict with them. Thus, non-state actors can be valuable allies, but they can equally hamper the implementation of states' foreign policies or in extreme cases force even great powers to adapt their foreign policies" (Stengel & Baumann, 2017). Unpredictability is therefore not only connected to the sponsor's limited capacity to monitor and control the proxy but also to the opacity surrounding the interests, capabilities, and intentions of organised criminal actors. As Bryjka (2020) points out, "surrogates often do not reveal to their patrons all the information about their own objectives, capabilities, and actions" (p. 197).

Dependency

Briefly but still important to mention is a fourth constraint that may be entailed in geocriminality: dependency. Lacking control over a possibly unpredictable agent, engaging in geocriminality may create an environment in which the state becomes reliant on the agent for

the attainment of strategic objectives, leaving the state with a certain degree of vulnerability. This risk is particularly pronounced in contexts where the state is politically and/or economically isolated and lacks alternative means of action. The greater the reliance on the organised criminal actor and the lower the level of control, the greater the vulnerability of the state. Under such conditions, there is a risk of an inversion of the principal-agent relationship, where the state becomes dependent on the agent (cf. Cilluffo & Clark, 2014, p. 50). In extreme cases, the state may even become a marionette of the very actors it seeks to instrumentalise. However, despite these constraints and risks, including the potential loss of legitimacy due to public scrutiny, the lack and loss of control over the agent, the unpredictability of organised criminal actors, and the risk of dependency, there still are cases, even though hard to reveal and even more difficult to prove, in which states' incentives outweigh these drawbacks and geocriminality is still selected as the most advantageous strategy within states' strategic calculus.

4.3. From Incentives to Action: The Mechanism Framework

Building on the previous elucidations, particularly the theoretical perspectives discussed in Chapter 3.2 as well as the incentive structures identified in Chapter 4.2, this section translates states' strategic incentives into observable patterns of action. Rather than interpreting geocriminality as a static foreign policy instrument, the present thesis conceptualises it as a dynamic process in which incentives are operationalised through a range of types of interaction between state and non-state actors. Herein, mechanisms constitute the connecting factor between *why* states are incentivised to employ organised crime as instruments of conflict and *how* these incentives materialise in practice.

Situated at the core of the process of translating incentives into action is the dynamic between the state actor and the organised crime actor. Proxy relationships do not necessarily require direct instruction or full control. Rather, they may also exist where a state simply tolerates or passively benefits from the actions of non-state actors. This illustrates that geocriminality exists within a spectrum of instrumentalisation rather than in the form of a binary of control versus non-control. States select proxies based on a myriad of factors, impacting both the form and intensity of such cooperation. In this regard, two central forms of interaction positioned at the ends of this spectrum can be distinguished: active instrumentalisation and passive benefit. In the former, the apex of geocriminality is reached where states deliberately employ organised crime actors as tools to achieve strategic objectives. In the latter, a permissive form of geocriminality manifests under the helm of state connivance where states may not directly delegate tasks but still benefit from, enable, or strategically ignore organised criminal activities.

These types of interaction can further be differentiated into stages of cooperation, ranging from toleration to cooperation (cf. Chapter 5.2.) and ultimately incorporation (cf. Chapter 5.1.). This coincides with existing typologies of state-crime relationships, which distinguish between use for political purposes, corruption-based collaboration, and deeper forms of state involvement, where the link between state actor and criminal agent falls more clearly under the concept of geocriminality (Chabat, 2019, pp. 16-17). Importantly, the degree of cooperation is not only a

strategic choice but also shaped by internal state dynamics. As Petta Gomes da Costa (2018, p. 13) points out, the state is not a unified actor but a fragmented one in which different internal actors and interests compete for power and influence over decision-making.

A further dimension concerns the temporal scope of geocriminality. As illustrated in Chapter 3.2., states may engage in organised crime on an episodic basis, for instance, for discrete operations such as cyberattacks or assassinations, or in a systemic manner, where criminal networks become embedded in long-term state strategy. This distinction is pivotal, as it affects both the stability of the principal-agent relationship and the scale of its strategic effects. As Giannopoulos et al. (2021) emphasise, non-state actors in hybrid threat environments can take multiple forms, ranging from long-term allies to short-term partners, or even "useful idiots" (p. 23), which are unaware of being instrumentalised by the state actor. States may employ these different forms simultaneously, depending on their strategic needs.

Within this context, the mechanisms identified in Chapter 2 can be framed as recurring causal trajectories that transform abstract incentives into real outcomes. Mechanisms such as plausible deniability, escalation control, outsourcing to illicit capacity, and the exploitation of criminal infrastructures describe how states translate covert activities under structural constraints into action. Simultaneously, mechanisms such as iterative disruption highlight the cumulative effects of these interactions, particularly the erosion of trust and legitimacy within target states. As Aho et al. (2023, p. 35) argue, hybrid threat activity ultimately sets out to subvert the pillars of democracy through the erosion of trust, which aligns with contemporary understandings of national security that go beyond territorial defence to include broader factors connected to societal stability (Grabosky, 2013, p. 19).

Finally, the effectiveness of these mechanisms is inextricably linked to perceptions of legitimacy. As Chambliss (1989) emphasises, "no state can survive without establishing legitimacy" (pp. 195-196). Geocriminality, by operating in legal and political grey zones, exploits this dependency through targeting not only material capabilities but also the perceived legitimacy of target states. All in all, this mechanism-based framework provides the analytical link between incentives and empirical observation. It allows the subsequent case studies to explicate how different configurations of interaction, cooperation, and temporal engagement activate specific mechanisms, thereby demonstrating the variation in states' use of organised crime as instruments of conflict.

5. CASE STUDY ANALYSIS

The previous chapters investigated the strategic logic, incentives as well as mechanisms which establish geocriminality as a form of hybrid threat activity. Building on this conceptual and theoretical foundation, the following chapter turns to the empirical analysis through the case studies of North Korea and Iran. Both cases illustrate how small and medium-sized powers, particularly those facing strategic constraints such as sanctions, diplomatic isolation, or conventional military asymmetries, may instrumentalise organised crime as a strategic tool to pursue foreign policy objectives. At the same time, the covert and opaque nature of geocriminality poses methodological challenges. As Galeotti (2019) points out, publicly available information on organised crime connections is often limited since investigations and court proceedings tend to remain concealed for long periods. The following case studies therefore rely on process tracing across publicly available reports, academic literature, and investigative journalism to identify recurring patterns and mechanisms of geocriminality.

5.1. Case Study: North Korea

North Korea (DPRK) was selected as a case study as it holds a unique position on the international stage and is widely alleged to display an extreme form of geocriminality with elements of organised crime deeply embedded within the state's strategic policy and illicit operations supporting the regime's geopolitical objectives.

Strategic Context and Structural Conditions

The DPRK is a highly centralised regime with minimal domestic constraints. There is virtually no freedom of speech and media, no political opposition or investigative journalism. Law enforcement, without exception, serves to sustain the established state apparatus rather than uphold the rule of law. Internet access is limited to a small, sycophantic elite, while the wider population is not only cut off from the outside world but regimented in a system in which human rights are effectively absent and regime control permeates nearly every aspect of human existence (cf. DiMaggio, 2022). The DPRK is therefore not merely authoritarian, but the epitome of a totalitarian regime.

Since being divided after the Second World War, North and South Korea have developed in ways that could not differ more. While South Korea experienced rapid economic growth following the Korean War (1950-53), the DPRK not only pursued isolationism with regard to prohibiting the vast majority of its population access to the outside world, but has also been isolated politically and economically by the international community. This extreme international isolation is reflected particularly in the multitude of comprehensive UN and unilateral sanctions imposed by the UN Security Council "in a bid to choke funding for Pyongyang's nuclear and ballistic missile programs" (Nichols, 2019), including inter alia bans

on fossil fuel imports as well as iron and lead exports. The Global Organized Crime Index additionally emphasises that "North Korea's participation in international frameworks is widely seen as performative, with ongoing violations of the very norms these treaties uphold" (Global Initiative Against Transnational Organized Crime [GI-TOC], 2025c, p. 6).

With few international partners available, the sanctions regime placed on the DPRK has left the state not only politically but also economically isolated, despite China remaining a long-term trading parter crucial for the regime's survival. Dependence is somewhat mutual, however, as the collapse of the DPRK would constitute an immediate danger for China with regard to an influx of North Korean refugees and the possible establishment of a 'Westernised' neighbouring state (cf. Short, 2022, p. 133). Severe economic sanctions "prohibit financial transactions [...], limit trade with North Korea via import and export bans or restrictions [...], and impose [...] restrictions on energy products" (Mallory, 2021, p. 14). These imposed constraints limit the DPRK's access to global markets and amplify its dependence on alternative revenue streams and strategic tools to circumvent sanctions.

The crippling need for hard currency is intensified by the costs related to sustaining "a large military, an expensive missile program, and a nuclear arsenal" (Short, 2022, pp. 132-133). This has inter alia led to the confiscation of the wages of "North Korean workers toiling on international projects" (Kelly, 2016) as well as the fostering of additional income streams such as weapons sales, particularly to African states, and other illicit activities (cf. Mallory, 2021, p. 7). These dynamics are furthered by a persistent power asymmetry. Compared to its adversaries, North Korea has limited conventional capabilities, which creates incentives for employing indirect strategies. Hill (2023) highlights with regard to North Korea that "states that are militarily weak on the conventional side often turn to asymmetric activities" (p. 93).

In conclusion, international isolation, economic constraints, and power asymmetry shape the DPRK's strategic environment fundamentally. In the context of a continuous conflict with South Korea and ongoing confrontation with Western states, the reliance on grey-zone activities rather than open conflict strongly influences the DPRK's strategic logic. These structural conditions incentivise the employment of covert, deniable, and illicit strategies, allowing geocriminality to function as a tool of regime survival.

Organised Crime in the Strategic Environment

Before analysing which of the identified mechanisms most strongly impact North Korea's strategic logic regarding alleged geocriminality, it is of interest to briefly scrutinise the prevalence of organised crime within the DPRK's strategic environment. The North Korean case displays a highly developed state-linked illicit ecosystem. What makes the DPRK particularly striking is not merely the toleration of organised crime but, in addition to cooperation with foreign organised criminal networks, the deep integration of organised crime into the state apparatus itself. Organised crime not only functions as an instrument of state strategy but is greatly institutionalised. Long (2025) emphasises that "criminal networks are deeply intertwined with governance" (p. 100), while Hill (2023) goes further, arguing that the

DPRK "stands out as a nation where the government itself is the criminal organization, directly conducting [...] criminal enterprises" (p. 89).

North Korea has repeatedly been accused of involvement in a multitude of illicit activities, from cybercrime (financial theft, hacking operations) to sanctions evasion networks (shipping, smuggling, shell companies), counterfeit currency and goods (cigarettes, pharmaceuticals), trafficking (humans, endangered species), as well as illicit trade (arms, drugs) (cf. Cockayne, 2016, p. 4; Hill, 2023, p. 92; Kan et al., 2010, p. 1; Kennedy & Southern, 2025; Moon, 2017). Particularly prominent are allegations in the realm of cybercrime, although "the degree to which the regime itself is involved in these is [oftentimes] unclear" (Hill, 2023, p. 93). According to the Global Organized Crime Index, the DPRK's "objective is twofold: to gather intelligence and to fund state operations" (GI-TOC, 2025c, p. 4). Alleged cybercriminal activities include "the theft of $81 million from the Bangladeshi central bank's account at the Federal Reserve Bank of New York in 2016; $13.5 million from India's Cosmos Bank in 2018; $10 million from the Bank of Chile's ATM network" (Galeotti, 2022, p. 113). Such activities are difficult to attribute due to their sophistication and are financially highly lucrative. For example, the cyberattack on Bangladesh's central bank was described as "the largest cyber bank heist in history" (Park, 2021, p. 38), while the Sony attack of 2014 and the WannaCry attack of 2017, two of the globally most significant ransomware attacks, were politically, yet not legally, attributed to North Korea (cf. Hicks et al., 2019, p. 11).

Counterfeiting and illicit trade have also been linked to the DPRK. However, as often, evidence is rare and the amount of income generated by the circulation of 'supernotes' remains obfuscated (cf. Wyler & Nanto, 2008, p. 9). Additionally, allegations of narcotics production have persisted for decades: "According to press reports and North Korean defectors, farmers in certain areas are ordered to grow opium poppies" (Wyler & Nanto, 2008, p. 5). Counterfeit cigarettes produced in North Korea have been seized abroad on multiple occasions, including "fake Marlboros, Mild Sevens, and other cigarettes [...] in Taiwan, the Philippines, Vietnam, and Belize" (Wyler & Nanto, 2008, p. 10). Other alleged revenue streams include arms trafficking as well as "illegal online gambling and cyber scams" (GI-TOC, 2025c, p. 4) supported by transnational money laundering networks.

This overview illustrates the rich 'portfolio' of criminal activities linked to the DPRK, whether conducted directly through state actors or through collaboration with foreign organised criminal networks. State involvement appears especially entrenched. The DPRK has repeatedly been accused of using diplomats for illicit activities such as the "smuggling [of] millions of cigarettes into Scandinavian countries in the 1970s" (Rademeyer, 2017, p. 9). Alleged involvement also includes incidents where the "German police arrested the North Korean deputy ambassador who possessed heroin [...], and Chinese authorities arrested a North Korean consulate employee with 9 kilograms of opium" (Kan et al., 2010, p. 11). Yet, state involvement seems to extend beyond individual officials to the degree of institutionalisation within the state apparatus itself.

In this context, Bureau 39 and Bureau 121 are particularly significant. Bureau 39, allegedly established in 1974, has been associated with generating foreign currency through counterfeiting, narcotics trafficking, sanctions evasion, and overseas front companies (cf. Galeotti, 2022, pp. 106f.; Kan et al., 2010, p. 9; Wang & Blancke, 2014, pp. 53-54). Miklaucic and Naím (2013) claim that North Korea's "government is reportedly directly involved in a wide range of transnational criminal activities sanctioned at the very highest level of the state" (p. 164). Likewise DiMaggio (2022) suggests that "Office 39 managed and laundered around $1 billion per year in stolen funds", a massive revenue for an economically depleted country.

Bureau 121, frequently associated with the Lazarus Group, has allegedly conducted cyber theft, ransomware, cryptocurrency heists, espionage, and financial cybercrime to support regime objectives, including weapons programs. DiMaggio (2022) claims that "service members from Unit 121 train and operate out of the basement of a restaurant attached to the Chilbosan Hotel, [...] in Shenyang, China" (DiMaggio, 2022). Given the country's "dismally poor [internet] infrastructure, cyber operations are almost certainly orchestrated from outside the country" (Lee, 2015). It is however important to mention that attribution remains contested. For instance, Lee (2015) observes that "the hack on Sony Pictures [...] could easily have been carried out by another sophisticated group simply emulating Bureau 121's style". These instances demonstrate the complexity of attribution as well as the challenge of distinguishing whether this still falls within the spectrum of geocriminality or is straightforward state crime. Consequently, the DPRK is frequently described as a criminal state (cf. Kan, 2019).

Crucial for the analysis of geocriminality is not merely state crime itself but the relationship between state and organised criminal actors. Albeit many alleged criminal activities appear incorporated in state structures, the DPRK's lack of openness and international isolation make foreign organised criminal networks important intermediaries. These criminal networks may be useful for procurement, shipping, money laundering, and sanctions circumvention. As Thorley (2026) argues, "geocriminal activity exists on a spectrum", ranging from clandestine diplomacy to "state crime itself: not simply state instrumentalisation of criminal elements abroad but also the state carrying out criminal activities" (p. 9). While Thorley (2026) suggests that "Bureau 39's activity does not neatly accord with the forms of geocriminality", he points out "that at this network's periphery there are instances of geocriminality, where the state has entrenched relationships with criminal networks it is able to instrumentalise and by which it pursues wider state objectives" (p. 9).

The DPRK has repeatedly been accused of cooperating with foreign organised criminal groups such as the Japanese Yakuza and Chinese triads (cf. Amerhauser & Goodwin, 2026, p. 25; Davies et al., 2023; Kan et al., 2010, p. 18; Wang & Blancke, 2014, p. 55). According to the Global Organized Crime Index, different actors in multiple "South East Asian and African nations are engaged in trade and logistical support, while mafia-style groups like the triads and the Yakuza assist in arms trafficking, oil smuggling and counterfeit operations" (GI-TOC, 2025c, p. 5). Additionally, Greitens (2014) importantly observes a pivot from the use of diplomats to increasing employment of foreign organised criminal actors: "drug activity inside

North Korea appears to have shifted away from an industry marked by regime sponsorship to one primarily characterized by quasi-private production and crony capitalism" (p. 78). Likewise, "North Korea began relying less on its own officials for distribution and more on organized crime" (Greitens, 2014, p. 31).

Mechanism-Based Analysis (Process Tracing)

The North Korean case displays active instrumentalisation of elements of organised crime to the point of high-level integration. According to Greitens (2014), this systemic form of geocriminality can be described as state-sponsored constitutes a core "policy, orchestrated, managed, and supported by the central government" (p. 39). This also falls within the layers of state engagement with criminal actors described by Hill (2023, pp. 90-91), ranging from passive complicity to encouragement, state-sponsorship and state-operation. Within the strategic landscape of international isolation and reliance on foreign illicit infrastructures, it is crucial to mention that the five established mechanisms are present in different levels of intensity and should not be understood as isolated phenomena, but rather as interconnected responses to geopolitical and economic constraints.

Mechanism 1: Plausible Deniability & Strategic Ambiguity

The DPRK may be incentivised to engage in geocriminality in order to avoid attribution under sanctions as well as international scrutiny, thereby minimising political, legal, and military consequences. Being under a strict and long-term sanctions regime, fragmenting the links between state structures, such as Bureau 39, and illicit operations functions as a means to prevent further sanctions to be imposed (cf. Salisbury, 2024, p. 2). The concealment of operations and obfuscation through collaboration with foreign organised criminal actors thereby renders attribution more complex, delays or constrains responses by target states, and reduces the risk of retaliation. Plausible deniability in the DPRK case is thus not solely achieved through secrecy, but through the deliberate fragmentation of operational chains.

The cyber operations allegedly carried out by the DPRK frequently resemble criminal cyber activity, allowing the state to deny direct involvement while still benefiting strategically. As Park (2021) elucidates, "the Guardians of Peace [aka the Lazarus Group] and the DPRK suffered virtually no retribution" (p. 36) for the 2014 Sony attack. This demonstrates the evident gap between political attribution, which can also lead to sanctions, and legally provable attribution. Also with regard to drugs and narcotics trafficking, establishing a quasi-domestic-monopoly and engaging foreign organised criminal actors for distribution "balances risk reduction with satisfactory profit, [...] eliminating competition over distribution, and obtaining cover of plausible deniability" (Kan et al., 2010, p. 11). Greitens (2014) explains that while production is located in North Korea, "drugs were handed off in large-scale shipments to criminal organizations for the final stages of transportation and distribution. Organizations such as the Japanese yakuza and the Chinese triad gangs would pick up packages of drugs dropped at sea, or would rendezvous with North Korean vessels in order to obtain a shipment" (p. 24). The strategic value therefore lies not merely in illicit production itself, but in outsourcing

transportation and distribution to foreign criminal actors, fostering the creation of additional layers of deniability. As Wang and Blancke (2014) point out, “there is little evidence of drug seizures linked directly to DPRK state institutions” (p. 52).

On the whole, it can be suggested that this mechanism is somewhat less central to the DPRK’s strategic logic than others, as North Korea already remains heavily sanctioned despite little provable legal responsibility. Plausible deniability thus does not necessarily prevent political consequences, though it still complicates legal attribution and constrains direct retaliation.

Mechanism 2: Escalation Control (Threshold Management)

In order to avoid military confrontation with stronger adversaries while still exerting pressure, reliance on non-kinetic and deniable activities through criminal actors may be an attractive means for the DPRK to attain strategic objectives. By maintaining sustained pressure without triggering escalation or military retaliation, for instance through perpetrating “cyber-dependent crimes and financial crimes operat[ing] through technological means, manipulation and fraud rather than physical coercion” (Global Initiative Against Transnational Organized Crime [GI-TOC], 2025a, pp. 14-15), the DPRK has largely avoided collective defence responses beyond sanctions. This allows for continuous low-level confrontation and demonstrates how geocriminality can function as a form of grey-zone conflict.

Non-kinetic ways of engaging in power competition, such as employing organised criminal groups for the distribution of counterfeit pharmaceuticals or procurement of sanctioned materials, are particularly suitable for the DPRK due to persistent power asymmetry. Despite possessing one of the world’s largest standing militaries and a nuclear arsenal (cf. Short, 2022, p. 37), North Korea remains heavily constrained economically. As Hill (2023) elaborates, states “can leverage TOC [Transnational organised crime] to offset disadvantages in the security and economic realms” (p. 91). Hence, geocriminality enables North Korea to engage in conflict through fusing the operations of state and non-state, domestic and foreign actors, thereby creating transnational ‘supply chains’ for illicit activities beyond its borders. While cybercrime may largely rely on state actors, operations involving counterfeit currency, narcotics, pharmaceuticals, or sanctioned materials depend heavily on foreign organised criminal actors for transportation, laundering, and distribution.

Mechanism 3: Outsourcing to Illicit Capacity (Cost Efficiency)

With the motive of compensating for limited domestic capabilities due to the regime’s de facto isolation, employing elements of organised crime functions as a means to access already existing illicit capacities abroad. It is crucial to highlight that this mechanism appears less prominent in the DPRK case compared to other mechanisms. The avoidance of building costly state capacities does not seem to concern the state to the same extent as it does other actors, particularly due to the high degree of institutionalisation of illicit activity within the DPRK.

Rather than reducing institutional exposure, outsourcing appears more relevant with regard to accessing specialised skills and infrastructures outside North Korea’s immediate reach,

particularly in transportation, laundering, and distribution. As Amerhauser and Goodwin (2026) mention, illicit expansion is facilitated through "countries where protection can be bought" and networks providing "a sufficient shield from outside eyes" (p. 15). In the DPRK's case, this is particularly relevant for maritime smuggling and transnational logistics.

It is further pivotal to note that the relationship between the DPRK and organised criminal actors should not be understood as purely hierarchical. In many cases, these relationships appear transactional and mutually beneficial. Foreign criminal actors are likely to cooperate because sanctions regimes and illicit markets create profitable opportunities. In this regard, the DPRK case showcases not merely outsourcing, but also a form of symbiotic interaction between state and criminal actors.

Mechanism 4: Exploitation of Illicit Infrastructures (Sanctions Evasion)

As a state under a heavy sanctions regime, the possibility to circumvent sanctions and economic restrictions and thereby ensure regime survival appears to be the most important incentive for North Korea to engage in geocriminality. By making use of foreign criminal infrastructures, such as smuggling routes, front companies, shell corporations, casinos, and actors involved in money laundering and illicit finance, the DPRK can ensure continued access to goods, capital, and markets while reducing the effectiveness of sanctions. Access to illicit infrastructure is central to North Korea's survival strategy. This "allows North Korea to feed its overriding need for hard currency to maintain the incumbent political regime in power and fund nuclear weapon and ballistic missile programs" (Mallory, 2021, p. 43). The DPRK case strongly suggests that sanctions themselves may contribute to deeper integration into transnational criminal ecosystems, as increasing restrictions incentivise reliance on illicit infrastructures abroad.

Using illicit infrastructures and criminal actors abroad, "North Korea has historically turned to the gambling industry for solutions, laundering money through casinos in Macau and South East Asia" (Kennedy & Southern, 2025). Especially Macau provides a crucial "window to the outside world" (Crowell, 2006) for North Korea. Similarly, "millions of dollars stolen from the Bangladesh Central Bank by North Korean hackers in 2016 were laundered through Macau junkets" (Davies et al., 2023). Cases like this demonstrate that geocriminality functions not merely as a means of profit generation, but as a mechanism of strategic adaptation under conditions of prolonged geopolitical containment. Other means of sanctions evasion are the employment of organised criminal actors for the transfer of counterfeit products over sea routes from North Korean territory abroad. For instance, in September 2022, the tanker *Unica* was allegedly involved in "a ship-to-ship transfer of oil in violation of UN sanctions on North Korea. The Unica is one of just three foreign vessels that still sails straight to North Korea" (Davies et al., 2023). Such opaque shipping networks demonstrate how criminal infrastructures sustain the DPRK's operational flexibility despite international restrictions.

Mechanism 5: Iterative Disruption & Cascading Destabilisation

Literature does not provide vast amounts of proof that cascading destabilisation constitutes a central strategic objective for North Korea, as the need for hard currency and sanctions evasion

appear to remain primary. However, it can be argued that repeated illicit operations nonetheless generate cumulative systemic effects which should not be underestimated. Counterfeit currency in particular appears to be such a means. “The U.S. Secret Service has said on several occasions that the North Korean-manufactured counterfeit U.S. $100 bills currently in circulation are the most sophisticated in the world” (Kan et al., 2010, p. 12). While highly lucrative – estimations range from $15 million to as much as $250 million in gains (cf. Greitens, 2014, pp. 25-26) – these operations may simultaneously undermine confidence in financial systems. As Greitens (2014) eludes to, “media reports have sometimes also suggested that seizures are not publicized because of fears about the impact on confidence in the U.S. currency worldwide” (p. 26).

Additionally, “North Korea’s drug trafficking also contributes to the deterioration of public health in countries where its product is sold. In Japan, it is estimated that some where between 40 to 67 percent of methamphetamine comes from North Korea, and has contributed to the rise in the numbers of addicts seeking treatment and rehabilitation” (Kan et al., 2010, p. 19). Such operations contribute to broader social and economic costs within target states. Simultaneously, persistent sanctions evasion through criminal infrastructures may gradually weaken the effectiveness and credibility of international sanctions enforcement itself. Consequently, while cascading destabilisation may not constitute the DPRK’s primary objective, the cumulative effects of repeated geocriminal activity can contribute to broader systemic vulnerabilities over time.

Interim Conclusion

Process tracing of the five established mechanisms suggests that the DPRK displays long-term, systemic geocriminality in its most extreme form. Organised crime is not merely instrumentalised as a tool of conflict and power competition but deeply embedded within state strategy to the point of institutionalisation. The lines between principal and agent blur to the extent of producing one state-led criminal actor. The geocriminal relationships with foreign organised criminal networks are marked by deep integration into foreign and security policy objectives. The dominant mechanisms in the North Korean case are M2 and M4 in particular as well as M1 and M3. M5 appears to constitute a welcome side effect rather than the primary objective of the DPRK.

The analysis suggests that North Korea’s strategic logic focuses on regime survival under conditions of sanctions and isolation despite limited domestic kinetic capabilities. With regard to M4 and sanctions circumvention, it is crucial to notice that in contrast to other nations, such as Iran, sanctions appear less effective against North Korea, as the DPRK has been subject to an extensive sanctions regime for decades and is thus better adapted to anticipate their effects. Additionally, “North Korea has no major foreign banks operating inside its territory, and its industries do not rely to the same extent on the dollar as an international reserve currency. [...] This limits the regime’s vulnerability to the global financial system at large” (Greitens, 2014, p. 109). As Rademeyer (2017) suggests, “economic sanctions and isolationist policies [...] will likely fuel the expansion of the regime’s illicit activities and state-sponsored criminal networks.

As legitimate revenue sources dry up, the quest for dark money to bolster the Kim regime is almost certain to intensify" (p. 29).

Overall, the case provides strong empirical support for the argument that states can employ organised crime as a structured, strategic instrument of conflict. However, North Korea differs from other cases in which states merely outsource to non-state criminal groups, such as mafias, militias, or cartels. In the DPRK, criminal structures appear directly integrated into the state-security apparatus itself. North Korea hence may be described not just as 'using' organised crime, but as a state-criminal hybrid system. The present thesis nevertheless argues that geocriminality exists on a spectrum, with North Korea representing an extreme form in which the distinction between state institutions and organised criminal enterprise becomes increasingly blurred.

5.2. Case Study: Iran

Iran was selected as a case study on the one hand due to its long-term alleged link to organised criminal groups and militias, its contemporary relevance in the global security context, and its situation in a strategic environment shaped by long-term conflict – largely below the threshold aside from the most recent developments of 2026. The analysis below reveals striking parallels in the strategic logic of North Korea and Iran regarding the engagement in geocriminality. However, it is pivotal to take into account differences in the structural conditions that underpin the possible incentives for both states to employ elements of organised crime as instruments of conflict.

Strategic Context and Structural Conditions

Iran's geopolitical environment is marked by the legacy of foreign influence, long-standing confrontation with the United States and Israel, and regional rivalry with Saudi Arabia and the Gulf states. As Esfahani (2018) points out, "the Great Powers' interventions continuously undermined the country's sovereignty in various forms, including colonial concessions" (p. 433). This intrusion of foreign powers into Iranian domestic politics did not end with the colonial era, but remained a recurring feature of Iran's modern history. For instance, "in 1953 a coup organized by the United States and the UK overthrew the democratically elected Mohammed Mosaddegh" (Short, 2022, p. 227).

What makes Iran such a hotspot for strategic competition is both its geostrategic location as well as its vast resource wealth, particularly oil. Located at the intersection of the Middle East, Central Asia, and the Persian Gulf, Iran occupies a crucial position within regional trade and global energy flows. As Short (2022) recognises, Iran's strategic importance has not gone unnoticed in contemporary great power competition; for example, China has sought "to make Iran a major hub in the Belt and Road Initiative (BRI), investing up to $400 billion in return or discounted oil. The Strait of Hormuz is a strategic maritime chokehold where 90 percent of global trade by weight and 20 percent of global crude oil flows across" (p. 230). Consequently, Iran has become a focal point of regional and international strategic competition.

These geopolitical conditions have inherently shaped not only Iran's external relations but also its self-perception. With regard to its domestic politics, the regime is frequently portrayed as highly restrictive, characterised by restrictions on media freedom, limited political participation, and persistent human rights concerns, particularly in light of the 2011 Arab Spring uprisings (cf. Lebrun, 2026, p. 9). Following the 1979 Islamic Revolution and the ousting of the Shah, Iran increasingly consolidated power and, as Short (2022) argues, "is moving from a clerical to a military autocracy with the military taking more control" (p. 228).

Concerning its foreign policy, Iran has been perceived as a revisionist and often aggressive actor. The 1979 hostage crisis and subsequent efforts to expand the reach of its domestic revolution contributed to growing regional fears and fostered diplomatic isolation. However, from the Iranian perspective, repeated experiences of foreign intervention and exclusion promoted a strong sense of distrust towards the international community. As Esfahani (2018) illuminates, "being unfairly treated [...] cemented Iran's [...] sense of victimhood, leading to a strategy of self-reliance and significant efforts towards developing its defence capabilities" (p. 437). Iran therefore inherently acts in the realist sense of security maximisation in a world where the balance of power is not tipped in its favour.

This strategic landscape became particularly important following the introduction of a strict sanctions regime in the aftermath of the 1979 Revolution. Sanctions intensified further in response to concerns surrounding Iran's alleged development of a nuclear programme, exerting economic pressure on an already diplomatically sequestered state. The resulting strategic constraints significantly restricted access to international markets as well as foreign investment, limiting Iran's access to the international financial system increasingly (cf. Clarke & Williams, 2024, p. 195; Keatinge, 2023, p. 1).

The existing power asymmetry, which has only been furthered by economic constraints, cannot be balanced out by Iran's considerable military capabilities, which have been significantly curtailed with sanctions complicating the acquisition of defence-related inputs and rendering the maintenance of "its military arsenal through formal channels" (Mailey, 2024, p. 7) virtually impossible. Simultaneously, Tehran has been left depleted, facing the challenge of sustaining regional influence despite political isolation, economic constraints, and a persistent need for hard currency. These pressures combined with recurring conflict reinforced what Esfahani (2018) describes as an "added emphasis on self-sufficiency, based on the bitter lessons of its war with Iraq" (p. 442).

The crippling need to overcome these restraints while competing with stronger adversaries produced a strategic culture characterised by asymmetric warfare, indirect confrontation, and the extensive use of proxies and non-state actors. The latter constitutes a particularly attractive approach given that "adversaries have formed alliances with Iran's neighbours, enabling the deployment of air, missile and offensive cyber capabilities in countries along Iran's periphery" (Mailey, 2024, p. 5). Consequently, while the state-embedded Islamic Revolutionary Guard Corps (IRGC) is a highly relevant tool for Iran's foreign policy, Iran has increasingly relied on

non-state actors for hybrid and grey-zone approaches that blur the boundaries between state and non-state activity.

Within this strategic environment, geocriminality becomes relevant not merely as a criminal phenomenon but as a potential instrument of statecraft. As Redhead (2025) scrutinises, members of the Iranian governing apparatus are "alleged to have associations with organised crime, despite the regime's theocratic basis" (p. 83). While narcotics trafficking and organised crime are fundamentally at odds with the regime's theocratic jurisprudence (cf. Mailey, 2024, p. 41), strategic incentives often outweigh ideological inconsistencies. Clarke and Williams (2024, pp. 195-196) argue that although Iran publicly combats drug trafficking and faces significant domestic addiction challenges, enforcement is selective and international commitment of countering organised crime remains performative.

By and large, persistent sanctions pressure, geopolitical rivalry, economic constraints, and the need to sustain regional influence play directly into Iran's strategic logic and create strong incentives for the engagement in geocriminality. The overlap between proxy networks, illicit economies, and transnational criminal infrastructures provides Tehran with opportunities to pursue strategic objectives under conditions of isolation and power asymmetry. It is within this broader strategic context that the instrumentalisation of organised crime becomes relevant as a tool of conflict and competition.

Organised Crime in the Strategic Environment

The strategic importance of Iran due to being geographically situated between Afghanistan, Pakistan, Central Asia, Türkiye, the Gulf states, and Europe has been recognised by a variety of state and non-state actors. Functioning as a transit hub, the region in and around Iran is particularly attractive for actors involved in illicit activities, especially those relying on cross-border criminal infrastructures, drug trafficking routes, and smuggling corridors. The strategic environment is therefore characterised by a convergence of licit and illicit networks spanning multiple regions. Here, cooperation with both state and non-state actors plays a pivotal role. For instance, Türkiye functions as "a physical and commercial gateway to Europe for licit and illicit enterprises" (Mailey, 2024, p. 31), while non-state actors such as Hezbollah have become deeply embedded in transnational illicit networks.

Illicit activities connected to Iran are not solely carried out by non-state actors. Similar to other states prone to engage in geocriminality, Iran's governing apparatus comprises a variety of state actors allegedly connected to criminal activities. According to the Global Initiative Against Transnational Organized Crime [GI-TOC] (2025b), the "IRGC and affiliated institutions are frequently cited in reporting on illicit activities, ranging from drug and arms trafficking to financial and cyber-enabled crimes" (p. 5), while maintaining connections with domestic as well as international militant and criminal groups. Additional units, including the Quds and Unit 190, have likewise been linked to smuggling operations and cooperation with cross-border criminal actors in support of Iranian power projection beyond its borders.

The malign activities conducted by these state-embedded actors and their criminal counterparts encompass a broad range of illicit markets. Trafficking in dual-use technologies and sanctioned goods, such as "radioactive materials, weapons systems, bomb components and replacement aircraft parts" (Mailey, 2024, p. 6), is particularly significant. Interestingly, "foreign criminal actors do not maintain a strong operational presence within Iran, largely due to the dominance of state-embedded actors over key criminal markets. [...] Cross-border smuggling involving drugs, fuel and people is prevalent in regions like Baluchistan and the western Kurdish areas, often in partnership with Afghan and Iraqi actors" (GI-TOC, 2025b, p. 5).

Among illicit economies, narcotics trafficking is perhaps one of the most lucrative revenue streams. As a transit country connecting Afghanistan to international markets, Iran holds a central position within regional drug routes. Clarke and Williams (2024) suggest that Iran has been greatly involved in Afghan opium and heroin trafficking with an "estimated 60% of Afghanistan's heroin and morphine" (p. 195) going through Iran on their way to 'export' destinations, particularly in Europe. This geographical position provides criminal actors with opportunities for cooperation, profit generation, and access to transnational smuggling infrastructures extending far beyond the region itself.

In addition to narcotics trafficking, Iran's strategic environment includes informal shipping networks, illicit oil, gold, and diamond trading, hawala systems, and highly sophisticated money laundering schemes. The most prominent external agent for Iran has allegedly been Hezbollah (cf. Bryjka, 2020, p. 195; Schuett, 2024, p. 8), facilitating financial operations through its "global network of money changing and foreign exchange houses; embedment in the illicit trade in diamonds; control over cash-intensive businesses across the Middle East, Africa and Latin America; and connections to the operatives and financiers of criminal enterprises in Europe and North America" (Mailey, 2024, p. 7).

Another noteworthy example is a network named the 'Dubai super-cartel'. According to Mailey (2024, p. 10), this network includes a variety of actors in a multiplicity of countries, ranging from the Moroccan gangs located in the Netherlands to Peruvian traffickers. This mutually beneficial principal-agent relationship with Iran enables these organised criminal actors to access financial exchange and hawala systems linked to Hezbollah and Iran and in turn grants Iran access to international criminal networks for their foreign operations. Such examples illustrate that Iran's strategic environment is characterised not only by the presence of organised crime, but also by the integration of criminal networks across a variety of jurisdictions.

These overseas operations span across a broad range of activities, including arms trafficking, fuel smuggling, the Captagon trade in Syria, counterfeit goods, human trafficking, and the recruitment of labourers and militia members (cf. Chambliss, 1989, p. 192; GI-TOC, 2025b, p. 3; Mailey, 2024, p. 13). While some of these activities contribute to sanctions evasion and access to hard currency, others support Iran's regional ambitions by extending its reach into neighbouring states to influence the balance of power in its adversaries regional allies. GI-TOC (2025b, p. 3) emphasises that not only have allied non-state groups such as Hezbollah and the

Houthis been the recipient of weapons transfers, but arms such as ballistic missiles have been traced from Iran to destinations in Africa as well as Latin America.

Iran's strategic landscape is not only shaped by tangible criminal activities. Organised crime is increasingly present within the cyber domain. Criminal syndicates, hackers-for-hire, hacktivists, and Hezbollah-linked actors have been associated with a variety of cases of ransomware, denial-of-service attacks, data theft, cyber-spying and disinformation campaigns (cf. Giambertoni, 2025, p. 1; Rauta, 2025, p. 8). According to the GI-TOC (2025b), many of these activities have been linked to actors "targeting political adversaries and critical infrastructure in Western Asia, Europe and North America" (p. 4). The cyber domain is especially significant, as the identification of whether a perpetrated act was based on state strategy or on the monetary objectives of an independent organised criminal actor is highly complex. "Iran's cyber ecosystem is increasingly integrated into global criminal networks, with malware and hacking services procured from international cybercrime forums" (GI-TOC, 2025b, p. 5). Similarly, Cilluffo and Clark (2014) elucidate that state-sponsored hacktivists may have been involved in "the 2011 cyber attacks that brought down the Dutch firm DigiNotar" (Cilluffo & Clark, 2014, p. 56), causing significant damage to Dutch cyber infrastructure.

Finally, while alleged state-orchestrated organised criminal activity in the Iranian case is most frequently attributed to sanctions evasion and procurement, this economic rationale does not capture the full scope of Iran's strategic calculus. Another crucial objective shaping Iran's strategic environment is situated in the sphere of ideology and politics. It is essential to acknowledge that ideological motivation constitutes a parallel driver that operates alongside and frequently also reinforces material objectives. Iran has repeatedly been accused of cooperating with Iranian as well as foreign organised criminal actors, such as the Zindashti Cartel, to intimidate dissidents, discourage political opposition, and target perceived adversaries abroad (cf. GI-TOC, 2025b, p. 5; Khoshnood, 2025, p. 1440). As Mailey (2024) argues, "targets of abduction and assassination plots [often] are of Iranian descent, including dissidents and opposition groups" (p. 5). A noteworthy example occurred in Sweden in 2024, where "criminal groups such as Foxtrot and Rumba have been implicated in attacks on Israeli and Jewish targets, including an unexploded grenade found at the Israeli Embassy in Stockholm in 2024" (The Soufan Center, 2024). According to Reuters (2024), the attack was allegedly orchestrated by the Iranian regime through proxy actors.

Ultimately, Iran's strategic landscape with regard to organised crime is characterised by the interplay of proxy networks, criminal economies, and state-embedded actors. In this environment, geocriminality does not merely offer economic opportunities, but also enables access to financial and logistical capabilities crucial for regime survival and influence expansion in the pursuit of broader strategic objectives.

Mechanism-Based Analysis (Process Tracing)

Marked by long-term political isolation, extensive sanctions pressure, and the strategic objective of projecting influence throughout the Middle East and beyond, the Iranian case

demonstrates state-sponsored organised crime as well as more flexible forms of collaboration with organised criminal actors. State-embedded actors such as the IRGC, the Quds Force, and Unit 190 have repeatedly been linked to illicit activities. Long-term relationships of mutual benefit with actors such as Hezbollah or the Dubai super-cartel illustrate a broader network of cooperation extending beyond direct state control. Hence, Iran's suspected geocriminality exhibits characteristics of both systemic and episodic geocriminality: while some activities are allegedly institutionalised, others rely on ad hoc arrangements for assassinations or the temporary engagement of cybercriminals. The Iranian case is therefore particularly suitable for examining how states employ elements of organised crime as instruments of conflict. The five established mechanisms are present to varying degrees and help explain why and how organised crime may become integrated into Iran's strategic repertoire.

Mechanism 1: Plausible Deniability & Strategic Ambiguity

Iran may be incentivised to engage in geocriminality to maintain strategic ambiguity through obfuscating responsibility, thereby avoiding attribution. The use of proxy groups and criminal networks allows it to obscure direct involvement in illicit activities while maintaining influence across the region. Narcotics and weapons transfers are more difficult to trace back to the sponsor if the agents themselves rely on a variety of illicit procurement networks. This is one reason why employing Hezbollah for illicit activities adds greatly to the maintenance of strategic ambiguity. By employing Hezbollah, Iran may not only engage the terror organisation for criminal activities but, as Clarke and Williams (2024) claim, "Hezbollah itself maintains a global footprint and various connections to illicit networks and markets. This allows Iran plausible deniability and the opportunity to work through fronts and cutouts to obfuscate its role" (p. 195).

Aside from smuggling, long-term state-crime cooperation has been reported in maritime operations, where covert oil shipments, ship-to-ship transfers, and falsified shipping documentation profit immensely from collaboration with non-state intermediaries. Investigative journalism suggests that "Iranian networks are able to exploit Turkish corporate, industrial and financial sectors to circumvent international sanctions regimes with relative ease" (Bozkurt, 2026). However, as in many cases, these allegations connecting Iran to weapons trafficking, narcotics smuggling through agents such as Hezbollah or Latin American cartels, and oil smuggling are largely unsubstantiated (cf. GI-TOC, 2025b, p. 4; Levitt, 2013).

Moreover, alongside long-term cooperative relationships with established proxies, other arrangements are marked by episodic geocriminality, where "intermediaries are recruited for specific missions where attribution avoidance and local access are paramount. Their value lies in providing operational discretion" (Khoshnood, 2025, p. 1437). Obfuscation becomes particularly paramount when the damage targets the public sector and civil society. The 2022 ransomware attack on the government service of Albania exemplifies this: the attack "was claimed by HomeLand Justice [...]. Investigations established that HomeLand Justice was in fact connected to the government of Iran, and that change in attribution shaped Albania's decision to sever diplomatic relations with Iran" (Singh, 2024). This illustrates both the

complexity of legal attribution due to the use of criminal intermediaries and the fact that political attribution can occur despite a lack of evidence for direct responsibility.

The mechanism of plausible deniability also comes into play when evading accountability. Iran has allegedly hired foreign criminal individuals and groups for assassinations and intimidation attacks on diaspora, dissidents, and political adversaries (cf. Lebrun, 2026, p. 26). For such attacks, employing "intermediaries is central [...] as it enables aggressors to obscure attribution, fragment accountability, and [...] permits the regime to exert coercive pressure abroad while avoiding overt military engagement or diplomatic fallout" (Khoshnood, 2025, p. 1438). Exemplary cases include the "2015 assassination of Mohammad Reza Kolahi in the Netherlands" (Khoshnood, 2025, p. 1443), and "the recruitment of [...] Sweden's "Kurdish Fox" [...] and "the Strawberry," whose gang carried out shootings on Tehran's orders" (Schuett & Schramm, 2025). In all of these cases, publicly accessible information providing attribution evidence remains evanescent. The outcome is fragmented attribution and constrained retaliation due to reduced accountability.

Mechanism 2: Escalation Control (Threshold Management)

Iran may additionally be incentivised to engage in geocriminality to achieve escalation control. By operating through intermediaries, Iran can apply pressure on its adversaries without crossing thresholds that would provoke full-scale war. Khoshnood (2025) summarises this: Iran "faces real limits: it cannot afford symmetrical conflict with more powerful states, and official operatives are increasingly subject to international surveillance and sanctions. This strategic environment makes covert outsourcing a rational adaptation: it enables projection of force without escalating confrontation" (pp. 1446-1447). Through avoiding direct confrontation by employing agents such as Hezbollah, the Houthis, or militias in Iraq, Iran obviates the repercussions of retaliation. For instance, prior to the 2026 Iran war, Salehyan (2009) describes that it has been a long time since Iran "engaged in direct state-to-state clashes with Israel but instead assist[s] the militant organization Hezbollah as a means to increase [...] bargaining leverage and influence in the region" (p. 2). Maritime harassment, indirect pressure on shipping, and money laundering through illicit oil shipping further plays into Iran's strategic objectives while remaining below the threshold of open conflict, as the lack of attribution precludes retaliation.

Additionally, "assassinations, terror plots, sabotage and cyber-attacks are areas where Iran can rely on criminal proxies to carry out asymmetric attacks" (Mailey, 2024, p. 8). The diversification of agents and targets spreads the risk of retaliation across many actors, facilitating threshold management. The involved networks include "Turkish import/export firms engaging in money laundering; Hezbollah front companies in Lebanon; and purchasers in China using shell companies in Hong Kong. The complexity of the networks involved" (Mailey, 2024, p. 7) would require coordinated retaliation across multiple stakeholders – and consensus is difficult to achieve in a politically fragmented world. Thus, to sustain coercion and exert pressure on asymmetrically stronger adversaries (cf. Galeotti, 2022, p. 111), engaging in geocriminality to obtain escalation control is a viable option, enabling Iran to "manipulate

foreign environments, deter opposition, and enforce regime interests abroad while avoiding overt conflict, minimizing backlash, and preserving cover" (Khoshnood, 2025, p. 1439).

Mechanism 3: Outsourcing to Illicit Capacity (Cost Efficiency)

Delegating operations to networks such as Hezbollah allows access to existing criminal expertise and infrastructure while reducing the financial and political costs of direct intervention. Although Hezbollah receives "somewhere between $100 and $200 million annually from Iran" (Levitt, 2013), these costs are minimal compared to the losses from imposed sanctions, which illicit activity through Hezbollah alleviates "with estimates suggesting Hezbollah alone raises around $300 million annually from illegal activities" (The Soufan Center, 2024). Iran frequently appears to leverage existing drug routes, border smuggling networks, money laundering structures, and sanctions evasion brokers rather than creating entirely new infrastructures. This satisfies the need for specialised capability, particularly for overseas operations outside the regime's immediate reach, thereby increasing operational flexibility while keeping costs to a minimum.

For instance, "in Western contexts, Iran faces intelligence and operational constraints: limited local networks, linguistic and cultural barriers, surveillance of known proxies, and visa restrictions. Criminal groups offer local access and logistical support that official operatives often lack" (Khoshnood, 2025, p. 1438). Mexican organised criminal groups and cartels allegedly provide Iran with access to smuggling routes throughout the Americas, as "the cartels have established routes into at least 233 American cities in 48 states" (Cilluffo & Clark, 2014, p. 53) while receiving trafficked arms from Iran in return. Moreover, outsourcing pertains greatly to the cyber domain. As Cilluffo and Clark (2014) illustrate, "Iran may not possess sufficiently robust cyber capabilities with which to attack the United States, but others do" (p. 52). While Iran has invested in improving its own capabilities, outsourcing to criminal hacking groups remains a lucrative way to be cost efficient and access specialised resources (cf. Redhead, 2025, p. 85).

Mechanism 4: Exploitation of Illicit Infrastructures (Sanctions Evasion)

A further mechanism at play in Iran's alleged engagement in geocriminality is the access to illicit infrastructure. Iran has been accused of using smuggling routes, black-market trade, and financial evasion systems to bypass sanctions and sustain its regional activities (cf. Keatinge, 2023, p. 3). The incentive to circumvent sanctions is connected to ensuring regime survival under great economic and political isolation, and even more importantly to preserving strategic autonomy in the quest for greater regional and global influence. Continued access to markets and capital through criminal infrastructure reduces the effectiveness of sanctions and increases regional reach. The networks organised criminal groups offer make them particularly attractive tools for sanctions circumvention. Front and shell companies operated by Iran's agents and involved in trade with sanctioned oil are allegedly located in countries such as Türkiye, Hong Kong, and the UAE. These illegal oil shipments frequently appear to be connected to trafficking

of other goods such as gold which inter alia Venezuela has allegedly used to pay for illicit oil imports from Iran (cf. Giambertoni, 2025, p. 4; Keatinge, 2023, p. 21; Normark, 2019, p. 4).

While Iran still possesses substantial legal economic capacity, sanctions have taken a great toll on its economic and political resources and on civil society, leaving the country depleted and without sufficient inflow of hard currency through licit means. Being cut off from most financial markets and as "its presence in an international transaction is inherently criminal, Iran often relies on illicit markets out of necessity" (Mailey, 2024, p. 6). Esfahani (2018) highlights that Iran is "struggling for survival and acting in its self-interest, under extremely difficult circumstances, within an anarchical international system and a crisis-ridden region" (p. 431). The outcome is a depleted state with increased reliance on illicit actors who have the means to trade on Iran's behalf, acting almost as a lifeline, not only aiding in the acquisition of sanctioned commodities but also in revenue generation.

Mechanism 5: Iterative Disruption & Cascading Destabilisation

While iterative disruption may be a side effect of geocriminality for some malign state actors, analysing Iran's statecraft shows that the regime appears to employ elements of organised crime particularly with the intent of creating cascading destabilisation effects. Criminal networks and individual criminal actors contribute to prolonged instability by sustaining illicit economies and infiltrating governance structures. Iran may indirectly weaken its regional competitors through geocriminality, as its criminal proxies erode state authority and further corruption through smuggling-facilitated militia activity. This pertains particularly to its direct neighbours such as Iraq, Syria, Lebanon, and Yemen as well as various European countries. Mailey (2024) remarks that in Türkiye, organised criminal forces allegedly connected to Iran "have penetrated or compromised state structures. In several cases, senior politicians, including ministers and confidants of Erdoğan, have been implicated in schemes to evade sanctions or help Iranian criminals evade scrutiny or accountability" (p. 33). Such instances drive institutional degradation and governance erosion.

Additionally, geocriminality may enable Iran to create insecurity among target populations from afar. Repeated acts of violence erode trust in institutions and the security apparatus. Frequently employed grey zone operations range from assassinations and arson to espionage and surveillance (cf. Lebrun, 2026, pp. 13-14). In 2023, for instance, Magomed-Husejn Dovtaev "was convicted of spying for Tehran after carrying out surveillance on the west London headquarters of the Farsi-language TV network Iran International. The reconnaissance was part of a wider plot by others to stage a terrorist attack against the broadcaster" (Holmes, 2026). Intermediaries with specialised local knowledge as well as the use of social media platforms such as Telegram for recruitment allegedly provide Iran with additional capabilities (cf. Holmes, 2026; Khoshnood, 2025, p. 1442).

Iterative disruption also pertains to the economic sphere. As criminal intermediaries target both the public and private sectors, abuse legitimate businesses for illegitimate activities, and carry out cyber-attacks and data theft, trust in security mechanisms further erodes (cf. Europol, 2024,

p. 17; Hicks et al., 2019, p. 10). Clarke and Williams (2024) elaborate that "Iranian hackers have [...] targeted, on multiple occasions, industrial control systems in both the public and private sectors" (p. 197). Most notably, disinformation and propaganda campaigns conducted through a variety of media outlets in various European countries have repeatedly been linked to Iranian leadership, serving as an attractive means of "weakening opponents from within" (Europol, 2025, p. 15). The cumulative outcome is cascading destabilisation: economic, political, and social systems gradually erode as trust diminishes and governance capacity weakens.

Interim Conclusion

The case study analysis shows that Iran exhibits a form of geocriminality that differs significantly from the DPRK model, albeit certain similarities in the structural conditions surrounding both states. Scrutinising the mechanisms at play demonstrates that Iran does not primarily employ organised crime for regime survival alone, though geocriminality provides lucrative means to evade sanctions and boost the nation's crippled economy. Rather, geocriminality forms part of a broader strategy of asymmetric statecraft. Through the selective instrumentalisation of criminal networks, smuggling infrastructures, informal financial systems, and illicit logistics chains, Iran is able to project influence, circumvent sanctions, and exert pressure on adversaries while remaining below the threshold of conventional conflict. This makes the Iranian case particularly illustrative of geocriminality as a tool of hybrid and grey-zone competition.

5.3. Discussion

This thesis addresses a fundamental question: *Why do states employ elements of organised crime as instruments of conflict?* Geocriminality, the strategic instrumentalisation of organised crime, is inherently difficult to attribute. However, analysing examples of states that allegedly employ organised criminal actors as proxies to achieve their strategic objectives reveals tactical parallels. The cases of North Korea and Iran highlight how these mechanisms function in practice.

Shared Structural Drivers of Geocriminality

North Korea and Iran both allegedly employ organised crime as they face similar strategic constraints. Common structural conditions are the experience of extensive sanctions regimes, prolonged diplomatic isolation, long-term confrontation with the United States, and significant military asymmetry despite maintaining respectively large conventional militaries. Both regimes possess limited financial resources compared to their opponents and encounter strong incentives to seek asymmetric alternatives to conventional competition.

Organised crime functions as a form of strategic adaptation and geocriminality aids states in overcoming structural constraints. Organised criminal actors pose valuable state agents as they provide access to hard currency, enable sanctions circumvention, expand transnational reach as well as enhance covert operational capabilities. It is crucial to highlight that organised crime is not employed as a tool due to these states being weak. On the contrary, organised crime

compensates limitations in specific domains, particularly in the economic one, when states cannot exhaust licit avenues. Thus, both cases suggest that geocriminality emerges primarily as a response to geopolitical constraint rather than criminal opportunism.

Comparing the Mechanisms: Similar Functions, Different Priorities

While the case study analysis demonstrates that all five mechanisms are present in both cases, they do not carry equal explanatory weight. In the following, the five mechanisms will be discussed under the lens of comparative observation. The comparison reveals two different patterns of geocriminality:

i. North Korea primarily employs organised crime for regime survival.
ii. Iran primarily employs organised crime for influence projection and asymmetric competition.

Consequently, different mechanisms (hereinafter referred to as M1, M2, M3, M4, and M5) become dominant in each case.

North Korea: Geocriminality for Regime Survival

For the DPRK, Exploitation of Illicit Infrastructure (M4) is the dominant mechanism. Organised crime acts as a crucial lifeline for the regime, providing hard currency and sanctions evasion networks, thereby rendering M4 the strongest driver for geocriminality. This is closely supported by Escalation Control (M2), which enables continued confrontation with stronger adversaries under conditions of asymmetry, where cybercrime, sanctions evasion, and illicit trade create pressure without provoking direct military retaliation.

Meanwhile, Plausible Deniability and Strategic Ambiguity (M1) and Outsourcing to Illicit Capacity (M3) serve as secondary enabling tools. Plausible deniability complicates attribution and obfuscates responsibility, while foreign criminal actors provide laundering, transport, and distribution capabilities. Importantly, these mechanism largely facilitate M4 and M2 and exist to make the economic survival loop work. Consequently, Iterative Disruption and Cascading Destabilisation (M5) is less pronounced. While destabilisation effects exist, evidence suggests that these outcomes are largely secondary to the pursuit of revenue and sanctions circumvention. Hence, for North Korea organised crime primarily functions as a mechanism of regime survival under conditions of isolation and economic pressure.

Iran: Geocriminality for Influence Projection

In contrast, Iran's strategic logic relies heavily on Escalation Control (M2) and Iterative Disruption (M5). M2 allows Iran to project power while avoiding direct confrontation. Criminal proxies, militias, smugglers, and cyber actors enable sustained grey-zone competition. This appears to be particularly important given Iran's inability to compete symmetrically with stronger adversaries. Unlike North Korea, M5 is pivotal for Iran's strategic logic. Criminal actors contribute to the intimidation of dissidents, facilitate political coercion abroad, and add to the overall weakening of rival governance structures. These activities generate cumulative effects that expand Iranian influence over time.

For Iran, Plausible Deniability (M1) and Illicit Infrastructure (M4) act as fundamental supporting mechanisms. While shielding the regime from direct responsibility and generating revenue to bolder a sanctions-ridden economy are vital, these functions appear subordinate to broader geopolitical objectives. Finally, Outsourcing (M3) provides Iran with local knowledge, operational access, and specialised capabilities abroad, which is particularly important for operations in Europe, the Middle East, and in cyberspace. Hence, in Iran organised crime primarily functions as an instrument of influence projection and coercion within a broader strategy of hybrid and grey-zone conflict.

The comparison suggests that while both states employ organised crime to compensate for structural constraints, the dominant mechanisms differ according to strategic priorities.

North Korea	Iran
M4 – Illicit infrastructure	M2 – Escalation control
M2 – Escalation control	M5 – Iterative disruption
M1 – Plausible deniability	M1 – Plausible deniability
M3 – Outsourcing	M4 – Illicit infrastructure
M5 – Iterative disruption	M3 – Outsourcing

Table 2: Comparative Synthesis of the Five Mechanisms in the Two Cases

Distinctively, North Korean engagement in geocriminality with regard to the five mechanisms may be labelled involvement in criminal activity for survival, while in the Iranian case, engagement in geocriminality pertains rather to sponsorship of organised crime for influence.

Explaining Variation: Why Do States Use Organised Crime Differently?

While the differences in the structural environments of the DPRK and Iran may appear obvious, it is of interest to explain the variation in the explanatory weight of the mechanisms. The comparison demonstrates that the two states employ organised crime for broadly similar reasons, but the form geocriminality takes varies according to their strategic environment and primary objectives. Importantly, the central difference between North Korea and Iran is not whether organised crime is employed, but what the state ultimately seeks to achieve through it.

North Korea's extreme, near-total isolation dictates its behaviour. Operating under an extensive sanctions regime with limited legal access to international markets and few international partners, as survival becomes the overriding strategic objective, the DPRK has greatly institutionalised organised crime within state structures. North Korea does not just hire criminals, although it allegedly collaborates with organised criminal actors to extend its operational reach beyond its borders; the state is the criminal enterprise. This near-total institutionalisation explains why M4 is dominant. For North Korea, geocriminality and crime are pillars of the survival architecture.

For Iran, regional competition and influence projection are pivotal. Iran also operates in a heavily sanctioned environment but is considerably less isolated than North Korea. It possesses a robust network of regional partners, proxy organisations, and economic connections. While in need of agents for market access and sanctions evasion, Iran seeks not only survival but importantly regional influence. Organised crime is not fully integrated into the state apparatus but is an external, transactional tool. This explains why M2 and M5 are central to Iran's strategic logic, M4 remains important for regime survival, and M1 and M3 are useful and play into the realisation of operations carried out under the helm of the other mechanisms. Thus, Iran engages in geocriminality to shape political environments and project influence while remaining below the threshold of conventional war; at least until the events of 2026.

The differing state-crime relationships in the context of geocriminality can therefore be framed as a reflection of strategic priorities. For North Korea, organised crime is the system. Criminality is deeply embedded within state structures, the state and criminal enterprises increasingly overlap, and geocriminality functions as a part of the regime's survival blueprint. For Iran, organised crime is a tool. Criminal actors remain external and relationships are more flexible. Thus, the variation between the two cases suggests that the engagement in geocriminality reflects the differing priorities with regard to strategic objectives. Where the central goal is regime survival under severe isolation, geocriminality may be at play in its most extreme form to the degree of institutionalisation. Where the objectives are influence projection and economic sustenance, organised crime is more likely to be employed selectively through proxies and criminal intermediaries. The comparison therefore suggests that states do not simply employ organised crime due to the availability of criminal actors, but because organised crime provides a flexible means of pursuing strategic objectives under extreme conditions of constraint.

Why Do States Employ Organised Crime as Instruments of Conflict?

The North Korean and Iranian cases demonstrate that states engage in geocriminality, as criminal networks provide capabilities that enable states to overcome geopolitical constraints while avoiding the costs and risks associated with conventional forms of power projection. As Khoshnood (2025) points out, "unlike [...] North Korea's use of cybercrime primarily for revenue generation and sanctions evasion, Iran's approach centers on both regime protection and extraterritorial repression through the strategic use of criminals" (p. 1442). Organised crime is an attractive instrument of asymmetric statecraft. The findings suggest that geocriminality is fundamentally a strategy of asymmetric adaptations when states face restrictions in their strategic mobility, such as economic constraints, sanctions regimes, military asymmetries, and varying degrees of international isolation. Under these conditions, the advantages of engaging in geocriminality become apparent in the established mechanisms. Geocriminality should not be understood as a by-product of weak governance or corruption. Rather, the findings suggest that states can deliberately instrumentalise criminal networks as flexible, deniable, and cost-effective tools of hybrid conflict.

6. CONCLUSION

What was already observable centuries ago, when imperial powers instrumentalised pirates to advance their strategic objectives, remains applicable to today: contemporary international politics is increasingly characterised by non-state actors being included in strategic competition frequently conducted below the threshold of armed conflict. The distinction between war and peace has blurred incrementally, as states seek out methods of coercion that minimise escalation, attribution, and legal accountability. Within this everchanging security landscape, organised crime has emerged as more than a challenge to criminology. Rather, it has turned into a phenomenon capable of generating strategic effects that may reverberate through governance, economic stability, and societal cohesion. The convergence of hybrid threats and organised crime demonstrates that contemporary security threats are multidimensional and include state as well as non-state actors.

This thesis set out to examine geocriminality, states' instrumentalisation of organised crime for strategic purposes, and to answer the question: *Why do states employ elements of organised crime as instruments of conflict?* Drawing on extensive literature, IR theory, and the case studies of North Korea and Iran, the findings suggest that organised crime offers a uniquely attractive mechanism for achieving strategic objectives while minimising the costs, risks, and constraints associated with conventional forms of power competition. By cooperating with or exploiting organised criminal actors, states can exert pressure on adversaries without directly crossing the threshold of armed conflict. Hence, the strategic value of geocriminality lies not in what criminal agents can do, but in their capacity to operate within legal grey areas, shielding their patron behind a veil of deniability. Rather than replacing conventional tools of statecraft, geocriminality expands the repertoire available to states. It constitutes a rational strategic choice, particularly where direct military action, economic coercion, or diplomatic confrontation would entail excessive political, legal, military, or economic repercussions. States facing extensive sanctions, diplomatic isolation, military asymmetry, or resource constraints encounter particularly strong incentives to engage in geocriminality.

The case analysis supports the argument that organised crime functions as a hybrid threat instrument capable of producing deniable, strategically relevant effects. Its value to states ranges from transnational reach, access to illicit infrastructures, and operational flexibility to the ability to generate iterative disruptive effects. Organised criminal actors serve state interests across a spectrum of interaction, from active sponsorship to tolerance and indirect benefit. Geocriminality therefore exists along a continuum rather than as a binary distinction.

The analysis identified five interconnected mechanisms that explain why organised crime appeals to state strategists. Through plausible deniability and strategic ambiguity (M1), states are able to benefit from criminal activities while distancing themselves from direct

involvement, obscuring attribution, and being enabled to challenge adversaries due to deniability. Escalation control through threshold management (M2) enables states to engage in sustained competition without triggering collective defence mechanisms, as criminal activities frequently fall short of constituting armed attacks under international law, allowing for exerting pressure below legal thresholds. Outsourcing to pre-existing illicit capacity (M3) is a crucial tool for states to access needed resources without developing expensive capabilities, such as expertise and logistics, which organised criminal networks already possess. Outsourcing therefore reduces monetary costs as well as political risks. Exploitation of illicit infrastructures (M4) is particularly pivotal in cases where states need to ensure regime survival, for instance, due to extensive sanctions regimes. Organised criminal networks provide access to smuggling routes, money laundering systems, and extensive sanctions evasion opportunities, enabling the state to generate revenue and acquire crucial resources. Lastly, iterative disruption and cascading destabilisation (M5) entail cumulative disruptions, ranging from corruption and coercion to violent acts like assassinations, gradually eroding institutional trust and security perceptions. Geocriminality therefore enables states to weaken their adversaries without direct confrontation.

These mechanisms are observable across different geopolitical contexts. Both North Korea and Iran allegedly engage in geocriminality to support their strategic objectives. While the North Korean case illustrates a particularly institutionalised form of geocriminality where activities are closely linked to regime survival, the Iranian case displays a more flexible pattern where organised criminal actors are employed episodically as well as in some cases systemically to project regional influence and circumvent constraints. Despite differences in structural conditions and operational methods, both cases reveal a common strategic logic, and the recurrence of the five mechanisms across both cases strengthens the explanatory value of the proposed framework.

This thesis aims to bridge the gap between criminology and security studies by demonstrating that organised crime can be integrated into broader theories of hybrid conflict and strategic competition. The concept of geocriminality provides an analytical lens, while the mechanism-based approach moves beyond descriptive accounts of the state-crime nexus toward a structured explanation of state incentives. The theoretical foundations underpin this: realism's emphasis on power maximisation, survival, and state-primacy illustrates why states seek advantages through indirect means; the English School highlights the tension between strategic competition and the norms of international society; Game Theory clarifies why states may select organised crime from a wider set of options; and the Principal-Agent Theory elucidates how states operationalise such choices through delegation and proxy relationships. In sum, these frameworks demonstrate that geocriminality is neither exceptional nor irrational; it is consistent with broader patterns of state behaviour. Organised crime should be understood not merely as a law-enforcement issue but as a strategic security concern. Geocriminality offers a viable means of undermining adversaries without resorting to conventional warfare for a range of potentially malign states. Traditional responses focused solely on criminal prosecution will

prove insufficient when criminal networks become embedded within broader geopolitical strategies.

This thesis acknowledges several limitations. The qualitative small-N design, limited to two cases, constrains the generalisability of the findings substantially. Reliance on open-source material limits the ability to establish direct proof of command-and-control relationships, which is why the analysis prioritises explanatory plausibility and mechanism tracing over conclusive attribution. Future research should expand the empirical base through additional case studies and explore the dichotomy between democratic and authoritarian patterns of geocriminality.

Geocriminality reflects a broader transformation in the nature of 21st century conflict. Organised crime no longer constitutes merely a threat to states' security; it may instead increasingly be perceived as a strategic resource states can deploy to achieve political objectives. Its capacity to generate influence, disruption, and coercion renders geocriminality particularly attractive to malign states. As strategic competition unfolds progressively within the blurred grey zone between war and peace, the significance of geocriminality is likely to grow. Understanding why states employ elements of organised crime as instruments of conflict is thus pivotal for grasping the evolving character of power, security, and the international order itself.

BIBLIOGRAPHY

Aho, A., Alonso Villota, M., Giannopoulos, G., Jungwirth, R., Lebrun, M., Savolainen, J., Smith, H., & Willkomm, E. (2023). *Hybrid threats: A comprehensive resilience ecosystem*. The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/

Akiyama, C., Federici, J., & Hicks, K. H. (2019, September). *Hybrid CoE Strategic Analysis 18: China in the grey zone*. European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-18-china-in-the-grey-zone/

Amerhauser, K., & Goodwin, A. (2026, March 16). *A world of deceit: Mapping the landscape of the global scam centre phenomenon* (Research report). Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/analysis/mapping-global-scam-center-phenomenon/

ART – Analysis and Research Team. (2025, July). *Organised crime: A growing threat to democracy* (Council of the European Union). https://www.consilium.europa.eu/media/3cpejugj/2025_683_art_organisedcrime_web_july-2025.pdf

Aukia, J., & Ingibergsson, R. (2023, June). *Threat potential in the economy: From vulnerabilities to China's increased coercion* (Hybrid CoE Trend Report No. 10). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-trend-report-10-threat-potential-in-the-economy-from-vulnerabilities-to-chinas-increased-coercion/

Aukia, J., & Kubica, L. (2023). *Russia and China as hybrid threat actors: The shared self-other dynamics* (Hybrid CoE Research Report 8). The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-research-report-8-russia-and-china-as-hybrid-threat-actors-the-shared-self-other-dynamics/

Bagley, B., Gurecki, A. M., Rosen, J. D., & Chabat, J. (2019). Introduction. In J. D. Rosen, B. Bagley, & J. Chabat (Eds.), *The criminalization of states: The relationship between states and organized crime* (pp. 1-14). Lexington Books.

Ball, J. (2018). *What is security? Everything.* Global Security Review. https://globalsecurityreview.com/what-is-security-everything/

Bankov, B. (2024). Hybrid warfare: How to escape the conceptual gray zone. *Journal of Strategic Security, 17*(1), 1–23. https://www.jstor.org/stable/48766103

Behalal, Z. (2025, July 1). *The long arm of Kigali: Rwanda's use of organized crime for geopolitical interests*. Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/analysis/rwanda-drc-peace-deal-m23-organized-crime-geocriminality/

Betti, S. (2024, May 27). *Who will guard the guardians? State-embedded criminality places the criminal justice treaty framework under strain*. Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/analysis/state-embedded-actors-criminality-ocindex/

Bozkurt, A. (2026, May 4). *Turkish company linked to covert Iranian oil smuggling network exposed in US court filing*. Nordic Monitor. https://nordicmonitor.com/2026/05/turkish-firm-linked-to-covert-iranian-oil-smuggling-network-exposed-in-us-court-filing/

Brandt, M. (2023). State-organised crime. In S. Hassan & D. Lett (Eds.), *Introduction to criminology: A Canadian open education resource* (pp. 432–436). Kwantlen Polytechnic University.

Bryjka, F. (2020). Operational control over non-state proxies. *Security and Defence Quarterly, 31*(4), 191–210. https://doi.org/10.35467/sdq/131044

Bundesministerium der Verteidigung. (2025, March 20). *Was sind hybride Bedrohungen?* https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen/was-sind-hybride-bedrohungen--13692

Burtin, A. (2024, November 7). *Weaponisation of migration: A conversation with Kelly Greenhill.* Voxeurop. https://voxeurop.eu/en/kelly-greenhill-weaponisation-migration/

Calcagni, M. (2010). The conceptualisation of transnational organised crime: A historical perspective. *SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis*, (2), 72–80. https://doi.org/10.7396/2010_2_G

Caparini, M. (2022, December). *Conflict, governance and organized crime: Complex challenges for UN stabilization operations* (SIPRI Report). Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2022-12/2212_sipri_report_un_stabilization_operations.pdf

Chabat, J. (2019). Criminally possessed states: A theoretical approach. In J. D. Rosen, B. Bagley, & J. Chabat (Eds.), *The criminalization of states: The relationship between states and organized crime* (pp. 15–30). Lexington Books.

Chambers, J., & Beehner, L. (2020, May–June). Competing below the threshold: Harnessing nonviolent action. *Military Review, 100*(3), 116–126. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2020/Chambers-Beehner-Competing-Below/

Chambliss, W. J. (1989). State-organized crime. *Criminology, 27*(2), 183–208. https://doi.org/10.1111/j.1745-9125.1989.tb01028.x

Chassay, L. (2019). Prisoner's dilemma outcomes. In T. Shackelford & V. Weekes-Shackelford (Eds.), *Encyclopedia of evolutionary psychological science* (pp. 6259–6261). Springer. https://doi.org/10.1007/978-3-319-16999-6_3517-1

Chen, N. E. (2022). *A description of game theory*. *Journal of Education, Humanities and Social Sciences, 2*, 199–204.

Cilluffo, F. J., & Clark, J. R. (2014). Thinking about strategic hybrid threats—In theory and in practice. *PRISM, 4*(1), 47–63.

Clarke, C. P., & Williams, P. (2024). Organized crime and proxy wars. In A. Moghadam, V. Rauta, & M. Wyss (Eds.), *Routledge handbook of proxy wars* (pp. 189–203). Routledge. https://doi.org/10.4324/9781003174066

Clausewitz, C. von. (1976). *On war* (M. Howard & P. Paret, Eds. & Trans.). Princeton University Press.

Cockayne, J. (2016). *Hidden power. The strategic logic of organized crime*. Oxford University Press.

Council of the European Union. (2025, December 15). *Hybrid threats*. https://www.consilium.europa.eu/en/policies/hybrid-threats/

Council on Foreign Relations. (2022, February 2). *What tools do foreign policy-makers have at their disposal?* https://education.cfr.org/learn/learning-journey/tools-foreign-policy/what-tools-do-foreign-policy-makers-have-at-their-disposal

Crowell, T. (2006, January 18). *North Korea, the "Sopranos" state*. *North Korean Economy Watch*. https://www.nkeconwatch.com/2006/01/18/dprk-soprano-state-accusation/

Davies, C., Riordan, P., Chan, H.-h., & Visual Storytelling Team. (2023, March 29). *Inside North Korea's oil smuggling: Triads, ghost ships and underground banks*. *Financial Times*. https://ig.ft.com/north-korea-oil-smuggling/

D'Cunha, S., Ferraro, T., & Rodenhäuser, T. (2025, January 16). 'Hybrid threats', 'grey zones', 'competition', and 'proxies': When is it actually war? *ICRC Humanitarian Law & Policy Blog*. https://blogs.icrc.org/law-and-policy/2025/01/16/hybrid-threats-grey-zones-competition-and-proxies-when-is-it-actually-war/

De Boer, J., & Bosetti, L. (2015, July). *The crime-conflict nexus: State of the evidence* (Occasional Paper No. 5). United Nations University Centre for Policy Research.

De Castro, A. (Ed.). (2025). *Organized crime and national security in Spain: Challenges and responses*. Routledge. https://doi.org/10.4324/9781003536284

Decoeur, H. (2018). *Confronting the shadow state: An international law perspective on state organized crime*. Oxford University Press.

de Liedekerke, A., & Toelen, M. (2022). *The relevance of Clausewitzian theory in hybrid war: The Iranian-Saudi rivalry* (Hybrid CoE Working Paper 15). The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-15-the-relevance-of-clausewitzian-theory-in-hybrid-war-the-iranian-saudi-rivalry/

Derks, H. (2012). *History of the opium problem: The assault on the East, ca. 1600–1950* (Vol. 105). Brill. http://www.jstor.org/stable/10.1163/j.ctv4cbhdf

DiMaggio, J. (2022, February 22). *North Korea: Intelligence assessment 2022*. *Analyst1*. https://analyst1.com/north-korea-intelligence-assessment-2022/

Esfahani, M. K. (2018). Political realism and Iran: Geopolitics and defensive realism. In R. Schuett & M. Hollingworth (Eds.), *The Edinburgh companion to political realism* (pp. 431–444). Edinburgh University Press.

Europol. (2017). Defining serious and organised crime. In *European Union serious and organised crime threat assessment 2017 (SOCTA 2017)*. https://www.europol.europa.eu/socta/2017/defining-serious-and-organised-crime.html

Europol. (2024, December). *Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures*. https://www.europol.europa.eu/publications-events/publications/leveraging-legitimacy-how-eu%E2%80%99s-most-threatening-criminal-networks-abuse-legal-business-structures

Europol. (2025). *European Union serious and organised crime threat assessment: The changing DNA of serious and organised crime*. Publications Office of the European Union. https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

Federal Ministry of the Interior and Community. (n.d.). *Disinformation & hybrid threats*. https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/article-disinformation-hybrid-threat.html

Felbab-Brown, V. (2023, March 31). *China's role in the fentanyl crisis*. Brookings Institution. https://www.brookings.edu/articles/chinas-role-in-the-fentanyl-crisis/

Felbab-Brown, V. (2025, December 9). *How Chinese criminal networks fuel illicit markets across the Americas*. Brookings Commentary/Testimony. https://www.brookings.edu/articles/how-chinese-criminal-networks-fuel-illicit-markets-across-the-americas/

Fisher-Onar, N. (2023). From realist billiard balls and liberal concentric circles to Global IR's Venn diagram? Rethinking international relations via Turkey's centennial. *Uluslararası İlişkiler, 20*(78), 97–118. https://doi.org/10.33458/uidergisi.1298208

Fiveable. (2024, August 1). *State security – European history – 1945 to present*. https://fiveable.me/key-terms/europe-since-1945/state-security

Freedman, L. (2014). Strategic studies and the problem of power. In J. Maiolo & T. Mahnken (Eds.), *Strategic studies: A reader* (pp. 18–20). Routledge.

Grabosky, P. (2013). Organized cybercrime and national security. In Korean Institute of Criminology & International Society of Criminology (Eds.), *Information society and cybercrime: Challenges for criminology and criminal justice* (Research Report Series 13-B-01, World Crime Forum 2013, pp. 19–30). Korean Institute of Criminology.

Galeotti, M. (2019, January 18). *Gangster geopolitics: The Kremlin's use of criminals as assets abroad*. *The Moscow Times*. https://www.themoscowtimes.com/2019/01/18/gangster-geopolitics-the-kremlins-use-of-criminals-as-assets-abroad-a64204

Galeotti, M. (2022). *The weaponization of everything. A field guide to the new way of war*. Yale: Yale University Press Publications.

Giambertoni, M. (2025, March 31). *Hezbollah's networks in Latin America: Potential implications for U.S. policy and research*. RAND. https://www.rand.org/pubs/perspectives/PEA3585-1.html

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The landscape of hybrid threats: A conceptual model* (EUR 30585 EN, JRC123305). Publications Office of the European Union. https://doi.org/10.2760/44985

Global Initiative Against Transnational Organized Crime. (2025a). *Global organized crime index 2025: Crime at a crossroads*. https://globalinitiative.net/analysis/the-global-organized-crime-index-2025/

Global Initiative Against Transnational Organized Crime. (2025b). *Iran: Global Organized Crime Index*. https://ocindex.net/country/iran

Global Initiative Against Transnational Organized Crime. (2025c). *Democratic People's Republic of Korea: Global Organized Crime Index*. https://ocindex.net/country/korea-dpr

Greitens, S. C. (2014). *Illicit: North Korea's evolving operations to earn hard currency*. Committee for Human Rights in North Korea.

Häggström, H. (2021). Hybrid threats and new challenges for multilateral intelligence cooperation. In M. Weissmann, N. Nilsson, B. Palmertz, & P. Thunholm (Eds.), *Hybrid warfare, security and asymmetric conflict in international relations* (pp. 132–144). I.B. Tauris.

Hicks, K. H., Friend, A. H., Federici, J., Shah, H., Donahoe, M., Conklin, M., Akca, A., Matlaga, M., & Sheppard, L. (2019). *By other means: Part I: Campaigning in the gray zone*. Center for Strategic & International Studies. https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone

Hill, B. (2023, January–February). The state as a transnational criminal organization: A North Korea case study. *Indo-Pacific Perspectives, 6*(1), 89–98. https://www.airuniversity.af.edu/JIPA/Display/Article/3285265/the-state-as-a-transnational-criminal-organization-a-north-korea-case-study/

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid warfare*. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Holmes, R. (2026, March 9). *Iran hires European criminals to work as spies via Telegram bots: Tehran-linked channels advertise paid assignments for surveillance and other tasks, raising concerns about a growing "gig-economy" espionage model across Europe*. *The i Paper*. https://inews.co.uk/news/iran-hires-european-criminals-work-spies-telegram-bots-4281573

Hybrid CoE. (n.d.). *Hybrid threats as a phenomenon*. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

International Law Commission. (2001). *Responsibility of States for internationally wrongful acts* (United Nations General Assembly Resolution 56/83, Annex). UN Doc. A/RES/56/83. un.org. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

Jarillo, J. C. (2003). *Strategic logic*. Palgrave Macmillan. https://doi.org/10.1057/9780230598140

Jervis, R. (1988). Realism, game theory, and cooperation. *World Politics, 40*(3), 317–349. Johns Hopkins University Press

Jokinen, J., Normark, M., & Fredholm. M. (2022, June). *Hybrid threats from non-state actors: A taxonomy* (Hybrid CoE Research Report No. 6). Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Research-Report-6-Non-state-actors-WEB.pdf

Jordan, J. (2020). International competition below the threshold of war: Toward a theory of gray zone conflict. *Journal of Strategic Security, 14*(1), 1–24. https://doi.org/10.5038/1944-0472.14.1.1836

Kaarbo, J., & Beasley, R. K. (1999). A practical guide to the comparative case study method in political psychology. *Political Psychology, 20*(2), 369–391.

Kan, P. R. (2019, July 24). *Dark international relations: When crime is the "DIME."* U.S. Army War College, War Room. https://warroom.armywarcollege.edu/articles/dark-international-relations-when-crime-is-the-dime/

Kan, P. R., Bechtol, B. E., Jr., & Collins, R. M. (2010, March). *Criminal sovereignty: Understanding North Korea's illicit international activities*. U.S. Army War College Strategic Studies Institute.

Karlén, N., & Rauta, V. (2021). Forum: Conflict delegation in civil wars: Introduction. *International Studies Review, 23*(4), 2048–2078.

Karstedt, S. (2014). Organizing crime: The state as agent. In L. Paoli (Ed.), *The Oxford handbook of organized crime* (pp. 303–320). Oxford University Press.

Keatinge, T. (2023, June 6). *Developing bad habits: What Russia might learn from Iran's sanctions evasion*. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/occasional-papers/developing-bad-habits-what-russia-might-learn-irans-sanctions-evasion

Keene, S. D. (2018). *Silent Partners: Organized Crime, Irregular Groups, And Nation-States*. Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep20096

Kelly, A. (2003). Introduction. In *Decision making using game theory: An introduction for managers* (pp. 1–16). Cambridge University Press.

Kelly, R. E. (2016, March 16). *North Korea as a "mafia state". The Interpreter, Lowy Institute*. https://www.lowyinstitute.org/the-interpreter/north-korea-mafia-state

Kennedy, L., & Southern, N. P. (2025, March 31). *Where does North Korea get its cash? How the scam industry created new money laundering avenues for North Korea*. Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/analysis/where-does-north-korea-get-its-cash/

Khoshnood, A. M. (2025). The Islamic Republic of Iran's use of criminal intermediaries for extraterritorial assassinations and covert violence: A gray zone strategy of outsourced repression. *Small Wars & Insurgencies, 36*(8), 1433–1461. https://doi.org/10.1080/09592318.2025.2555583

Kriener, F. (2023). Intervention, prohibition of. In *Max Planck Encyclopedia of Public International Law (MPEPIL)*. Max Planck Institute for Comparative Public Law and International Law. Oxford University Press. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1434

Lamb, A. (2021). *Jamaica in the grey zone: Responding to the hybrid threat of organized crime* (JCSP 46 DL – PCEMI 46 AD, Solo Flight). Canadian Forces College.

Lebrun, M. (2023). *Watching out for populism: Authoritarian logics as a vulnerability to hybrid threat activity* (Hybrid CoE Working Paper 22). The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-22-watching-out-for-populism-authoritarian-logics-as-a-vulnerability-to-hybrid-threat-activity/

Lebrun, M. (2026, March). *MENA: Four political trends shaping the hybrid threat landscape* (Hybrid CoE Trend Report 11). European Centre of Excellence for Countering Hybrid Threats.

https://www.hybridcoe.fi/publications/mena-four-political-trends-shaping-the-hybrid-threat-landscape/

Lee, D. (2015, May 29). *Bureau 121: How good are Kim Jong-un's elite hackers? BBC News*. https://www.bbc.com/news/technology-32925503

Lemke, D. (2025). *Realism, the English School, and the survival of states*. In *How states die: Membership and survival in the international system*. Oxford University Press. https://doi.org/10.1093/9780197805053.003.0007

Levitt, M. (2013, October 2). *Hezbollah as a criminal organisation*. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/hezbollah-criminal-organisation

Liyanage, C. (2022, October 20). Geopolitics of impunity: Transnational organised crime in the context of the rise of global authoritarianism. *Royal United Services Institute*. https://www.rusi.org/networks/shoc/informer/geopolitics-impunity-transnational-organised-crime-context-rise-global-authoritarianism

Locke, R. (2012, July). *Organized crime, conflict, and fragility: A new approach*. International Peace Institute. https://www.ipinst.org/wp-content/uploads/publications/icr_3.pdf

Löjdquist, F. (2021). Foreword: Hybrid threats and hybrid warfare—Security and asymmetric conflict in the grey zone. In M. Weissmann, N. Nilsson, B. Palmertz, & P. Thunholm (Eds.), *Hybrid warfare, security and asymmetric conflict in international relations* (pp. viii–x). I.B. Tauris.

Long, M. (2025). Shadows of power beneath the threshold: Where covert action, organized crime and irregular warfare converge. *Intelligence and National Security, 40*(1), 87–113. https://doi.org/10.1080/02684527.2024.2417454

Lopez, C. T. (2021, May 14). *In cyber, differentiating between state actors, criminals is a blur*. *DOD News*. https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/

Luyten, K. (2020). *Understanding the EU's response to organised crime* (EPRS Briefing No. PE 652.043). European Parliamentary Research Service, European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652043/EPRS_BRI(2020)652043_EN.pdf

Mailey, J. R. (2024, October). *Iran's criminal statecraft: How Tehran weaponizes illicit markets*. Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/analysis/irans-criminal-statecraft-how-teheran-weaponizes-illicit-markets/

Mallory, K. (2021). *North Korean sanctions evasion techniques*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1537-1.html

Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict* (Monograph). US Army War College Press. https://press.armywarcollege.edu/monographs/428

McGinley, W. (2014). Mechanisms and microfoundations in international relations theory. *Review of International Studies, 40*(2), 367–389. https://doi.org/10.1017/S0260210513000156

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. New York & London: W.W. Norton & Company.

Miklaucic, M., & Naím, M. (2013). The criminal state. In M. Miklaucic & J. Brewer (Eds.), *Convergence: Illicit networks and national security in the age of globalization* (pp. 149–170). National Defense University Press.

Moiseienko, A. (2024). Crime and Sanctions: Beyond Sanctions as a Foreign Policy Tool. *German Law Journal*, *25*(1), 17–47. https://doi.org/10.1017/glj.2023.103.

Monaghan, M., & Prideaux, S. (2016). The state, corporations and organised crime. In *State crime and immorality: The corrupting influence of the powerful* (pp. 61–88). Bristol University Press.

Monaghan, S. (2019, October). *Countering hybrid warfare: So what for the future joint force? PRISM, 8*(2). U.S. National Defense University Press. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf

Moon, M. (2017, June 14). *US: North Korea's been hacking everyone since 2009*. *Engadget*. https://www.engadget.com/2017-06-14-us-issues-alert-north-korea-cyber-attack-hidden-cobra.html

Muggah, R. (2023). Organized crime in armed conflicts and other situations of violence. *International Review of the Red Cross, 105*(923), 569–574. https://doi.org/10.1017/S1816383123000036

NATO. (2026, January 29). *Countering hybrid threats*. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

Nichols, M. (2019, August 5). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. *Reuters*. https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX/

Nilsson, N., Weissmann, M., Palmertz, B., Thunholm, P., & Häggström, H. (2021). Security challenges in the grey zone: Hybrid threats and hybrid warfare. In M. Weissmann, N. Nilsson, B. Palmertz, & P. Thunholm (Eds.), *Hybrid warfare, security and asymmetric conflict in international relations* (pp. 1–18). I.B. Tauris.

Normark, M. (2019, April). *Hybrid CoE Strategic Analysis 15: How states use non-state actors: A modus operandi for covert state subversion and malign networks*. European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-

coe-strategic-analysis-15-how-states-use-non-state-actors-a-modus-operandi-for-covert-state-subversion-and-malign-networks/

O'Neill, B. (1994). Game theory models of peace and war. In R. J. Aumann & S. Hart (Eds.), *Handbook of game theory with economic applications* (Vol. 2, pp. 995–1053). Elsevier. https://doi.org/10.1016/S1574-0005(05)80061-X

Park, J. (2021). The Lazarus Group: The cybercrime syndicate financing the North Korea state. *Harvard International Review, 42*(2), 34–39.

Pawlak, P. (2015, June). *Understanding hybrid threats*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf

Petta Gomes da Costa, D. L. (2018). *Organized crime and the nation-state: Geopolitics and national sovereignty*. Routledge. https://doi.org/10.4324/9780429426315

Rademeyer, J. (2017). *Diplomats and deceit: North Korea's criminal activities in Africa*. Global Initiative Against Transnational Organized Crime.

Rauta, V. (2025, February). *Countering state-sponsored proxies: Designing a robust policy* (Hybrid CoE Paper No. 23). European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-paper-23-countering-state-sponsored-proxies-designing-a-robust-policy/

Redhead, M. R. (2025). *Old wine, new bottles? The challenge of state threats* (SOC ACE Research Paper No. 32). University of Birmingham. https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/67852e69ff4ff4079a9c3000/1736781420568/SOCACE-RP32-OldWineNewBottles_final.pdf

Reuters. (2024, May 30). *Swedish security service says Iran uses criminal networks in Sweden*. Reuters. https://www.reuters.com/world/swedish-security-service-says-iran-uses-criminal-networks-sweden-2024-05-30/

Salehyan, I. (2009). The delegation of war to rebel organizations. *Journal of Conflict Resolution, 54*(3), 493–515. https://doi.org/10.1177/0022002709357890

Salisbury, D. (2024). *Shopping for mass destruction: North Korea's illicit procurement networks* (Occasional paper). Royal United Services Institute for Defence and Security Studies. https://www.rusi.org/explore-our-research/publications/occasional-papers/shopping-mass-destruction-north-koreas-illicit-procurement-networks

Sari, A. (2026). Warfare below the threshold of war: Hybrid threats and the role of international law. In P. A. L. Ducheine, T. D. Gill, P. B. M. J. Pijpers, & M. C. Zwanenburg (Eds.), *A research agenda for military law* (pp. 29–40). Edward Elgar Publishing. https://doi.org/10.4337/9781035353507.00011

Schroefl, J., & Kaufman, S. J. (2014). Hybrid actors, tactical variety: Rethinking asymmetric and hybrid war. *Studies in Conflict & Terrorism, 37*(10), 862–880. https://doi.org/10.1080/1057610X.2014.941435

Schuett, R. (2024). Geopolitik und organisierte Kriminalität: Grenzüberschreitende OK als (harter) geopolitischer Akteur. *SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis*, (2), 4–18. https://doi.org/10.7396/2024_2_A

Schuett, R. & Williams, J. (2024) Intelligence in international society: An English school perspective on the 'five eyes'. Global Policy, 15, 223–233. Available from: https://doi.org/10.1111/1758-5899.13362

Schuett, R., & Schramm, P. (2025, April 22). *Gangs of geopolitics*. Global Policy Journal. https://www.globalpolicyjournal.com/blog/22/04/2025/gangs-geopolitics

Schuett, R., & Trenta, L. (2025, May 27). Covert wars, criminal gangs, and the 'new threat' environment. *RUSI Commentary*. https://www.rusi.org/explore-our-research/publications/commentary/covert-wars-criminal-gangs-and-new-threat-environment

Shehu, D. M. (2024). The multi-dimensional nature of international relations. *International Journal of Innovation Research and Advanced Studies, 5*(2), 83–92. https://harvardpublications.com/hijiras/article/view/158

Short, J. R. (2022). *Geopolitics. Making Sense of a Changing World*. Rowman & Littlefield.

Singh, V. V. (2024, November 20). *The six degrees of cyber attribution*. IISS Cyber Power Matrix. https://www.iiss.org/online-analysis/cyber-power-matrix/2024/11/the-six-degrees-of-cyber-attribution/

Stengel, F. A., & Baumann, R. (2017, September 26). *Non-state actors and foreign policy*. In E. Hannah (Ed.), *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.456

Sullivan, J. P., & Jones, N. P. (2024). Hybrid threats: Cartel and gang links to illicit global networks. *International Journal on Criminology, 11*(2), 13–38. https://www.criminologyjournal.org/hybrid-threats-cartel-and-gang-links-to-illicit-global-networks.html

Sun Tzu. (2017). *The art of war* (L. Giles, Trans.; J. Minford, Foreword). Tuttle Publishing.

The Lightning Press. (n.d.). *The instruments of national power*. https://www.thelightningpress.com/the-instruments-of-national-power/

The Soufan Center. (2024, November 1). *Hidden warfare: Iran's growing dependence on criminal networks*. The Soufan Center. https://thesoufancenter.org/intelbrief-2024-november-1/

Thorley, M. (2025, March 17). *Of kingdoms and crooks: The rise of geocriminality*. Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/analysis/the-rise-of-geocriminality/

Thorley, M. (2026). Evolution of the state-crime nexus: Presenting geocriminality. *Journal of Illicit Economies and Development, 8*(1), 1–14. https://doi.org/10.31389/jied.339

Troy, J. (2018) *Political Realism and the English School. Is there really no international theory? Martin Wight and Hans Morgenthau on international political theory.* In: The Edinburgh Companion to Political Realism. (pp. 85–96). Edited by Robert Schuett and Miles Hollingworth. Edinburgh University Press.

United Nations. (n.d.). *United Nations Convention against Transnational Organized Crime: Status of ratification*. United Nations Treaty Collection. Retrieved June 4, 2026, from https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en

United Nations. (1945). *Charter of the United Nations and Statute of the International Court of Justice*. https://www.un.org/en/about-us/un-charter/full-text

United Nations Office on Drugs and Crime. (n.d.). *Defining organized crime.* https://www.unodc.org/e4j/ru/organized-crime/module-1/key-issues/defining-organized-crime.html

United Nations Office on Drugs and Crime. (2004). *United Nations Convention against Transnational Organized Crime and the Protocols thereto*. https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

United Nations Office on Drugs and Crime. (2017). *Legislative guide for the implementation of the United Nations Convention against Transnational Organized Crime*. United Nations. https://www.unodc.org/unodc/en/treaties/CTOC/legislative-guide.html

United Nations Office on Drugs and Crime. (2018, April). *Organized Crime Module 1 Key Issues: Defining Organized Crime*. Education for Justice (E4J). https://www.unodc.org/e4j/ru/organized-crime/module-1/key-issues/defining-organized-crime.html

Voyger, M. (2021, February 24). *What is "hybrid warfare," really? What NATO should do to stay resilient in the face of its challenge*. Center for European Policy Analysis. https://cepa.org/article/what-is-hybrid-warfare-really/

Wang, P., & Blancke, S. (2014). *Mafia state: The evolving threat of North Korean narcotics trafficking*. *RUSI Journal, 159*(5), 52–59. https://www.academia.edu/10274872/Mafia_State_The_Evolving_Threat_of_North_Korean_Narcotics_Trafficking

Waugh, L., & Yousuf, Z. (2022, May). *Organised crime and conflict: Implications for peacebuilding*. Saferworld. https://www.saferworld-global.org/resources/publications/1392-organised-crime-and-conflict-implications-for-peacebuilding-

Wigell, M. (2019) 'Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy', *International Affairs, 95*(2), 255–275. https://doi.org/10.1093/ia/iiz018

Wigell, M., Mikkola, H., & Juntunen, T. (2021, May). *Best practices in the whole-of-society approach in countering hybrid threats* (PE 653.632). Policy Department for External Relations, Directorate-General for External Policies of the Union, European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653632

Wyler, L. S., & Nanto, D. K. (2008, January 29). *North Korean crime-for-profit activities* (Order Code RL33885). Congressional Research Service.

Ylikoski, P. (2019). Mechanism-based theorizing and generalization from case studies. *Studies in History and Philosophy of Science Part A, 78*, 14–22. https://doi.org/10.1016/j.shpsa.2018.11.009

Youde, J. (2018). The English School and the Emergence of International Society. In *Global Health Governance in International Society*. Oxford University Press. https://doi.org/10.1093/oso/9780198813057.003.0002

ANNEX

Annex 1: Glossary

Overview: Central Terms, Explanations, and Definitions[5]

Hybrid threat: "Hybrid threats usually refer to coordinated harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined. These means may include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force. Hybrid tactics are used by both state and non-state actors and are growing in complexity and sophistication. In addition to the security risk, they pose a threat to democracy, targeting its core values and aiming to fracture society and undermine political decision-making. Hybrid campaigns are designed in a way that makes detecting and defending against them difficult" (Council of the European Union, 2025).

Organised crime: "Organized crime is a continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through corruption of public officials and the use of intimidation, threats or force to protect its operations" (United Nations Office on Drugs and Crime [UNODC], 2018).

Organised criminal group/network: Criminal groups or organised criminal groups "are as varied as the markets they service and the activities they engage in. In many cases, OCGs reflect the societies, cultures and value systems they originate from. As societies across Europe become more interconnected and international in outlook, organised crime is now also more connected and internationally active than ever before. Since the year 2000, the United Nations Convention against Transnational Organized Crime has provided an internationally shared definition of an organised criminal group as 'a group of three or more persons existing over a period of time acting in concert with the aim of committing crimes for financial or material benefit'" (Europol, 2017). The present thesis frequently uses the terms criminal group and criminal network synonymously. It acknowledges, however, that a criminal group may refer rather to a defined, relatively bounded set of individuals who act together to commit criminal activities, while a criminal network is a broader, more fluid system of actors connected through functional, logistical, or financial relationships rather than fixed membership. States may be more likely to tolerate or exploit criminal networks than individual groups, as networks are harder to attribute and dismantle.

[5] The terms presented here including their definitions are incorporated in the different sections of the present thesis as well. Some of the following terms, such as 'Hybrid threat', are highly fluid and definitions may vary across sources concerning the extent of components they encompass.

State security and National security: “State security refers to the measures and actions taken by a government to protect its sovereignty, territorial integrity, and the safety of its citizens from external threats and internal disturbances” (Fiveable, 2024). ‘National security’ is a broader concept. “The category ‘national security’ is multidimensional and includes such types as state security, public security, personal security, information security, environmental security, transport security and others” (Iroshnikov, 2018, p. 11).

Proxy: “‘Proxy warfare’ is a term used to refer to armed hostilities involving entities (both state and non-state actors) that other states or non-state actors may support directly or indirectly – politically, materially, financially, militarily or otherwise – in line with their own strategic interests against another state or non-state actor” (D’Cunha, Ferraro & Rodenhäuser, 2025). Based on this definition of ‘proxy warfare’, a ‘proxy’ can be understood as an actor that is not formally part of a state’s institutional apparatus but whose actions serve, intentionally or unintentionally, the strategic interests of a state. Proxy relationships do not necessarily require direct instruction or full control; rather, they may also exist where a state tolerates, enables, or passively benefits from the actions of non-state actors, including organised criminal networks.

Below the threshold: Below the threshold of armed conflict refers to actions that impose coercive, disruptive, or destabilising effects on a state while deliberately avoiding the scale, attribution, and physical violence required to trigger an armed conflict or the application of the law of armed conflict. “Competition below the threshold of armed conflict is characterized by several features. First, measures short of war often exploit or generate ambiguity. Hostile actors typically deny or hide their involvement in malign activities to avoid attribution, for example by employing proxies or using means that are not easily linked to their authors, such as influencing operations promoting social divisions. Second, such measures often seek to achieve non-kinetic effects, in other words effects that do not involve material destruction or injury, but instead cause other, intangible harms, such as loss of trust, reputational costs or financial damage. Third, they are often characterized by incrementalism, designed to change the status quo slowly and without provoking a military response. This might include the gradual build-up of capacity, persistent activities meant to achieve strategic gains over time or small-scale engagements of limited intensity that, when taken by themselves, do not merit a robust response by the target. Fourth, competition below the threshold of open hostilities is multidomain in character, often deploying a mix of measures across several domains to achieve synergistic effects and to overwhelm the opponent’s ability to respond” (Sari, 2026, p. 31).

Grey zone: When entities act within the grey zone, “they maneuver in the ambiguous no-man’s-land between peace and war, reflecting the sort of aggressive, persistent, determined campaigns characteristic of warfare but without the overt use of military force” (Mazarr, 2015, p. 2). “Gray zone conflict might be understood as having a number of characteristics. It could be considered as a form of conflict that: pursues political objectives through cohesive, integrated campaigns; employs mostly nonmilitary or nonkinetic tools; strives to remain under key escalatory or red line thresholds to avoid outright, conventional conflict; and moves gradually toward its

objectives rather than seeking conclusive results in a specific period of time" (Mazarr, 2015, p. 58).

Conventional means/instruments: Conventional means or instruments of state power refer "to the tools a country uses to influence other countries or international organizations or even non-state actors. [...] In the American perspective, the instruments of national power are: Diplomacy, Information, Military, and Economic" (The Lightning Press, n.d.). Conventional means are often characterised by being state-owned, overt or at least formally attributable, governed by established legal and normative frameworks, and inherently escalatory, as their use carries a higher risk of retaliation, countermeasures, or even armed conflict. These conventional instruments stand in contrast to unconventional means such as the use of organised crime as a proxy, which relies on non-state actors, exploits deniability and legal ambiguity, and enables coercive pressure to be exerted below the threshold of armed conflict.