MASTER THESIS | MASTER‘S THESIS

Titel | Title

Synthetic Drug Supply Chains as Hybrid Security Threats: Logistics Infrastructure, Border Control Technologies and the Geopolitics of Illicit Markets in the European Security Perimeter

verfasst von | submitted by

Daniel Schattauer

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

Synthetic drug supply chains have expanded in scale and strategic significance across the European security perimeter despite continuous reform of border governance and sustained investment in control technologies. This thesis examines why. It argues that the answer is structural rather than institutional: the design features that make European ports, land-border corridors and precursor chemical trade networks maximally efficient for licit commerce are precisely the features that render them exploitable by illicit supply chains. This *dual-use paradox of logistics infrastructure* generates exploitability not as a correctable governance failure but as an irreducible by-product of any system that must simultaneously maximise commercial throughput and maintain security control.

The thesis develops an integrated analytical framework combining four lenses: security governance as the analytical engine, hybrid threat theory as the strategic frame, the international political economy of illicit markets as the explanatory mechanism, and societal resilience for assessing the stakes. This framework is operationalised through an original typology distinguishing infrastructure, governance and integrity vulnerabilities. It further introduces a distinction between *hybrid effects*, the cross-domain security consequences produced within the EU's internal security space, and *hybrid entanglement*, the constitutive integration of drug economies into conflict dynamics and state-crime linkages in the wider neighbourhood.

Using qualitative, comparative document analysis, the framework is applied to three cases capturing production-transit-entry dynamics: the Port of Antwerp-Bruges, the Western Balkans land corridor, and the Captagon economy of the Levant. Each is dominated by a different vulnerability and demands a different governance register. The comparative finding is that the paradox manifests at every supply-chain level through the same structural logic but cannot be addressed by any single-sector response. Governance can manage exploitability, but it cannot eliminate it.

Abstrakt

Synthetische Drogenlieferketten haben innerhalb des europäischen Sicherheitsperimeters an Umfang und strategischer Bedeutung gewonnen, obwohl Grenzgovernance kontinuierlich reformiert und erheblich in Kontrolltechnologien investiert wurde. Diese Thesis argumentiert, dass die Ursache strukturell ist: Die Merkmale, die europäische Häfen, Landgrenzkorridore und den Vorläuferchemikalienhandel für den legalen Warenverkehr effizient machen, schaffen zugleich systematische Ausbeutungsmöglichkeiten für illegale Lieferketten. Dieses *Dual-Use-Paradox der Logistikinfrastruktur* erzeugt Ausbeutbarkeit nicht als korrigierbares Governance-Versagen, sondern als unvermeidbares Nebenprodukt jedes Systems, das gleichzeitig kommerziellen Durchsatz und Sicherheitskontrolle gewährleisten muss.

Die Thesis entwickelt ein integriertes analytisches Rahmenwerk, das Sicherheitsgovernance, hybride Bedrohungstheorie, die politische Ökonomie illegaler Märkte und gesellschaftliche Resilienz verbindet. Es wird auf drei Fallstudien angewendet: den Hafen Antwerpen-Brügge, den Westbalkan-Korridor und die Captagon-Ökonomie der Levante. Der Vergleich zeigt, dass das Paradox auf jeder Ebene der Lieferkette durch dieselbe strukturelle Logik wirkt. Governance kann Ausbeutbarkeit steuern, aber nicht beseitigen.

Table of Contents

List of Abbreviations

ATS	Amphetamine-Type Stimulants
CCP	Container Control Programme (UNODC-WCO)
CEPOL	European Union Agency for Law Enforcement Training
CTIF	*Cellule de Traitement des Informations Financières* (Belgian Financial Intelligence Unit)
DP World	Dubai Ports World (global terminal operator)
EC	European Commission
EEAS	European External Action Service
EPPO	European Public Prosecutor's Office
EU	European Union
EUDA	European Union Drugs Agency
Europol	European Union Agency for Law Enforcement Cooperation
Frontex	European Border and Coast Guard Agency
GDP	Gross Domestic Product
GI-TOC	Global Initiative Against Transnational Organized Crime
INCB	International Narcotics Control Board
INL	Bureau of International Narcotics and Law Enforcement Affairs (US Department of State)
IPA	Instrument for Pre-Accession Assistance
MAIS	Master of Advanced International Studies
MSC	Mediterranean Shipping Company
NATO	North Atlantic Treaty Organization
NPS	New Psychoactive Substances
OLAF	European Anti-Fraud Office (*Office européen de lutte antifraude*)
OSCE	Organization for Security and Co-operation in Europe

PCCP	Passenger and Cargo Control Programme
PSA	PSA International (global terminal operator)
SOCTA	(EU) Serious and Organised Crime Threat Assessment
TEU	Twenty-foot Equivalent Unit
TIL	Terminal Investment Limited (MSC terminal operator)
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNODC	United Nations Office on Drugs and Crime
US	United States
WCO	World Customs Organization

1. Introduction and Research Question

In 2023, authorities at the Port of Antwerp-Bruges seized a record 116 tonnes of cocaine (EMCDDA 2024b, 57), the largest annual haul in European history. The following year, seizures remained at historically elevated levels. These numbers are remarkable. Not because they reveal how much drug trafficking is being stopped, but because of what they imply about what is not. Antwerp-Bruges handles approximately 14 million container units annually, making thorough inspection physically and economically impossible. Fewer than two per cent of containers are ever opened (UNODC/WCO/INTERPOL/ICAO 2025, 1; Europol 2023, 7).

The port's role as a trade hub and a major drug trafficking gateway is not coincidental: it reflects the same structural reality. The same infrastructure optimised for commercial throughput, including containerisation, trusted trader schemes, risk-based selective inspection, and just-in-time logistics, is precisely what makes the port systematically exploitable by illicit supply chains. More enforcement resources, better scanning technology and enhanced inter-agency coordination have not resolved this tension. They have managed it.

This thesis argues that the reason is structural, not institutional: the exploitability of European logistics infrastructure is not a governance failure that reform can eliminate, but a design feature of any system that must at the same time maximise commercial efficiency and maintain security. Understanding why requires a different analytical framework than existing approaches provide. Although cocaine trafficking is not the empirical focus of this thesis, the Antwerp-Bruges case shows the broader structural susceptibility of containerised logistics systems that synthetic drug and precursor networks take advantage of through the same structural mechanisms.

Synthetic drugs, including amphetamine-type stimulants (ATS) and new psychoactive substances (NPS), have become the fastest-growing and most analytically challenging segment of the European illicit drug market. Among these, Captagon is particularly significant because it connects synthetic drug production to conflict-linked political economies affecting the European security perimeter. Unlike plant-based drugs, synthetic substances are not geographically limited: they can be produced in proximity to consumer

markets, do not depend on agricultural conditions, and rely on globally traded precursor chemicals that are deeply embedded in licit pharmaceutical and chemical industries.

This structural flexibility renders synthetic drug supply chains fundamentally different in their security implications from heroin or cocaine, and demands approaches that can capture their dynamic, multi-nodal and infrastructure-exploiting character.

The institutional assessments created by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA 2023b, 2024b), its successor the European Union Drugs Agency (EUDA 2025), and Europol (2023, 2025), consistently document the expansion of these markets in scale, geographic reach, and strategic complexity. And yet, the analytical tools available to governance actors remain fragmented across disciplinary and institutional boundaries that criminal networks do not respect.

The strategic weight of these developments extends well beyond the domain of law enforcement. Synthetic drug supply chains interact directly with the European Union's external border regime, its critical transport infrastructure and its internal security architecture in ways that generate effects analytically comparable to other forms of hybrid security threats such as erosion of institutional integrity, degradation of governance capacity, exploitation of jurisdictional seams, and cumulative damage to societal resilience.

At the same time, in Europe's wider neighbourhood, synthetic drug economies have become structurally entangled with conflict dynamics, war economies, and sanctions-evasion networks in ways that link the governance of illicit supply chains directly to matters of geopolitical stability. The Captagon economy centred on Syria represents the most fully developed case of this entanglement, though not the only one. State military structures became directly involved in industrial-scale production and export, generating revenues estimated in the billions, sustaining armed actors and corrupted regional governance structures.

European and international institutions have not been passive in the face of these developments. The EU's border governance architecture has been continuously reformed, container control technologies upgraded, risk profiling systems enhanced, and inter-agency coordination mechanisms amplified. The NATO Strategic Concept (2022), the EU Strategic Compass (2022), and the EU Security Union Strategy (2020) have all explicitly

acknowledged organised crime and illicit economies as components of the hybrid threat environment. The UNODC-WCO Container Control Programme has since been integrated into the broader Passenger and Cargo Control Programme (PCCP), operationalised on 1 January 2025, which links cargo and passenger risk management across maritime, aviation and land-border environments. In 2025, PCCP supported 197 frontline units and National Targeting Centres in 94 countries, while participating countries recorded 4,791 seizures, an 83 per cent increase compared with 2024 (UNODC/WCO/INTERPOL/ICAO 2026, 4–5). Europol's port liaison networks have expanded massively. And yet, synthetic drug supply chains have not diminished in scale or strategic significance. They have expanded. The puzzle, therefore, is less about criminal adaptability itself than about the sustained difficulty sophisticated governance systems encounter in reducing the exploitability of the logistical infrastructures these networks need to succeed.

The existing literature, ranging across criminology, security studies, border governance research, and international political economy, provides rich partial accounts of why this might be the case: criminal adaptability, institutional fragmentation, coordination failures, and resource asymmetries. Yet these accounts are rarely integrated into a coherent explanation of why the governance architecture as a whole, not just individual institutions, struggles to reduce the exploitability of European logistics infrastructure confronted with versatile synthetic drug supply chains. This explanatory gap is the intellectual motivation for the analytical framework developed in this thesis.

The argument here is that the persistence of synthetic drug supply chains as hybrid security challenges within the European security perimeter, understood here as the layered space in which EU internal security, external border governance, neighbouring transit corridors and conflict-linked production zones interact to shape European security outcomes, is not primarily a product of insufficient resources, political will or individual institutional failures, although these factors play a role. It is first and foremost a product of a structural condition that existing governance frameworks have not adequately theorised: the dual-use paradox of logistics infrastructure.

The paradox is that the design features that make European ports, border corridors and precursor chemical trade networks maximally efficient for licit commerce are exactly the features that make them also structurally exploitable by illicit supply chains. Throughput optimisation, risk-based selective inspection, trusted trader schemes, and supply-chain

integration are design successes that nevertheless generate exploitability as an irreducible by-product.

Governance reform cannot eliminate this tension completely. Instead, it can only manage it more or less effectively, and managing it better than current architectures allow requires a fundamentally different understanding of what the governance problem actually is.

Against this background, this thesis addresses the following main research question:

Why have synthetic drug supply chains been able to evolve into hybrid security challenges within the European security perimeter despite increasingly sophisticated border governance and control technologies?

Three supporting sub-questions guide the analysis:

1. Why do structural characteristics of logistical nodes, precursor regimes and trade facilitation systems render them systematically exploitable by synthetic drug networks?
2. Why do intelligence-led border control technologies and risk-based governance practices generate adaptation, displacement, and recurring vulnerabilities rather than durable deterrence?
3. Why do existing EU and international security governance frameworks struggle to integrate border security, organised crime control, and societal resilience in a strategically coherent manner?

To answer these questions, this thesis develops an integrated analytical framework that combines four theoretical lenses in a deliberate hierarchical arrangement. Security governance theory serves as the analytical engine, directing attention to the institutional architecture within which the dual-use paradox operates and generates governance failures. Hybrid threat theory provides the strategic frame, situating the cross-domain security effects of synthetic drug supply chains within the contemporary European security environment and introducing an original analytical nuance between hybrid effects, the cross-domain security consequences produced within the EU's internal security space, and hybrid entanglement, the structural intertwining of drug economies with conflict dynamics and state-crime linkages in the wider neighbourhood. The international political economy of illicit markets supplies the explanatory mechanism, accounting for the adaptive resilience of criminal networks through the logic of profit-

maximising rational actors responding to the incentive structures created by governance fragmentation. And societal resilience provides the framework for assessing the downstream institutional and societal consequences of persistent supply chain exploitation.

The dual-use paradox connects these four lenses and is operationalised through an original vulnerability typology distinguishing infrastructure, governance and integrity vulnerabilities.

The empirical analysis is organised around three comparative case studies selected to capture the production-transit-entry dynamics of synthetic drug supply chains across distinct governance environments.

Case 1 examines the Port of Antwerp-Bruges, with Rotterdam as a contextual comparator, as the paradigmatic site of infrastructure and integrity vulnerability within the EU's internal security space.

Case 2 analyses the Western Balkans land corridor as a lens on governance vulnerability and enforcement-adaptation dynamics along the EU's external border regime.

Case 3 examines the Captagon economy of the Levant, centred on the Syria-Jordan corridor and Eastern Mediterranean maritime routes, as the clearest case of hybrid entanglement, where synthetic drug production is constitutively integrated into a conflict economy, sanctions-evasion architecture and state-crime nexus.

Together, these three cases enable systematic cross-case comparison of which vulnerabilities are structurally recurrent across governance environments and which are context-specific, thereby generating the comparative leverage that single-case studies cannot provide.

The thesis proceeds as follows. Section 2 sets out the expected contributions and originality of the research. Section 3 reviews the four principal strands of academic and policy literature that inform the analysis, identifies the analytical gaps they collectively reveal, and situates the present thesis within those gaps. Section 4 develops the integrated theoretical framework in full, presenting the dual-use paradox, the four conceptual lenses and the vulnerability typology in their hierarchical arrangement. Section 5 sets out the qualitative, comparative methodology, including the research design, source base, case

selection logic and analytical strategy. The empirical case studies are presented in Chapters 6, 7 and 8, followed by a comparative conclusion in Chapter 9.

2. Expected Contribution and Originality

The persistence of synthetic drug supply chains as hybrid security challenges within the European security perimeter stems less from insufficient enforcement resources, inadequate technology or political inattention than from a structural condition that existing governance frameworks have not adequately theorised: the dual-use paradox of logistics infrastructure.

The dual-use paradox of European trade architectures dictates that systematic exploitability is an intrinsic by-product of the design parameters that maximise commercial efficiency. This thesis contributes an integrated analytical framework that explains why this paradox persists, how it operates across distinct governance environments, and what a structurally coherent governance response would require.

This argument speaks directly to the literature on security governance and border regimes. Existing governance accounts are superb at describing the multiplicity of actors involved in European security, including Europol, Frontex, national customs authorities, port operators, law enforcement agencies, EU institutions, and international organisations, but they are less effective at explaining why this dense institutional architecture does not translate into durable reductions in supply chain exploitability.

By placing the dual-use paradox at the centre of the analysis, the thesis offers a structural explanation for this gap. It shows that mandate fragmentation, coordination frictions and capability asymmetries are not incidental problems within an otherwise coherent system, but recurring features of a governance architecture that was not designed to match the integrated operational logic of synthetic drug supply chains. In doing so, the thesis seeks to move beyond descriptive accounts of institutional complexity toward an explanation of why institutional complexity itself can become exploitable.

A second major contribution lies in the thesis's application and refinement of the hybrid threat concept. Hybrid threats are increasingly recognised in EU and NATO policy documents as encompassing organised crime and illicit economies, but the analytical meaning of this recognition remains underdeveloped. This thesis contributes by distinguishing between hybrid effects and hybrid entanglement. Hybrid effects refer to

the cross-domain security consequences generated within the EU's internal security space through the exploitation of port ecosystems, logistics infrastructures, insider access, regulatory seams and coordination gaps. Hybrid entanglement refers to the structural intertwining of drug economies with conflict dynamics, sanctions evasion, state-crime linkages and war economies in the wider neighbourhood, as illustrated by the Captagon economy of the Levant.

This distinction allows the thesis to avoid conceptual inflation: synthetic drug supply chains are not treated as hybrid threats because criminal actors necessarily pursue geopolitical strategies. Rather, they are treated as hybrid threats because their operations generate effects and entanglements that are strategically relevant to European security governance.

A third contribution is the thesis's vulnerability typology, which distinguishes between infrastructure vulnerabilities, governance vulnerabilities and integrity vulnerabilities. This typology forms the main operational tool through which the theoretical framework is applied to the empirical cases.

Infrastructure vulnerabilities refer to the exploitable features of logistics systems themselves, including containerisation, node dependence, throughput pressure, selective inspection and the opacity of complex supply chains. Governance vulnerabilities refer to the institutional and regulatory flaws that arise from mandate fragmentation, uneven enforcement capacity, limited information sharing, jurisdictional seams, and the difficulty of coordinating across agencies and borders. Integrity vulnerabilities refer to corruption exposure, insider facilitation, institutional capture and the susceptibility of human nodes within logistics and enforcement systems to criminal pressure.

The typology also provides the thesis with comparative leverage. The selected cases, Antwerp-Bruges and Rotterdam as port ecosystems, the Western Balkans as a land corridor, and the Captagon economy of the Levant as a conflict-linked production and transit system, differ significantly in geography, institutional setting and empirical form. A conventional case comparison could therefore appear methodologically asymmetrical. The vulnerability typology addresses this problem by establishing functional equivalence across the cases. Each case is analysed not because it is identical in form, but because it represents a different interface at which synthetic drug supply chains encounter, exploit

and adapt to governance systems. This allows the thesis to identify which vulnerabilities recur across different governance environments and which are context-specific. The result is a comparative design that avoids both narrow single-case description and overly abstract generalisation.

This empirical contribution is particularly relevant because synthetic drugs differ structurally from plant-based drug markets. Unlike cocaine or heroin, synthetic substances are not dependent on specific agricultural production zones. They can be produced closer to consumer markets, relocated in response to enforcement pressure, manufactured through adaptable chemical processes, and sustained through precursor chemicals that are embedded in licit pharmaceutical and industrial trade. These characteristics make synthetic drug supply chains especially suitable for exploiting the dual-use character of global logistics and regulatory systems. The thesis therefore treats synthetic drugs as a qualitatively distinctive supply-chain phenomenon rather than simply as another category of narcotics.

A further empirical contribution lies in integrating precursor chemical governance into the analysis. Rather than treating precursor control as a technical subfield of drug policy, the thesis analyses it as an upstream security problem at the interface of licit chemical trade, international regulation, sanctions enforcement, and conflict economies. This is especially important in the Captagon case, where diversion cannot be understood solely as criminal trafficking but must be situated in relation to state capacity, sanctions pressure, regional conflict dynamics, and the limits of international monitoring systems.

From a policy perspective, the thesis argues that more resources, better technology and improved coordination are necessary but insufficient unless embedded in a governance architecture that recognises the structural character of the problem. Policy cannot be oriented toward eliminating vulnerability alone. It must manage residual risk, reduce predictable exploitation points, enhance institutional integrity and align mandates more closely with the supply-chain logic of the threat.

The overall originality of the thesis lies in treating synthetic drug supply chains as adaptive systems that exploit the structural tension between commercial openness and security control, rather than as criminal networks moving illicit commodities through otherwise neutral infrastructure.

3. Literature Review

The academic and policy literature relevant to this thesis bridges several distinct disciplinary and institutional communities. Scholarship on synthetic drugs, organised crime, border security, port governance, hybrid threats and societal resilience has advanced considerably, but these bodies of work have developed largely in isolation from one another.

This review maps four principal strands of literature, identifies their individual contributions and caveats, and shows why their fragmentation leaves an explanatory gap concerning the interaction between synthetic drug supply chains, logistics systems, and European security governance.

Beyond documenting fragmentation across these literatures, the review advances a specific analytical argument: that existing fields are individually sophisticated but collectively insufficient to explain why highly regulated, technology-intensive logistics systems remain structurally exploitable by adaptive synthetic drug supply chains.

3.1 Synthetic Drugs, Transnational Organised Crime and the Political Economy of Illicit Markets

The most substantial body of literature directly relevant to this thesis concerns the production, trafficking and market dynamics of synthetic drugs and their entanglement with transnational organised crime. Foundational contributions by Williams (2023) and Shelley (2014) have established that transnational organised crime is not a marginal or episodic phenomenon but a structurally embedded feature of the contemporary international order: one that exploits the same internationalised networks of trade, finance and communication that enable licit economic activity.

Naylor (2005) extends this argument by showing that illicit markets operate according to recognisable economic logics of supply, demand and profit maximisation, and that their persistence reflects structural incentives embedded in global trade and financial architectures, rather than enforcement failure alone. This political-economy perspective is foundational for the present thesis, which treats synthetic drug supply chains as profit-driven, adaptive systems rather than as the product of individual criminal pathology or temporary regulatory gaps.

Within this broader framework, the literature on synthetic drugs has expanded vastly since the early 2000s, driven in large part by the proliferation of amphetamine-type stimulants (ATS), new psychoactive substances (NPS) and, more recently, Captagon. Institutional assessments produced by the United Nations Office on Drugs and Crime (UNODC 2020, 2021, 2024, 2025), the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA 2023b, 2024b), and its successor, the European Union Drugs Agency (EUDA 2025), provide the most comprehensive empirical documentation of international synthetic drug markets, charting production volumes, precursor flows, trafficking routes, and market structures across regions.

These reports consistently underscore the adaptive resilience of synthetic drug networks, above all their reliance on flexible production sites, internationally traded precursor chemicals and rapid adjustment to enforcement pressure. This makes synthetic drugs a distinctive object of supply-chain governance, rather than simply another category of illicit narcotics.

The political economy of illicit markets has been further elaborated through the literature on war economies and conflict-linked supply chains. Kaldor's (2012) seminal analysis of new wars as networked, economically driven conflicts, in which the distinction between combatants and civilians, and between war and organised crime, is systematically eroded, provides a key conceptual framework for understanding how synthetic drug production can become structurally embedded in fragile and conflict-affected environments.

In this regard, the Captagon economy centred on Syria is paradigmatic. EMCDDA (2023a) and Steenkamp's qualitative study of the Jordan-Syria borderland show how Captagon production and export became woven into Syria's wartime political economy, connecting pre-existing pharmaceutical and transport infrastructure to state-crime relations, border insecurity and regional trafficking routes (Steenkamp 2025, 484–486, 488–491). This literature is central to the thesis's treatment of Captagon as a case of hybrid entanglement rather than merely as a criminal market.

Andreas (2013) provides a broader historical perspective on how illicit trade has persistently shaped state formation and geopolitical competition, contextualising the Syrian Captagon economy within longer cycles of state-crime interaction.

The growing literature on hybrid threats and criminal governance offers further conceptual grounding for situating synthetic drug supply chains within a security framework. Sullivan and Jones (2024), writing in the context of Latin American organised crime, examine how transnational criminal organisations generate security effects analytically comparable to state-sponsored hybrid actors through the systematic exploitation of governance gaps, corruption and critical infrastructure vulnerabilities.

Although their empirical focus is Latin America, especially Mexico, Venezuela, Brazil and Central America, the conceptual contribution is directly applicable to the European context: their demonstration that criminal networks can produce cross-domain effects on institutional integrity, governance capacity and state legitimacy, operating through networked alliances of criminal and corrupt state actors, supplies a model for understanding how synthetic drug supply chains cause hybrid security effects within the EU security perimeter. Sullivan and Jones differentiate carefully between intentional hybrid strategies and hybrid security effects, a distinction this thesis adopts in its analytical framework.

The Global Initiative Against Transnational Organized Crime (GI-TOC 2025) extends this line of analysis to the European context, documenting how criminal networks operating from the Western Balkans and other regions exploit jurisdictional seams, enforcement asymmetries, and corruption vulnerabilities in ways that systematically outpace incremental institutional reform.

Despite these major contributions, the literature on synthetic drugs and transnational organised crime has important limitations for the purposes of the present analysis. Much of this work remains primarily criminological or public health-oriented in its framing, treating logistics infrastructures and border regimes as technical variables rather than as strategic security vulnerabilities. The embeddedness of synthetic drug supply chains within European critical transport infrastructure, and their implications for institutional integrity, governance capacity and societal resilience, are rarely examined systematically.

3.2 Border Governance, Port Security and Maritime Supply Chain Vulnerability

A second major strand of literature analyses border governance, port security and the exposure inherent in maritime and containerised supply chains. This academic field

combines security studies, logistics research and operational assessments by international organisations, providing the empirical and conceptual foundations for understanding how major transport nodes function simultaneously as critical infrastructure for international trade and as structural vulnerabilities exploitable by illicit actors.

Notteboom, Pallis and Rodrigue (2026), in their comprehensive textbook on port economics and governance, describe major ports as complex, multi-actor ecosystems integrating commercial, regulatory, governance, and operational functions across public and private actors. Their analysis of port governance architectures, terminal concession arrangements, and port authority responsibilities establishes the institutional complexity that defines high-volume container hubs: a complexity that, as Ekwall (2009) shows, creates systematic constraints on security-oriented risk management. Ekwall's analysis of antagonistic threats against transport networks shows that the throughput pressures inherent in commercial port operations structurally limit the depth of inspection regimes, as intelligence-led targeting must operate within capacity and time constraints that organised criminal actors can anticipate and exploit.

This combination, institutional complexity documented by Notteboom et al. and structural throughput constraints analysed by Ekwall, directly informs the infrastructure vulnerability dimension of this thesis's analytical framework. Ekwall and Lantz (2018) extend this analysis to cargo crime specifically, demonstrating a persistent adaptation dynamic between control technologies and illicit network innovation, directly confirmed by Europol's (2023) documentation of criminal organisations exploiting gaps in risk-profiling systems at Antwerp-Bruges and Rotterdam.

The specifically security-oriented literature on port vulnerability and container control has developed substantially since the post-9/11 reconfiguration of international maritime security regimes. Barnes and Oloruntoba (2005) examine the conceptual dimensions of vulnerability in maritime supply chains, establishing an approach for understanding how dependencies on specific logistics nodes and the opacity of containerised flows create exploitable exposure.

Hintsa et al. (2009) analyse supply chain security management from a systems perspective, emphasising that effective security governance demands integration across

commercial, regulatory and enforcement actors, an integration that remains structurally incomplete in most major port ecosystems. Acciaro and Serra (2013) provide a critical review of maritime supply chain security, identifying persistent gaps between the formal architecture of international security regimes and operational realities at the port level.

A particularly significant addition to the formalisation of screening trade-offs comes from McLay and Dreiding (2012, 522), who develop linear programming models for multilevel, threshold-based cargo container security screening. Their analysis, focused on nuclear material detection at US ports of entry, shows that risk-based screening systems face fundamental trade-offs between detection probability and secondary screening capacity that cannot be resolved by simply upgrading inspection technology. While their specific models address nuclear rather than drug trafficking, the structural logic transfers directly: the trade-off between maximising commercial throughput and maximising inspection depth is mathematically irreducible under budget constraints, meaning that risk-based regimes will always generate residual vulnerabilities exploitable by illicit actors who understand the targeting logic. This formalisation offers analytical grounding for one of the thesis's core arguments: namely, that the persistence of drug trafficking through highly regulated port environments is not a governance failure amenable to incremental reform, but a structural feature of risk-based logistics security architecture.

In their comparative volume Ports, Crime and Security: Governing and Policing Seaports in a Changing World, Sergi, Reid, Storti and Easton (2021) provide a cross-national analysis of how port governance architectures, including public-private integration, law enforcement mandates, and customs cultures, shape exposure to organised crime infiltration. Sergi's broader research programme on port-crime interfaces (2020) shows that corruption and insider facilitation are not aberrant deviations from otherwise secure systems, but recurring features of ports as complex socio-economic environments, where the density of interactions between legitimate and illegitimate actors and opaque logistics processes create persistent integrity risks. This perspective supports the thesis's treatment of integrity vulnerabilities as a distinct analytical category.

The empirical literature on drug trafficking in major European ports has grown massively in recent years, fuelled by record-level seizures at Antwerp-Bruges and Rotterdam. Roks, Bisschop and Staring (2021, 171) provide a detailed analysis of cocaine trafficking networks operating through the Port of Rotterdam, examining through 73 interviews and

analysis of 10 criminal investigations how organised crime groups abuse the socio-spatial organisation of port ecosystems and cultivate insider relationships with dock workers, terminal operators and logistics personnel. Their key empirical finding, that transatlantic shipping lines structurally define Rotterdam's drug trafficking problem, since traffickers exploit existing licit trade routes rather than creating new ones, directly supports this thesis's argument about the dual-use character of logistics infrastructure.

Eski and Buijt (2017) complement this with their analysis of corruption dynamics among Rotterdam port employees, demonstrating that systemic integrity vulnerabilities rooted in the opacity and complexity of port operations enable sustained illicit access to containerised flows in ways that cannot be addressed through individual-level integrity measures alone.

The institutional literature created by Frontex (Annual Risk Analyses 2023, 2024, 2025), the EU Maritime Security Strategy (Council of the European Union 2023), and the World Customs Organization complements academic contributions by documenting operational dimensions of risk profiling, scanning technologies and inter-agency coordination across European borders.

However, this institutional literature tends to analyse border control from an operational and regulatory perspective, with limited engagement with the political economy of illicit markets and the strategic-level implications of synthetic drug supply chains for European security governance.

3.3 Hybrid Threats, Security Governance and European Institutional Architecture

A third body of literature, increasingly prominent in both academic and policy communities, merges hybrid threats, security governance and societal resilience within the European security space. The concept of hybrid threats, as elaborated in EU, NATO and OSCE doctrinal frameworks and developed in security studies scholarship, denotes the coordinated or cumulative use of military and non-military instruments, including economic, criminal, informational and societal tools, to undermine state and societal stability underneath the threshold of open armed conflict.

The NATO Strategic Concept (2022), the EU Strategic Compass (EEAS 2022), and the EU Security Union Strategy (European Commission 2020) all acknowledge organised crime,

corruption and illicit economies as components of the hybrid threat environment, reflecting a significant broadening of the concept beyond its original focus on state-sponsored disinformation and military ambiguity. This institutional recognition provides the policy architecture within which the present thesis situates its analytical argument.

The securitisation framework developed by Buzan, Wæver and de Wilde (1998) offers essential conceptual tools for understanding the processes through which issues are constituted as security problems and the institutional and political consequences they produce. Steenkamp (2025, 487–489) illustrates this dynamic empirically in her analysis of the Jordan-Syria borderland: she shows how Captagon trafficking came to be framed as a serious border-security threat by Jordanian authorities, contributing to an increasingly militarised border response. This included the deployment of the army instead of civilian border patrols and a more forceful interdiction posture against suspected smugglers. Steenkamp links this posture to dozens of deaths by 2022 (Steenkamp 2025, 478). This specific case shows both the analytical utility and the normative complexity of securitisation: it can mobilise institutional responses to serious security threats, but it can also generate difficult trade-offs for borderland communities affected by militarised enforcement (Steenkamp 2025, 489–491).

For this thesis, the securitisation framework matters in two ways: analytically, it directs attention to the framing processes through which synthetic drug trafficking has been increasingly positioned as a security challenge by Europol, EUDA, Frontex and national authorities. Normatively, it raises the question of whether such securitisation is analytically warranted or risks distorting policy responses.

Sullivan and Jones (2024) show, through their analysis of Latin American cartel and gang networks, that hybrid threats do not need to originate exclusively from state actors: criminal organisations can generate security effects comparable to state-sponsored hybrid actors through systematic exploitation of governance gaps, corruption, and critical infrastructure vulnerabilities. In their analysis of the Venezuelan Cartel of the Suns, using social network analysis of US Department of Justice indictments, they demonstrate how state and criminal actors become so intertwined as to erode the boundary between them, creating what they term 'state transformation' by organised crime. While the empirical cases are Latin American, the conceptual framework is directly transferable to the European context: the thesis argues that synthetic drug supply chains generate analogous

cross-domain effects on institutional integrity, governance capacity, and societal resilience within the EU security perimeter, independently of deliberate hybrid intent by criminal actors.

Security governance theory, as applied to the European context, shifts the analytical focus from individual state actors to the networks of institutions, legal frameworks, technologies, and practices involved in the collective provision of security across jurisdictions. The multi-level architecture of EU security institutions, encompassing Europol, Frontex, national customs and police authorities, port governance bodies, and international partners, including the UNODC and the World Customs Organization, constitutes the institutional environment within which synthetic drug supply chains are managed and, the thesis argues, systematically under-governed. The Europol SOCTA (2025) and GI-TOC's *Intersections* report (2024) document these coordination challenges empirically, noting that criminal networks exploit jurisdictional seams, information-sharing gaps and uneven enforcement capacity in ways that consistently outpace incremental institutional reform. The OSCE's work on countering illicit trade and enhancing transparency in free trade zones (OSCE 2024) provides additional institutional evidence of how specific governance architectures create and sustain exploitable vulnerabilities in cross-border commerce.

The concept of societal resilience has gained increasing prominence in European security discourse as a complement to deterrence- and enforcement-focused frameworks. Walker and Cooper (2011), in a foundational genealogical study published in Security Dialogue, trace how resilience as a risk management concept migrated from systems ecology in the 1970s into financial, urban and security governance discourses, where it came to reflect a broad consensus about managing risk through adaptation rather than elimination. Their key contribution, directly applicable to the present thesis, is that resilience frameworks can function ideologically to normalise structural vulnerability: by framing adaptation as the primary response to systemic risk, they can deflect attention from the structural conditions that generate exploitability in the first place.

For the analysis of synthetic drug supply chains, this element is significant: a resilience framework that focuses on institutional adaptation without interrogating why border governance architectures remain structurally exploitable risks reproducing rather than resolving the governance failures it seeks to address.

This thesis operationalises societal resilience across three dimensions: institutional, governance, and public health resilience to move beyond this limitation and assess concretely how synthetic drug supply chains affect the robustness of institutions and communities.

Steenkamp (2025, 489–491) also shows the complexity of border-security responses empirically in the Jordanian case. Jordan faced a serious and escalating Captagon trafficking threat along its northern border, leading to intensified enforcement measures and a more militarised border posture. These measures affected borderland communities, including bahhara cross-border trading networks, while trafficking networks adapted by drawing on pre-existing kinship networks and routes (Steenkamp 2025, 491–492).

A significant limitation of the hybrid threat and security governance literature remains: synthetic drug markets and their exploitation of global logistics systems have received limited systematic attention within these frameworks, which continue to focus predominantly on cyber operations, disinformation, energy security and state-sponsored influence activities.

3.4 Precursor Chemical Governance and the Upstream Political Economy of Synthetic Drug Production

A fourth strand of literature, less extensively developed in academic security studies but of central strategic importance to the present thesis, is about the governance of precursor chemicals and the international political economy of chemical trade regulation.

The control of precursor chemicals constitutes a critical upstream dimension of any comprehensive strategy to disrupt synthetic drug supply chains: without sustained access to the chemical inputs required for their manufacture, industrial-scale synthetic drug production cannot be maintained. The international regulatory framework for precursor control is anchored in the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and, in the EU, operationalised through instruments such as Regulation (EC) No 273/2004. Its central challenge is to reconcile legitimate pharmaceutical and chemical trade with the prevention of diversion into illicit production.

The International Narcotics Control Board (INCB 2024) provides the most authoritative institutional documentation of global precursor flows and diversion patterns, tracking

how criminal networks exploit flaws in export notification systems, free trade zones, and the regulatory capacity of transit and destination states. A consistent finding is that the geographic concentration of licit precursor chemical production, notably in China and India, which account for a substantial share of global production of key synthetic drug precursors, creates structural exposures at the interface between licit trade and illicit diversion. The UNODC's Global Synthetic Drugs Assessment situates precursor governance within the broader architecture of international drug control, identifying persistent vulnerabilities in the chain of custody between industrial production and diversion into conflict-linked or clandestine production networks (UNODC 2020). The OECD's 2025 implementation report on transparency in Free Trade Zones supports this point, noting that supervisory gaps, inadequate monitoring and limited transparency in these zones can enable the movement, storage and smuggling of illicit goods (OECD 2025, 3–4).

The Captagon case constitutes the most analytically developed illustration of how precursor governance failures interact with conflict economies and sanctions evasion. Steenkamp (2025, 485) documents that Syria's pre-war pharmaceutical industry, with its established infrastructure, technical expertise, and chemical supply networks, provided the structural foundation upon which wartime Captagon production was built. Precursor chemicals entered Syrian production networks through regime-controlled customs and import systems under the cover of legitimate industrial use, a dynamic that exposes a fundamental flaw of the international precursor control regime: its reliance on export notification and risk-based monitoring is structurally undermined when state-linked actors in the importing jurisdiction are themselves involved in the illicit production system.

The International Narcotics Control Strategy Report provides complementary intelligence-oriented assessments of precursor trafficking flows and the diplomatic dimensions of counter-narcotics cooperation, situating precursor governance within the broader geopolitical context of chemical trade regulation between major producer states and destination jurisdictions (United States Department of State 2025).

The academic literature on precursor chemical governance remains notably thinner than that on other dimensions of drug control, reflecting a broader neglect of the upstream political economy of synthetic drug production in security studies scholarship. What

exists tends to focus on specific chemical compounds and regulatory classification, or on case-specific investigations of diversion networks, without developing more expansive theoretical frameworks for understanding precursor governance as a dimension of international political economy.

3.5 Synthesis: The Analytical Gap and the Contribution of This Thesis

The four strands of literature reviewed above reveal a significant and consequential analytical gap. Synthetic drugs are well studied as criminal and public health phenomena. Border and port security are extensively analysed from technical, operational and regulatory perspectives. Hybrid threats are increasingly theorised in security studies and institutionalised in EU and NATO doctrine, while precursor governance is documented, if insufficiently theorised, in international drug-control literature. Yet integrated research remains limited on how synthetic drug supply chains operate as hybrid security threats integrated into international logistics systems, and on how illicit supply chain dynamics interact with border governance architectures and European security institutions. This absence is more than a cataloguing deficiency. It reflects a deeper theoretical problem: existing frameworks are better at describing institutional arrangements than at explaining why they fail to reduce exploitability in the face of adaptive illicit actors.

Three specific lacunae emerge from this review that the present thesis seeks to address. First, the dual-use character of trade and logistics infrastructure is systematically under-theorised in both the security governance and organised crime literatures: ports, containerisation, risk-based customs controls, and trade facilitation regimes simultaneously maximise legal throughput while generating predictable vulnerabilities exploitable by illicit actors. The mathematical formalisation offered by McLay and Dreiding (2012) for nuclear screening contexts demonstrates this irreducibility at the level of resource-constrained optimisation. The present thesis extends this structural finding to the domain of synthetic drug trafficking, arguing that the persistence of exploitability is not a governance flaw but a design feature of risk-based logistics security.

Second, the mechanisms through which synthetic drug supply chains produce cross-domain security effects, simultaneously affecting border infrastructure, institutional integrity and societal resilience, have not been coherently analysed within security studies frameworks. Sullivan and Jones (2024) offer conceptual foundations for

understanding criminal networks as hybrid threat actors, but their Latin American empirical focus leaves the European synthetic drug context analytically underserved.

Third, the connections between upstream precursor governance, regional geopolitics, and conflict-linked production networks, as documented by Steenkamp (2025, 479–486) for the Syria-Jordan corridor and institutionally mapped by the INCB and UNODC, have not been analytically integrated with the port-level and border-level governance challenges that constitute the downstream interface of the European security perimeter.

The vulnerability typology developed in this thesis provides the conceptual architecture through which these lacunae are addressed and through which the thesis assesses, comparatively across its three case studies, the structural mechanisms that allow synthetic drug supply chains to persist and evolve as hybrid security challenges despite continuous institutional reform and technological upgrading.

By combining concepts from security studies, international political economy, border governance research, and organised crime scholarship, this thesis addresses an explanatory puzzle that no single existing framework fully captures.

4. Theoretical Framework

This thesis treats synthetic drug supply chains as structural security problems rooted in international logistics and European border governance, rather than as criminal phenomena that use infrastructure. This distinction is the organising premise of the theoretical framework developed here.

Security governance is the analytical engine: the central puzzle is a governance paradox, not a criminal one. Criminal adaptability is well established. The more important question is why sophisticated, well-resourced and continuously reformed governance systems struggle to translate institutional investment into commensurate reductions in exploitability. Hybrid threat theory provides the strategic frame, the international political economy of illicit markets explains criminal adaptation, and societal resilience assesses the downstream effects on institutions, governance capacity and communities.

These four lenses are integrated through a single analytical logic: the dual-use paradox of logistics infrastructure.

4.1 The Dual-Use Paradox as the Central Analytical Tension

The central analytical tension of this thesis is what it terms the dual-use paradox of logistics infrastructure.

The paradox is this: the design features that make European ports, containerised shipping systems, land-border corridors, and precursor chemical trade networks maximally efficient for licit commerce are precisely the features that make them structurally exploitable by synthetic drug supply chains. Throughput optimisation, risk-based selective inspection, trusted trader schemes, transit facilitation, and supply-chain integration are not failures of governance that have inadvertently created vulnerabilities but rather successes that generate vulnerability as a predictable by-product.

If the exploitability of logistics infrastructure were a governance failure, it could be resolved through institutional reform, additional resources or better inter-agency coordination. If it is instead a structural consequence of the dual-use character of trade infrastructure, as this thesis argues, then no amount of incremental reform will eliminate it. The residual vulnerability is not an anomaly in the system. It is a structural feature of any logistics architecture that must simultaneously maximise commercial throughput and maintain security screening.

McLay and Dreiding (2012, 522) conceptualise this trade-off in the context of nuclear material screening: under any resource-constrained, risk-based regime, detection probability, and throughput efficiency are in irreducible tension. The present thesis extends this structural logic from nuclear security to synthetic drug trafficking, arguing that the comparable structural logic applies and generates the same implication: that risk-based border regimes will always contain exploitable residual vulnerabilities for illicit actors who understand the targeting logic.

The dual-use paradox operates at three levels that correspond directly to the thesis's three empirical cases. At the infrastructure level, containerised port ecosystems such as Antwerp-Bruges are optimised for high-speed, high-volume throughput in ways that structurally limit the depth of inspection regimes.

At the corridor level, land-border transit facilitation in the Western Balkans creates legal movement pathways that can also be exploited by synthetic drug and precursor trafficking networks.

At the upstream level, the global licit trade in chemical precursors, integrated into pharmaceutical and industrial supply chains, creates diversion opportunities that conflict-linked production networks exploit, as the Captagon economy of Syria-Jordan demonstrates.

4.2 Security Governance: The Analytical Engine

Security governance, as the analytical engine of this framework, shifts the focus from the attributes of criminal actors to the properties of the institutional systems that seek to manage them. The key question is therefore not whether criminal networks adapt, but why governance systems create conditions under which adaptation is rewarded. This approach is relevant for policy because it identifies institutional leverage points, even if these cannot eliminate the underlying dual-use tension.

Applied to the European context, security governance theory conceptualises security as the product of networks of institutions, legal frameworks, technologies and practices operating across multiple jurisdictions and sectors. In the domain of synthetic drug supply-chain governance, this network includes Frontex, Europol, the EU Drugs Agency, national customs, police and border authorities, port governance bodies, terminal operators, and international partners such as the UNODC, the World Customs Organization and the INCB. Each actor operates with a distinct mandate, risk model and organisational culture. This institutional plurality is both a resource and a structural source of coordination friction.

Three governance vulnerabilities are analytically central to this framework. The first is mandate fragmentation: the gap between the jurisdictional scope of individual institutions and the transnational operational scope of synthetic drug supply chains. Frontex operates at external borders, Europol conducts criminal intelligence, national customs authorities manage commercial flows, and port authorities govern terminal operations. Each institution is optimised for its own mandate. None is designed to govern the supply chain as an integrated system. Criminal networks, by contrast, operate across these institutional boundaries and exploit the gaps between them as structural entry points.

The second governance vulnerability is capability asymmetry: the gap between the rapid adaptation and technical sophistication of illicit supply-chains and the slower pace of

institutional reform. Europol's SOCTA (2025) documents how criminal networks respond to enforcement pressure by displacing flows, modifying concealment techniques, recruiting new insider networks and exploiting digital coordination tools in ways that outpace incremental regulatory change.

The third governance vulnerability is the legitimacy tension inherent in risk-based border regimes. Any governance approach that prioritises throughput and selective targeting over universal inspection must trade commercial facilitation against security depth. This creates predictable residual vulnerabilities. The tension cannot be resolved by governance reform alone. It can only be managed, and its management requires explicit acknowledgement of the trade-off rather than the assumption that it can be fully overcome.

The implication is not that European institutions are inadequately resourced or politically inattentive. The deeper problem is structural misalignment. The governance architecture is organised around mandates designed for distinct institutional purposes, while synthetic drug supply chains operate according to integrated supply-chain logic. Effective governance responses therefore require a coordination architecture capable of matching that logic, not simply more coordination among existing mandates.

4.3 Hybrid Security Threats: The Strategic Frame

The concept of hybrid threats, as employed in this thesis, requires careful analytical handling. The existing literature, including EU, NATO and OSCE doctrinal frameworks, uses the term primarily to describe state-sponsored strategies that combine military and non-military instruments to undermine adversaries below the threshold of open conflict. This state-centric framing is analytically insufficient for the purposes of the present thesis, for two reasons. First, synthetic drug supply chains are not primarily state-sponsored. They are fuelled by profit-maximising criminal networks whose strategic interests are economic, not geopolitical. Second, the hybrid character of these supply chains does not stem from deliberate strategy. The thesis makes no claim that synthetic drug trafficking constitutes hybrid warfare, nor that criminal actors pursue geopolitical goals. Rather, the hybrid character derives from the structural properties of the supply chains themselves: their ability to generate cross-domain security effects by exploiting institutional seams, logistical infrastructure and regulatory gaps, independently of any intent to do so. What

matters for European security governance is not the intent behind these operations but the strategically relevant effects and entanglements they produce.

This thesis therefore proposes an analytically refined application of the hybrid concept organised around two distinct modes. The first, hybrid effects, describes the cross-domain security consequences that synthetic drug supply chains produce within the EU's internal security space, independently of deliberate hybrid intent by criminal actors. These effects include the erosion of institutional integrity through corruption and insider facilitation, the degradation of governance capacity through the systematic exploitation of coordination failures, and the undermining of societal resilience through the public health, social cohesion and trust-in-institutions effects of synthetic drug markets. The second mode, hybrid entanglement, describes the contexts in the EU's wider neighbourhood where synthetic drug economies are structurally intertwined with conflict dynamics, sanctions evasion and state or quasi-state criminal linkages. The Captagon economy of Syria and its Eastern Mediterranean trafficking interfaces is the paradigmatic case. Here, the drug economy operates as a constitutive part of the conflict environment, with state military structures, foreign militia networks, and sanctions-evasion mechanisms forming the production and export infrastructure.

The distinction also enables differentiated empirical analysis: the Antwerp-Bruges case study primarily involves hybrid effects, while the Captagon/Levant case study involves hybrid entanglement, and the Western Balkans corridor case sits between them. It further generates governance-relevant propositions. Hybrid effects call for responses focused on institutional integrity, coordination architecture and resilience. Hybrid entanglement calls for responses that engage the geopolitical and sanctions-evasion dimensions of the supply chain.

The strategic salience of synthetic drug supply chains within the contemporary European security environment derives not from their analogy to military hybrid threats but from three structural features that distinguish them from conventional organised crime challenges. First, their scale and economic power create persistent capability asymmetries, as synthetic drug markets generate revenues that dwarf the budgets of many of the institutions tasked with governing them. Second, their cyber-physical integration means that the documented use of encrypted communications, data-driven container targeting and dark web coordination tools allows synthetic drug logistics to

operate as cyber-physical systems that outpace governance regimes designed for physical inspection. Third, their cross-domain coupling means that the same supply chain simultaneously exploits border control practices, logistics infrastructure, chemical regulation and institutional integrity, generating security effects across multiple governance domains that no single-sector institutional framework is equipped to address.

It is this third feature, cross-domain coupling, that most clearly distinguishes synthetic drug supply chains as hybrid security threats and most urgently demands an integrated governance response.

4.4 The International Political Economy of Illicit Markets: The Explanatory Mechanism

If security governance explains why institutional systems struggle, the international political economy of illicit markets explains why criminal systems succeed. This lens accounts for the adaptive resilience of synthetic drug supply chains and grounds the governance argument in the economic logic of profit-driven, transnational criminal networks.

The political-economy perspective treats synthetic drug supply chains not as pathological deviations from licit economic behaviour, but as economic systems operating according to recognisable logics of supply, demand, profit maximisation, and risk management. Their persistence reflects rational responses to the incentive structures created by the combination of prohibition, global trade integration and governance fragmentation. Three political-economy arguments are analytically central to the framework.

First, synthetic drug networks are rooted in licit trade infrastructure. They do not operate alongside the global logistics system but through it, exploiting the same containerised shipping routes, free trade zones, air cargo hubs and precursor chemical supply chains that underpin licit commerce. This embeddedness is not incidental but strategic: licit trade flows provide cover, capacity and connectivity that criminal networks could not replicate independently.

Second, criminal adaptation follows enforcement pressure with a structural regularity that reflects the economic logic of risk and return: when enforcement raises the cost of one trafficking modality, rational criminal actors shift to lower-cost alternatives,

producing the displacement dynamics that law enforcement agencies consistently document and that no border control technology has yet durably resolved.

Third, in conflict-affected environments such as Syria, the political economy of illicit markets intersects with war economies in ways that fundamentally alter the structure of the supply chain: state and quasi-state actors become participants rather than adversaries, sanctions regimes create both barriers and arbitrage opportunities, and the collapse of legitimate economic structures makes illicit production the rational choice for a wide range of actors who would not engage in it under normal conditions.

The upstream precursor dimension of the political economy deserves particular analytical attention because it is the dimension most neglected in existing governance frameworks. The global trade in chemical precursors is a licit, highly regulated and commercially essential activity: the same chemicals required for synthetic drug production are also required for pharmaceutical manufacturing, agricultural applications and industrial processes. The regulatory regime governing precursor trade, anchored in the 1988 UN Convention and operationalised through the INCB's monitoring functions, is structurally limited by its dependence on the cooperation of exporting states and the commercial interests of the chemical industry.

When state-linked actors in the importing jurisdiction are themselves implicated in the illicit production system, as in the Syrian Captagon case, this regulatory architecture loses much of its practical leverage, and the political economy of precursor diversion becomes a geopolitical problem that chemical regulation alone cannot address.

4.5 Societal Resilience: Assessing the Stakes

The fourth lens, societal resilience, serves a specific analytical function in this framework: it operationalises the downstream consequences of the dual-use paradox and the governance failures it generates, connecting the supply-chain analysis to the institutional and societal effects that give the governance puzzle its strategic significance.

This thesis operationalises societal resilience along three analytically distinct dimensions. Institutional resilience refers to the integrity and corruption-resistance of the organisations at the front line of supply-chain governance such as border authorities, customs administrations, port operators and law enforcement bodies. The documented evidence of systematic insider facilitation and corruption at major European ports is not

an institutional aberration, but rather a predictable consequence of the sustained, well-resourced pressure that high-value synthetic drug networks exert on the human nodes of the governance architecture. Institutional resilience, so understood, is not primarily a matter of individual integrity but of the structural conditions, such as workload, oversight, remuneration, and institutional culture, that make corruption a rational or irrational choice for the individuals occupying those nodes.

Governance resilience refers to the capacity of the multi-level EU and international security architecture to coordinate across agencies and jurisdictions, adapt to evolving trafficking modalities and sustain effective risk management under conditions of persistent adversarial adaptation. The consistent finding of governance fragmentation across the existing literature, documented by Europol, Frontex and the GI-TOC, suggests that governance resilience is the weakest dimension of the European response, and the one most directly targeted by the cross-domain coupling strategy of synthetic drug supply chains.

Public health and social resilience refers to the downstream effects of synthetic drug markets on health systems, community stability, social cohesion, and trust in public institutions. This dimension gives the governance challenge its ultimate societal significance and links the security analysis to the broader security-wellbeing nexus that European institutions have increasingly recognised.

The critical contribution of Walker and Cooper's (2011) genealogy of resilience to this framework is its warning against resilience discourse that naturalises structural vulnerability: framing adaptation to risk as a substitute for addressing the structural conditions that generate it. This thesis takes that warning seriously. The resilience framework employed here does not counsel acceptance.

It provides an analytical tool for identifying where the dual-use paradox inflicts the most damage on institutions and communities, and where governance reform is most urgently needed. The policy implication is to move beyond building more adaptive institutions and to change the governance architecture so that adaptation is not the only available response.

4.6 The Vulnerability Typology: An Original Analytical Contribution

The four theoretical lenses described above are integrated into an operational analytical instrument: a typology of synthetic drug supply-chain vulnerabilities organised around three categories, infrastructure vulnerabilities, governance vulnerabilities and integrity vulnerabilities. This typology functions as more than a descriptive classification scheme. It provides a theoretically grounded analytical tool that operationalises the intersection of logistics economics, security governance theory and institutional integrity research in ways that existing single-sector frameworks struggle to capture, and that generates directly comparable categories of evidence across the three case studies.

Infrastructure vulnerabilities are those that derive from the design properties of logistics systems such as the throughput optimisation, node dependence, containerisation opacity and risk-based inspection architecture that constitute the dual-use paradox in its most concrete form. They are structural and persistent: they cannot be eliminated by governance reform because they are not governance failures but design features. What governance reform can do is change the distribution of risk across the infrastructure system, shifting inspection burdens, altering targeting logics or restructuring incentive frameworks, without eliminating the underlying vulnerability. Understanding infrastructure vulnerabilities as structural rather than contingent recalibrates policy expectations: the goal of governance is not to eliminate exploitability but to manage it more effectively than current architectures allow.

Governance vulnerabilities are those that derive from the properties of the institutional architecture such as mandate fragmentation, coordination frictions, capability asymmetries and the legitimacy tensions inherent in risk-based governance. They are not structural in the same sense as infrastructure vulnerabilities, they are in principle amenable to reform, but they are deeply entrenched because they reflect the path-dependent development of European security institutions that were not designed to govern supply-chain-integrated threats. The analytical value of distinguishing governance vulnerabilities from infrastructure vulnerabilities is that it identifies a domain where targeted institutional reform can produce meaningful improvements in governance effectiveness, even if it cannot resolve the underlying dual-use paradox.

Integrity vulnerabilities are those that derive from the susceptibility of human and institutional nodes in the governance architecture to corruption, capture and insider facilitation.

They are the most politically sensitive category and the most directly amenable to supply-chain governance by criminal networks with sufficient economic resources. The systematic evidence of insider facilitation at Antwerp-Bruges and Rotterdam, documented by Roks, Bisschop and Staring (2021), Eski and Buijt (2017) and Sergi et al. (2021), demonstrates that integrity vulnerabilities are not random failures of individual actors but structural features of port ecosystems in which the density of interactions between licit and illicit actors, and the opacity of logistics processes, create endemic conditions for corruption. Addressing integrity vulnerabilities requires not just anti-corruption measures but a structural analysis of the conditions that make insider recruitment economically attractive.

The analytical power of the typology lies in its comparative application. By treating infrastructure, governance and integrity vulnerabilities as the common unit of comparison across the three empirical cases, Antwerp-Bruges, the Western Balkans corridor and the Captagon/Levant system, the thesis can identify which vulnerabilities are structurally recurrent across governance environments and which are context-specific. This comparative leverage is precisely what single-case port security studies or single-region drug trafficking analyses cannot generate.

4.7 Framework Integration and Governance Implications

The framework is integrated through the dual-use paradox. Security governance identifies the institutional conditions under which exploitability persists. The international political economy of illicit markets explains criminal adaptation, hybrid threat theory frames the cross-domain security effects, and the resilience lens assesses the cumulative institutional and societal damage. The vulnerability typology then translates this framework into comparable empirical categories across the three cases.

Three governance implications flow directly from this integrated framework and are assessed comparatively across the case studies. First, the persistent exploitability of European logistics infrastructure cannot be eliminated entirely. It must be managed through an explicit acknowledgement of the dual-use trade-off and a recalibration of

governance practices around residual vulnerability. Second, effective governance responses to synthetic drug supply chains require supply-chain integration of the institutional response, including a redesign of the mandate architecture to match the integrated operational logic of the threat. Third, the distinction between hybrid effects within the EU security space and hybrid entanglement in the wider neighbourhood has direct implications for institutional design: the former calls for integrity-focused, coordination-centred domestic governance responses, while the latter calls for geopolitically engaged, diplomatically active external responses that address the conflict and sanctions-evasion dimensions of the supply chain that domestic governance architectures are structurally unable to reach.

5. Methodology

This thesis uses a qualitative, interdisciplinary research design combining document analysis, comparative case study research, and institutional analysis to examine synthetic drug supply chains as hybrid security threats within the European security perimeter.

5.1 Research Design and Approach

Given the strategic, institutional, and transnational nature of the research question, a qualitative methodology is most appropriate. The methodological design takes the dual-use paradox of logistics infrastructure as its analytical point of departure: because the exploitability of European logistics systems is treated as a structural condition rather than a correctable governance failure, the analysis is oriented not toward measuring interdiction performance but toward identifying the mechanisms through which structural vulnerabilities are generated, maintained and exploited across distinct governance environments.

The thesis employs a structured analysis of policy documents, strategic concepts, and empirical reports in order to trace how synthetic drug production, trafficking routes, logistics hubs, and border control systems interact and how they are framed and addressed by European and international security actors.

This approach allows for an in-depth examination of governance structures, threat perceptions, and operational responses that cannot be adequately captured through quantitative methods alone.

The analytical strategy follows a mechanism-centred logic, advancing causal claims only where sequences are supported by congruent evidence from at least two independent source types, such as seizure data and judicial files, institutional assessments, and investigative journalism.

The comparative case design is intended to identify recurring structural mechanisms across distinct governance environments, thereby generating explanatory leverage rather than descriptive case narratives.

The thesis explicitly acknowledges that empirical data on illicit markets is inherently partial and often "dark": seizures, arrests, and institutional reporting reflect enforcement activity and visibility rather than the true volume or structure of flows. To mitigate this bias, the analysis relies on systematic triangulation across multiple independent source types (EUDA and UNODC market assessments, Europol and Frontex threat and risk analyses, World Customs Organization operational material, and peer-reviewed academic research), and treats quantitative indicators as signals of patterns and vulnerabilities rather than direct measures of market size.

Causal inferences are therefore formulated cautiously and grounded in convergent evidence across institutional, judicial and analytical sources.

The document analysis proceeds through a structured thematic approach based on the vulnerability typology. Sources are analysed for evidence of infrastructure vulnerability, governance vulnerability, integrity vulnerability, hybrid effects and hybrid entanglement. Within each category, the analysis identifies recurring indicators, causal mechanisms, and governance responses. This analytical categorisation is not intended to produce quantitative tallies, but to ensure that evidence is assessed consistently across cases and that cross-case comparison is based on the same analytical categories. Applying the same analytical framework across all three cases enables the comparative identification of which vulnerabilities are structurally recurrent and which are context-specific.

5.2 Sources

The empirical basis of the study consists primarily of institutional reports and strategic documents produced by UNODC, EUDA, Europol, Frontex, the World Customs Organization, the European Commission, the European External Action Service, the OSCE, and NATO. These sources are complemented by academic literature on hybrid threats,

security governance, border control, organised crime, synthetic drug markets, and illicit political economies, as well as policy papers and assessments by research institutes working on transnational crime, port security, sanctions evasion, war economies and societal resilience.

These sources are analysed with regard to their conceptual framing of synthetic drugs, their assessment of logistical and border vulnerabilities, and their evaluation of existing institutional responses.

More specifically, reports and practical guidance materials produced by the UNODC, including the UN Toolkit on Synthetic Drugs, as well as reports by the EU Drugs Agency (EUDA), Europol, and the International Narcotics Control Board, are used to analyse trends in synthetic drug production, precursor chemical flows, trafficking routes, market structures, and institutional response tools (UNODC 2020; UNODC 2026; EUDA 2025; Europol 2025; INCB 2024).

Frontex risk analyses, the Council of the European Union's Maritime Security Strategy, and World Customs Organization Container Control Programme reports provide the empirical basis for assessing vulnerabilities in ports and land-border regimes, as well as the role of risk profiling, scanning technologies and intelligence-led control. Strategic and doctrinal documents from the European Union, NATO and the OSCE, including the Strategic Compass, the Security Union Strategy, and the NATO Strategic Concept, are used to situate synthetic drug trafficking within broader hybrid threat and resilience frameworks.

Academic studies on port security, organised crime, and illicit political economy complement these institutional sources by offering conceptual and empirical analysis of how logistics infrastructures and governance arrangements are exploited by criminal networks.

5.3 Case Selection and Empirical Focus

To ground the analysis in concrete operational contexts while retaining comparative and analytical leverage, the thesis employs a comparative case study design centred on three complementary empirical arenas that together capture the production-transit-entry dynamics of synthetic drug supply chains relevant to the European security perimeter.

The cases are selected on the basis of (i) their strategic relevance for European security governance, (ii) their documented linkage to synthetic drug and precursor trafficking, and (iii) the availability of robust academic, institutional and open-source material.

Data availability differs across cases. While port ecosystems such as Antwerp-Bruges generate comparatively dense institutional reporting, corridor dynamics in the Western Balkans are characterised by "darker" and unevenly observed data. To mitigate this, the thesis relies on triangulation across independent source types (EUDA/UNODC market reporting, Europol threat assessments, Frontex risk analyses, OSCE and WCO documentation, and peer-reviewed regional research), and focuses on governance arrangements, enforcement-adaptation dynamics and documented route displacement patterns rather than attempting shipment-level reconstruction where evidence is not robust.

5.3.1 Case 1: The Port of Antwerp-Bruges (with Rotterdam as contextual comparator)

The Port of Antwerp-Bruges, as one of Europe's largest container hubs and a focal point of recent law enforcement and policy concern, constitutes a critical gateway for both licit trade and illicit flows, including synthetic drugs and precursor chemicals.

Together with the Port of Rotterdam as a comparative reference, this case is used to analyse vulnerabilities in port governance, containerised supply chains and critical infrastructure, with particular attention to risk profiling, non-intrusive inspection technologies, intelligence-led targeting, corruption and "insider" facilitation within complex port ecosystems.

5.3.2 Case 2: The Western Balkans land corridor

The Western Balkans corridor provides a key lens for examining the EU's external border regime and the interaction between transnational organised crime, border control capacities and multi-level security governance.

This case assesses how synthetic drugs and precursors move across land borders under conditions of uneven enforcement capacity, how trafficking routes adapt to interdiction pressure, and how institutional coordination operates between EU agencies, Member States and partner countries in Europe's immediate neighbourhood.

5.3.3 Case 3: The Captagon Economy of the Levant: War Economy, Transit States and the Eastern Mediterranean Interface (Syria-Jordan-Maritime Routes)

The Captagon economy centred on Syria represents a paradigmatic example of a conflict-linked synthetic drug system embedded in a war economy, a sanctions environment and state-crime or quasi-state entanglements. A central analytical focus is the upstream geopolitics of precursor supply.

Key chemical inputs used in Captagon production originate within the global pharmaceutical and chemical industries, notably in major producer states such as China and India, and enter the region through licit trade channels before being diverted into conflict-linked production networks.

Examining these precursor flows allows the case study to connect regional war economies to global regulatory regimes, export controls and diplomatic cooperation, thereby situating the Levantine Captagon system within the broader international political economy of chemical governance and sanctions enforcement.

Recent reporting suggests that the weakening and fragmentation of centralised regime control has transformed rather than resolved the Captagon production problem, with production reportedly becoming more dispersed and decentralised in parts of Syria. This reinforces the relevance of the case under conditions of fragmented state authority.

The analysis situates precursor diversion and control within relevant international and European regulatory frameworks, including the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (precursor control provisions) and the EU's precursor-control regime (e.g., Regulation (EC) No 273/2004 and related implementing instruments), as well as the institutional roles of the International Narcotics Control Board (INCB) and operational practices in export notification and risk-based monitoring.

In parallel, neighbouring transit states, in particular Jordan, constitute critical nodes of border governance and interdiction capacity along the land and air interfaces between production zones and export routes.

This case analyses upstream production and precursor diversion, transit-state border governance, maritime export routes towards European markets, and the ways in which

European and international actors respond to drug economies shaped by regional geopolitics, sanctions evasion and hybrid security dynamics.

The three cases therefore enable a structured and comparative analysis of:
(i) vulnerabilities in critical transport and logistics infrastructure within the EU;
(ii) governance challenges and coordination mechanisms along the EU's external land borders; and
(iii) the external, conflict-linked and geopolitical dimensions of synthetic drug supply chains affecting the European security perimeter.

While air cargo systems and the upstream geopolitics of precursor production inform the analytical framework, the thesis maintains a deliberately bounded empirical scope. The primary empirical focus is on (i) maritime containerised flows and port-ecosystem vulnerabilities (Case 1) and (ii) land-border corridor governance and adaptation dynamics (Case 2). Case 3 is analysed primarily through conflict-linked production, precursor diversion and the Eastern Mediterranean interface, rather than attempting comprehensive end-to-end mapping of all trafficking routes. Air cargo is acknowledged as relevant to contemporary synthetic drug logistics but falls outside the thesis's primary empirical focus due to data constraints and scope limitations.

While the three cases differ in geographic scale and empirical form (node, corridor, and conflict-linked production-transit ecosystem), analytical comparability is ensured through functional equivalence. The thesis treats the vulnerability typology, comprising infrastructure, governance, and integrity vulnerabilities, as the common unit of comparison across cases. Infrastructure vulnerabilities are assessed through dependence on specific logistics nodes and control chokepoints (e.g., containerised gateways, corridor bottlenecks, maritime interfaces). Governance vulnerabilities are assessed through mandate fragmentation, coordination mechanisms, and the operationalisation of risk-based control across agencies and jurisdictions. Integrity vulnerabilities are assessed through documented insider facilitation, corruption exposure, and institutional resilience to capture and compromise. This design enables systematic cross-case pattern identification despite differences in spatial scale.

The following matrix operationalises the vulnerability typology across the three case studies, specifying the empirical indicators and primary sources through which each

vulnerability dimension is assessed. This ensures that the comparative analysis produces directly comparable categories of evidence across cases that differ in geographic scale and institutional form.

Dimension	Empirical Indicators	Primary Sources	Case Application
Infrastructure vulnerability	Throughput pressure, node dependence, inspection limits, route concentration, containerisation opacity	Port authority reports, Europol, WCO, academic port security studies	All three cases; dominant in Case 1
Governance vulnerability	Mandate fragmentation, coordination gaps, uneven enforcement capacity, risk-based control limits, jurisdictional seams	Frontex, Europol, EU policy documents, OSCE, UNODC	All three cases; dominant in Case 2
Integrity vulnerability	Corruption exposure, insider facilitation, institutional capture, document fraud, susceptibility to criminal pressure	Judicial records, Europol, investigative reports, academic port studies	All three cases; especially port ecosystems and state-crime interfaces
Hybrid effects	Institutional erosion, cross-domain disruption, public trust degradation, resilience damage within EU security space	EU/NATO/OSCE strategic documents, EUDA, Europol threat assessments	Cases 1 and 2
Hybrid entanglement	Conflict economy integration, sanctions evasion, state-crime nexus, precursor diversion, war economy linkages	EUDA, UNODC, INCB, Steenkamp (2025), GI-TOC, policy reports	Case 3 (Captagon/Levant)

Table 1: Analytical Matrix: Vulnerability Typology, Indicators and Case Application

The case design thus juxtaposes hybrid effects within the EU's internal security space with hybrid entanglement in the EU's wider neighbourhood. This allows the hybridity

framework to connect internal border-governance challenges with external conflict-linked and geopolitical dynamics.

5.4 Analytical Strategy

The analysis proceeds in four steps.

Step 1: Supply chain mapping and node identification.

Synthetic drug supply chains relevant to Europe are mapped at the level of functionally relevant nodes, corridors and interfaces rather than as comprehensive end-to-end global chains. The mapping identifies the principal actors, logistics chokepoints, precursor-control interfaces and regulatory environments that connect (i) EU port entry ecosystems, (ii) external land-border corridors, and (iii) conflict-linked production-transit systems in Europe's wider neighbourhood.

Step 2: Analysis of enablement and disruption dynamics.

For each case, the analysis traces how illicit flows are enabled and where intervention points exist across the chain, including concealment modalities, insider facilitation, document fraud and routing practices.

Particular attention is given to the interaction between enforcement pressure and adaptation/displacement dynamics.

Step 3: Comparative assessment of border control technologies and governance practices.

The thesis compares how border control technologies and intelligence-led risk management are operationalised across cases, including container scanning, non-intrusive inspection, risk profiling, targeting systems, information exchange and multi-agency coordination, and how these measures shape interdiction capacity and criminal adaptation.

The analysis also considers cyber-physical facilitation, understood as the use of encrypted communications, digital coordination tools and logistics data to organise, conceal and adapt physical consignments. This dimension is not treated as a standalone cybersecurity domain, but as an enabling layer that interacts with risk-based border control, insider corruption and trade documentation practices.

Step 4: Governance gap and resilience assessment.

Using the hybrid security threat and societal resilience lenses, the thesis assesses broader implications for institutional integrity, governance capacity, corruption exposure, public health and social cohesion.

This step culminates in an assessment of structural gaps across EU and international response frameworks, focusing on coherence, mandate alignment, coordination mechanisms and strategic integration across crime control, border governance and resilience.

Throughout the analysis, the vulnerability typology serves as the primary comparative instrument, while the hybridity lens distinguishes between hybrid effects within the EU security space and hybrid entanglement in the wider neighbourhood. This ensures that the case studies generate comparable evidence rather than parallel descriptive narratives.

5.5 Interdisciplinary Dimension

The methodological design is anchored primarily in International Relations, specifically security studies, with international political economy serving as the secondary disciplinary lens. While security studies provides the conceptual tools to analyse hybrid threats, border regimes and institutional responses, international political economy helps explain the structure and functioning of illicit markets, supply chains, war economies and incentive structures.

This interdisciplinary approach enables a comprehensive analysis of synthetic drug trafficking as both a security and an economic phenomenon, and of border control as both a technical-operational and a political-governance challenge.

This methodology is designed to ensure analytical depth, policy relevance and theoretical coherence, and to allow for a systematic assessment of how synthetic drug supply chains challenge European security governance and societal resilience in a hybrid threat environment.

6. Case 1: The Port of Antwerp-Bruges: Infrastructure, Governance and Integrity Vulnerabilities in a High-Volume Container Ecosystem

The Port of Antwerp-Bruges is widely treated as Europe's most significant cocaine entry point. It is the paradigmatic site at which the dual-use paradox of logistics infrastructure becomes empirically visible in its most concentrated form, where all three categories of the vulnerability typology operate simultaneously and reinforce one another in ways that no single-sector governance response has proved capable of disrupting. This chapter applies the analytical framework developed in Section 4 to the Antwerp-Bruges case, with the Port of Rotterdam introduced at specific points as a contextual comparator. Its central empirical argument is that the exploitability of Antwerp-Bruges is not reducible to infrastructure design, governance fragmentation or insider corruption in isolation, but arises from the systemic interaction between all three. It is this interlocking character that makes the case analytically significant beyond its operational scale: Antwerp-Bruges shows that the dual-use paradox generates a self-reinforcing vulnerability architecture in which each category of weakness creates the conditions under which the others are amplified.

Although the most visible empirical evidence from Antwerp-Bruges concerns cocaine trafficking, the evidentiary centre of gravity of this case should not be confused with its analytical object. The chapter does not treat cocaine trafficking as interchangeable with synthetic drug trafficking, nor does it claim that Antwerp-Bruges is empirically representative of all synthetic drug supply chains. Rather, it uses Antwerp-Bruges as a high-intensity case of containerised logistics exploitability. This matters for the thesis because the same risk-based customs architecture, documentary verification systems, terminal data infrastructures and insider-access vulnerabilities that enable cocaine trafficking also create exploitable conditions for synthetic drug and precursor flows.

The chapter proceeds in four sections. Section 6.1 analyses the infrastructure vulnerabilities of the Antwerp-Bruges port ecosystem, examining how containerisation, throughput pressure and risk-based inspection architecture generate structurally embedded exploitability. Section 6.2 examines governance vulnerabilities, with the Stroomplan, Belgium's most ambitious coordinated response to port-based drug trafficking, as the analytical lens for understanding why even integrated governance

initiatives cannot resolve the structural tension at the core of the dual-use paradox. Section 6.3 analyses integrity vulnerabilities, arguing that insider facilitation at Antwerp-Bruges is a systemic feature of the port's socio-economic architecture rather than a correctable individual-level problem. Section 6.4 synthesises the three vulnerability categories in terms of their interaction effects, assesses the hybrid security implications for the EU's internal security space, and draws the comparative implications for the wider thesis framework.

6.1 Infrastructure Vulnerabilities: The Dual-Use Paradox in Concrete Form

6.1.1 Scale, Throughput and the Structural Limits of Inspection

The infrastructure of the Port of Antwerp-Bruges embodies the dual-use paradox at its most direct. The port handled approximately 13 to 14 million twenty-foot equivalent units (TEUs) annually (Port of Antwerp-Bruges 2025; Port of Antwerp-Bruges 2026), a slight increase on the previous year, ranking it among the top five container ports globally and the second largest in Europe after Rotterdam (Notteboom, Pallis and Rodrigue 2026).

Its commercial value to the Belgian and broader European economy is substantial: the port complex contributes an estimated 9.3 per cent of Belgium's GDP and directly and indirectly employs over 160,000 people (Port of Antwerp-Bruges 2023). This scale is not incidental to the port's vulnerability. Rather, it is constitutive of it. The same volume that makes Antwerp-Bruges indispensable to European trade logistics makes comprehensive physical inspection economically and operationally impossible. McLay and Dreiding (2012) model this trade-off in the context of risk-based container screening for nuclear material, showing that detection probability and throughput efficiency remain in persistent tension under resource-constrained regimes. The relevance for Antwerp-Bruges lies not in the specific commodity being screened, but in the shared optimisation problem: finite inspection capacity must be allocated across very large container flows. Increasing inspection depth without proportional increases in capacity necessarily reduces throughput, while maintaining throughput necessarily accepts a residual detection gap. At Antwerp-Bruges, this gap is structural and persistent.

Belgian customs authorities inspect fewer than two per cent of containers entering the port through physical examination, relying instead on risk-based profiling systems that

select a broader subset for non-intrusive scanning, primarily X-ray and gamma-ray imaging technologies, while allowing the majority of flows to proceed on the basis of documentary and intelligence assessments (UNODC/WCO/INTERPOL/ICAO 2025, 1; Europol 2023, 7). Containers are selected for inspection through indicators such as origin and transit route, commodity type, shipping documentation, consignee history, intelligence inputs and anomalies in cargo declarations. This creates an unavoidable asymmetry: customs and port-security actors must identify suspicious containers within a massive flow of legitimate trade, while trafficking networks need only insert illicit consignments into the residual space that remains outside inspection.

Criminal organisations have proven sustained ability to exploit this selectivity by routing shipments through intermediary ports in lower-risk jurisdictions, using front companies with established legitimate import histories and timing shipments to exploit periods of reduced inspection capacity (Europol 2023; GI-TOC 2024; Roks, Bisschop and Staring 2021). The result is not a failure of the targeting system but a structural feature of any risk-based regime: the targeting logic that makes selective inspection operationally feasible simultaneously provides illicit actors with a roadmap for evasion.

6.1.2 Containerisation, Node Dependence and the Opacity of Supply Chains

The containerisation system that underpins global trade logistics generates a specific form of infrastructure vulnerability that is distinct from throughput pressure: the opacity of containerised flows. A standard shipping container is a closed, sealed unit whose contents are declared through documentation but not directly observable without physical inspection. The global containerised logistics system processes over 800 million TEU movements annually (UNCTAD 2023), creating a volume of flows so large that the documentary declaration system, bills of lading, customs manifests, phytosanitary certificates, certificates of origin, functions as the primary verification mechanism for the overwhelming majority of commercial movements. This documentary architecture is simultaneously a commercial necessity and a structural vulnerability: it creates a system in which the integrity of the declared content is dependent on the integrity of the documentation, and documentation integrity is dependent on the integrity of the actors who produce it.

At Antwerp-Bruges, the node dependence of the European containerised logistics system amplifies this opacity vulnerability. The port's position as a primary transshipment hub for Northern and Central European markets means that a disproportionate share of containerised trade to and from a vast hinterland passes through a geographically concentrated infrastructure. This infrastructure consists of a handful of major terminals operated by a small number of global terminal operators including PSA International, DP World and MSC's TIL. This concentration creates both risk and opportunity for governance: risk, because successful penetration of the node provides access to a large volume of flows and opportunity, because the concentration of flows through monitored chokepoints creates the conditions for intelligence-led interception. The challenge is that the same terminal operators who manage the physical movement of containers also manage the data systems, port community information systems, container management platforms, booking and manifest data, on which risk-profiling depends. The cyber-physical integration of modern port logistics means that data access can become almost as operationally valuable as physical access: a criminal network with reliable intelligence about container movements, inspection schedules and targeting criteria possesses an informational advantage that partially neutralises the deterrent effect of scanning technology (Europol 2023; Sergi et al. 2021).

The synthetic drug and precursor dimension of Antwerp-Bruges's logistics vulnerability, while less extensively documented than cocaine trafficking, is empirically grounded. Belgium and the Netherlands together constitute the primary European production zone for MDMA and amphetamine-type stimulants, with Belgium reporting four MDMA laboratories dismantled in 2023 and the Netherlands reporting 32 (EUDA 2025). The precursor chemicals required for this production, including PMK glycidic derivatives, BMK glycidic derivatives and methylamine, are documented as entering the region through containerised import flows originating primarily from China, exploiting the same risk-based customs architecture and documentary verification systems that enable cocaine concealment (EMCDDA and Europol 2024a; EUDA 2025). In 2023, seizures of MDMA precursors in the EU reached 64.1 tonnes, up from 20.5 tonnes in 2022. That is a dramatic increase that EUDA attributes partly to improved detection but also to the expanding scale of precursor flows entering European logistics systems (EUDA 2025). The port ecosystem of Antwerp-Bruges and Rotterdam thus functions as a dual entry

point: for finished illicit commodities concealed within containerised cargo, and for the precursor chemicals that sustain synthetic drug production within the EU's own territory.

6.2 Governance Vulnerabilities: The Stroomplan and the Limits of Integrated Response

6.2.1 The Architecture of Fragmentation

The governance architecture of port security at Antwerp-Bruges involves a multiplicity of actors whose mandates, risk models and institutional cultures are systematically misaligned with the supply-chain integration of the illicit flows they seek to disrupt. Belgian federal police, the judicial police, customs authorities, the port authority, terminal operators' security departments, Europol liaison officers, and the Belgian financial intelligence unit (CTIF) all hold distinct and partially overlapping responsibilities for aspects of port security. At the European level, Frontex, Europol, the EU Anti-Fraud Office (OLAF) and the European Public Prosecutor's Office (EPPO) exercise varying degrees of coordination and oversight function. At the international level, the WCO's Container Control Programme, UNODC operational partnerships and bilateral customs cooperation agreements add further layers.

No single actor in this architecture has the mandate or the data access to govern the supply chain as an integrated system. Each institution is optimised for its specific function, customs for revenue and compliance, police for criminal investigation, intelligence services for threat assessment, port authority for operational management, and the seams between these functions are precisely the spaces that organised criminal networks systematically exploit (Easton 2020; Dinchel and Easton 2020).

The Rotterdam comparison is instructive here. The Port of Rotterdam operates under a governance architecture that differs from Antwerp-Bruges in one structurally significant respect: the Rotterdam port authority exercises a more centralised coordination function over security actors within the port perimeter, and the Dutch national police has historically maintained a more integrated presence within terminal security operations than its Belgian counterpart (Eski and Buijt 2017; Roks, Bisschop and Staring 2021). Rotterdam’s port-security ecosystem is also shaped by a denser institutional interface between municipal authorities, customs, port management, terminal operators and specialised police units, which allows security concerns to be integrated more directly

into port governance than in more fragmented institutional settings. At the same time, the Dutch case shows that governance integration changes the distribution of vulnerability rather than eliminating it: Roks, Bisschop and Staring's analysis of Rotterdam shows how trafficking networks exploit existing transatlantic shipping routes, container-handling routines and insider relations with dock workers and logistics personnel, while Eski and Buijt document how corruption among port employees remains embedded in the socio-economic organisation of port labour. Rotterdam therefore remains one of Europe's major cocaine entry points despite its more integrated governance architecture. The comparison illustrates a governance-analytical point that is central to this thesis: institutional integration can reduce some mandate-fragmentation vulnerabilities, but it cannot abolish the infrastructure and integrity vulnerabilities generated by high-volume containerised logistics.

6.2.2 The Stroomplan: Integrated Response and its Structural Limits

In direct response to the escalating cocaine crisis at Antwerp-Bruges, Belgian authorities launched the Stroomplan: a comprehensive, multi-agency policy framework designed to address drug trafficking through the port through integrated enforcement, prevention and institutional coordination. Initiated under the direction of the Belgian Federal Judicial Police in Antwerp and subsequently expanded in scope, the Stroomplan represents the most ambitious institutional attempt in Western Europe to operationalise a supply-chain integrated governance response to port-based drug trafficking. It established four working groups addressing respectively enforcement coordination, port employment and integrity, financial disruption, and international cooperation, and brought together actors from across the Belgian security, judicial and port management architecture in a sustained collaborative effort (Easton 2020; Sergi et al. 2021).

Institutionally, Stroomplan sought to move the Antwerp response away from fragmented enforcement by creating a more integrated port-security architecture linking federal police, customs, local authorities, prosecutors and port actors. Its measures included stronger information exchange, more targeted container controls, increased attention to insider threats, enhanced cooperation between law enforcement and port stakeholders, and a more explicit recognition of the port as a critical security rather than merely a commercial logistics node (Easton 2020; Sergi et al. 2021). These changes matter analytically because they show that Antwerp's vulnerability was not ignored by

governance actors. It was actively targeted through institutional integration. The persistence of trafficking despite these reforms therefore strengthens, rather than weakens, the thesis's argument that the problem is structural as well as institutional.

The Stroomplan produced measurable results. Seizures at Antwerp-Bruges increased substantially following its implementation, reaching record levels in 2022 and 2023. The working group on port employment developed new integrity screening frameworks for dock workers and terminal employees. The financial disruption component produced a number of significant asset seizures and money laundering investigations. International cooperation was expanded, particularly with Colombian and Ecuadorian authorities responsible for the primary cocaine export corridors (Port of Antwerp-Bruges 2023; Europol 2023).

And yet the Stroomplan has not resolved the fundamental problem. Seizure records are simultaneously evidence of enforcement success and evidence of the sustained scale of trafficking flows: a port at which 116 tonnes of cocaine can be seized in a single year is a port through which multiples of that quantity are moving undetected. The displacement dynamic documented between Antwerp-Bruges and Rotterdam illustrates the structural limit most clearly: as enforcement intensity increased at Antwerp-Bruges, trafficking networks adapted by increasing their use of Rotterdam and other secondary European ports, before returning to Antwerp-Bruges as enforcement attention shifted (Europol 2023; GI-TOC 2025). This is not a failure of the Stroomplan. Rather, it is evidence of the dual-use paradox operating precisely as the theoretical framework predicts. Enforcement investment raises the cost of exploitation at a specific node. Rational criminal actors then shift to lower-cost alternatives, enforcement follows, and criminal actors shift again. The supply-chain integration of the criminal network consistently outpaces the mandate-constrained, institutionally segmented response of the governance architecture.

The governance effect of intensified enforcement is therefore best understood as adaptive pressure rather than linear deterrence: successful disruption at one node can raise costs and interrupt flows, but it can also incentivise changes in routing, concealment, documentation practices and reliance on insiders capable of reading the control environment.

The Stroomplan's structural limit is analytically important for a reason that goes beyond its Belgian operational context. It shows that even the most ambitious integrated governance initiative available within existing institutional architectures cannot resolve the exploitability of logistics infrastructure, because the source of that exploitability is not institutional fragmentation per se. It is the dual-use design of the infrastructure itself. Institutional integration reduces governance vulnerability, but it does not eliminate infrastructure vulnerability. The Stroomplan addressed important governance vulnerabilities, but could not resolve the infrastructure dimension, because doing so would require restricting the commercial throughput on which the port's economic function depends. This is the governance paradox in its most concrete empirical form.

6.3 Integrity Vulnerabilities: Systemic Insider Facilitation and the Corruption Architecture of Port Ecosystems

6.3.1 Insider Facilitation as Structural Feature

The third category of vulnerability, integrity vulnerability, is the dimension that most directly connects the infrastructure and governance weaknesses of the Antwerp-Bruges ecosystem to the operational success of drug trafficking networks. Insider facilitation refers to the involvement of port employees, terminal operators, logistics company staff, customs officials and other individuals with authorised access to the port ecosystem in the enabling of illicit flows, whether through active participation in trafficking operations, passive tolerance of suspicious activity, or the provision of information about container movements, inspection schedules and targeting criteria to criminal networks.

The operational importance of insiders becomes particularly visible in so-called “rip-on/rip-off” methods, in which drugs are inserted into otherwise legitimate containers before shipment and removed after arrival without the knowledge of the cargo owner. This requires precise information about container numbers, terminal location, arrival time, security procedures and extraction windows. Other methods include the manipulation of container documentation, the use of cloned or fraudulent access credentials, and the recruitment of port workers or logistics personnel able to locate, release or move containers within the terminal environment. These practices show why port corruption is not an external addition to the trafficking process but an operational solution to the opacity and scale of containerised logistics (Europol 2023; Roks, Bisschop and Staring 2021).

The academic and institutional literature on insider facilitation at Antwerp-Bruges and Rotterdam consistently frames it as a structural feature of port ecosystems rather than an individual deviance problem. Roks, Bisschop and Staring (2021, 171), drawing on 73 interviews and the analysis of ten criminal investigations at Rotterdam, document how criminal networks systematically cultivate relationships with dock workers and terminal employees over extended periods, exploiting the social networks of port labour communities to identify and recruit individuals with the specific operational access required for particular trafficking operations. Their key finding, that trafficking networks do not corrupt the port so much as they exploit the social and organisational conditions the port already produces, is analytically central to the present thesis's treatment of integrity vulnerability as structurally embedded rather than contingent. Eski and Buijt (2017) reach an equivalent conclusion in their ethnographic study of corruption dynamics among Rotterdam port employees: the conditions that make individual port workers susceptible to criminal recruitment such as relatively modest remuneration combined with high-value access, the opacity of logistics processes that makes surveillance difficult, the normalisation of informal arrangements in a labour environment historically characterised by strong union culture and fragmented oversight are structural properties of the port labour market, not individual moral failures.

The structural conditions of port labour further increase this vulnerability. High-value consignments move through environments in which many workers occupy relatively routine positions but control access to commercially and criminally valuable information. The gap between ordinary wages and the potential value of a successful extraction creates strong recruitment incentives, while the complexity of subcontracting, shift work, temporary access rights and dispersed terminal operations makes oversight difficult. Corruption pressure is therefore not evenly distributed across the port: it concentrates on human nodes that combine access, information and weak visibility (Roks, Bisschop and Staring 2021; Eski and Buijt 2017).

At Antwerp-Bruges, the insider facilitation problem has been documented with particular specificity in recent Europol reporting (2023) and in the operational findings of the Stroomplan working group on port employment. The category of “insider” should therefore be understood broadly, encompassing not only corrupt officials but also dock workers, crane and straddle carrier operators, truck drivers, terminal employees,

customs liaison staff, logistics intermediaries and administrative personnel with access to container-management systems. The pattern that emerges from this evidence is consistent with the Roks et al. framework: criminal networks identify individuals with specific operational roles, container checkers, straddle carrier operators, gate clerks, customs liaison staff, whose position in the logistics chain provides the specific access required for a particular operation, and cultivate relationships with those individuals through social networks that predate and exist independently of any specific trafficking operation. The recruitment is often gradual and the initial asks are minor, information about a specific container's location, advance notice of an inspection, before escalating to direct participation in extraction operations. This gradualism makes early detection difficult and produces a population of port workers who are embedded in criminal relationships before any single act of facilitation that would trigger formal investigation.

6.3.2 The Rational Structure of Corruption and the Limits of Integrity Measures

The analytical significance of this pattern for the thesis's framework lies in what it reveals about the interaction between integrity vulnerability and the other two vulnerability categories. Infrastructure vulnerability creates the conditions under which insider knowledge has extraordinary value: in a system where fewer than two per cent of containers are physically inspected and the targeting logic is algorithmic, reliable intelligence about which containers are under scrutiny and which are passing freely is worth substantial sums to trafficking networks. The economic logic of corruption is therefore not aberrant but rational: the information asymmetry created by the risk-based inspection architecture generates a rent that criminal networks will consistently seek to capture through corruption, and the scale of the drug economy generates the financial resources to do so at a price that many port workers, earning wages that represent a small fraction of the value of a single successful trafficking operation, have proved susceptible to accepting.

Governance vulnerability amplifies this dynamic in a specific way. The mandate fragmentation that characterises the Antwerp-Bruges security architecture means that no single institution has comprehensive oversight of the human nodes through which insider facilitation operates. Terminal operators conduct their own background screening, the port authority manages access credentials, police intelligence tracks known criminal associations, and customs authorities monitor compliance behaviour. But the integration

of these oversight functions is incomplete, and the gaps between them create spaces in which individuals can maintain relationships with criminal networks without triggering a response from any single oversight actor. The Stroomplan's port employment working group identified this fragmentation as a primary structural barrier to effective integrity management, recommending consolidated personnel security screening across public and private actors. This is a recommendation that has been partially implemented but not fully resolved (Easton 2020).

The limits of integrity measures as a response to structurally embedded corruption are analytically important. Anti-corruption initiatives at Antwerp-Bruges, such as background screening, lifestyle auditing, anonymous reporting mechanisms, and awareness campaigns, address the individual dimension of the problem: they raise the cost of individual participation and improve the detection of established corrupt relationships. What they cannot do is alter the structural conditions that make corruption rational: the information asymmetry created by risk-based inspection, the wage differential between port employment and criminal recruitment payments, and the social network density of port labour communities that creates the recruitment pathways in the first place. These structural conditions are features of the port ecosystem that cannot be modified without altering either the commercial architecture of containerised logistics or the labour market conditions of port employment since both involve economic trade-offs that extend far beyond the institutional mandate of any security actor.

6.4 Synthesis: The Interlocking Vulnerability Architecture and its Hybrid Security Implications

The three vulnerability categories analysed in this chapter do not operate in isolation: they form an interlocking architecture in which each category creates and sustains the conditions under which the others are amplified. Infrastructure vulnerability generates the information asymmetries and inspection gaps that give insider knowledge its exceptional value, making corruption economically rational. Integrity vulnerability, the systematic cultivation of insider relationships, provides criminal networks with the information and access required to exploit infrastructure vulnerabilities more reliably than targeting algorithms can anticipate, further reducing the effective detection rate and reinforcing the operational logic of investment in corruption. Governance vulnerability prevents any single institutional actor from achieving the systemic oversight that would

be required to intervene in this feedback loop at multiple points simultaneously: the mandate fragmentation that distributes responsibility across customs, police, port authority, terminal operators and international partners ensures that the seams between institutional functions remain available as exploitation pathways even as individual institutional components improve their performance.

This interlocking character is the central empirical finding of this chapter, and it carries a specific implication for governance design that neither the infrastructure literature, the corruption literature, nor the security governance literature has previously articulated in integrated form. Addressing any single vulnerability category in isolation is likely to produce displacement rather than resolution. More scanning technology without integrity reform shifts criminal networks toward more sophisticated insider facilitation. Integrity reform without governance integration shifts exploitation toward the coordination gaps between reformed and unreformed institutional components. Governance integration without acknowledgement of the infrastructure constraint produces over-optimistic expectations about what institutional coordination can achieve against a structural design feature of commercial logistics. A governance response adequate to the interlocking vulnerability architecture must address all three categories simultaneously and must do so with explicit acknowledgement that the infrastructure constraint cannot be resolved, only managed, within the economic parameters of any port that must remain commercially competitive.

In terms of the thesis's hybrid security framework, the Antwerp-Bruges case primarily instantiates the hybrid effects mode. The cross-domain security consequences produced by the port ecosystem's exploitation are not the result of deliberate hybrid strategy by criminal actors but rather structural outputs of the system operating as designed. Institutional integrity is eroded through the systematic corruption of port workers and logistics personnel in ways that extend beyond individual criminal operations to affect the organisational culture and oversight capacity of the institutions involved. Governance capacity is degraded through the sustained exploitation of coordination gaps that leaves the security architecture perpetually reactive rather than preventive. And societal resilience is undermined in three ways: through the broader public health consequences of illicit drug markets linked to port-based supply chains, including but not limited to synthetic drug and precursor flows, through the trust-in-institutions effects of

documented corruption scandals involving port officials, and through the economic costs of an illicit economy embedded in Belgium's most strategically significant commercial infrastructure. These are hybrid effects in the analytically precise sense developed in Section 4.3: cross-domain security consequences produced below the threshold of deliberate strategic action, through the exploitation of structural vulnerabilities in systems designed for purposes other than security.

The Rotterdam comparator reinforces this analysis in a specific and comparative way. Rotterdam's somewhat more integrated governance architecture, particularly the more centralised coordination function of its port authority, has produced a different distribution of vulnerability without eliminating the fundamental dynamic. Rotterdam's somewhat stronger governance integration appears to reduce the governance vulnerability dimension relative to Antwerp-Bruges, but this has been partially offset by adaptation: criminal networks have demonstrated the capacity to shift operational emphasis between the two ports in response to enforcement pressure, exploiting the absence of a truly integrated cross-border governance response that treats the two ports as nodes in a single logistics system. The displacement dynamic documented between Antwerp-Bruges and Rotterdam is perhaps the clearest empirical demonstration available of the dual-use paradox operating at the system level: the governance response is necessarily bounded by national and institutional mandates, while the criminal network operates across those bounds with the same supply-chain integration as the licit logistics system it exploits.

This case has three governance implications. First, integrity reform at Antwerp-Bruges requires structural analysis of the conditions that make corruption rational, including wage structures, information asymmetries, and oversight gaps. Individual-level screening and awareness measures remain useful, but they are insufficient on their own. Second, the Stroomplan's integrated approach represents the appropriate governance direction but requires extension beyond Belgian national architecture to encompass a genuinely supply-chain integrated European response that treats Antwerp-Bruges and Rotterdam as components of a single governance problem. Third, and most fundamentally, the persistence of infrastructure vulnerability requires a recalibration of policy expectations. Governance at Antwerp-Bruges should not be framed around the elimination of drug trafficking, a standard that cannot be met without undermining the commercial

architecture that makes the port economically viable, but around the progressive reduction of exploitability through the simultaneous management of infrastructure, governance and integrity vulnerabilities.

7. Case 2: The Western Balkans Land Corridor: Governance Vulnerability, Route Adaptation and the Limits of EU External Border Coordination

If Case 1 confirms the dual-use paradox operating within the EU's internal logistics infrastructure, Case 2 shows it operating at the boundary between the EU's regulatory space and its immediate neighbourhood, portraying a boundary that is simultaneously a legal frontier, a governance seam and a persistently exploited trafficking corridor. The Western Balkans land route constitutes an important overland interface for illicit commodities, including synthetic drugs and chemical precursors moving between production and transit zones in the EU's wider neighbourhood and consumer markets within the Schengen area. Unlike the maritime port ecosystem of Antwerp-Bruges, the corridor's vulnerability is not primarily architectural, it is institutional. The dominant vulnerability category in this case is governance: fragmentation of mandates, capacities and coordination mechanisms across the EU, Member States, candidate countries and third-country partners prevents the external-border architecture from matching the supply-chain integration of the networks it seeks to disrupt.

The corridor is not analysed here as a synthetic-drug route in isolation. Like major European ports, it is a multi-commodity trafficking environment. Its relevance for this thesis lies in the fact that the same governance seams, transit facilitation arrangements, route-displacement dynamics and integrity vulnerabilities that structure broader illicit flows are directly relevant to synthetic drugs and precursor diversion.

The chapter is structured as follows. Section 7.1 analyses the corridor infrastructure, including the geography, route logic and transit facilitation arrangements that define the Western Balkans as a trafficking pathway. Section 7.2 examines governance vulnerabilities in depth, focusing on the coordination architecture between Frontex, Europol, national border forces and partner country authorities. Section 7.3 addresses integrity vulnerabilities, including the documented corruption and political-criminal linkages in Western Balkans border governance that partially overlap with hybrid entanglement dynamics. Section 7.4 synthesises the findings, assesses the route

adaptation dynamic as empirical evidence of the dual-use paradox at the corridor level, and positions the case within the hybrid effects/entanglement continuum established in the theoretical framework.

7.1 Corridor Infrastructure: Transit Facilitation and Structural Exploitability

The Western Balkans corridor is not a single route but a network of overlapping land-transit pathways connecting Turkey, the Western Balkans states, as in Serbia, North Macedonia, Bosnia and Herzegovina, Albania, Montenegro and Kosovo, to EU entry points in Croatia, Slovenia, Hungary, Bulgaria and Romania. Although the Balkan route has historically been associated above all with heroin trafficking, its contemporary relevance for this thesis lies in its broader function as a multi-commodity corridor through which synthetic drugs and precursor chemicals can exploit the same border-governance vulnerabilities. Its strategic significance for illicit supply chains derives directly from its significance for licit ones: the corridor is one of the primary overland arteries for commercial freight between Southeast Asia, the Middle East, Turkey and Central Europe, carrying hundreds of thousands of truck movements annually through border crossings that must process high volumes of commercial traffic within commercially viable timeframes (Frontex 2024; UNODC 2024).

Operationally, this corridor is structured around several recurring route logics rather than a single linear pathway. The central axis runs from Turkey through Bulgaria or North Macedonia into Serbia and onward toward Hungary, Croatia and Slovenia as entry points into the Schengen area. Alternative branches run through Albania, Montenegro, Kosovo and Bosnia and Herzegovina, linking Adriatic ports, secondary road networks and less monitored border segments to the wider European transport system. This multiplicity of route options matters analytically because it gives trafficking networks a wider adaptation space than a single port node: when enforcement pressure increases at one crossing or along one national segment, flows can be displaced toward neighbouring crossings, secondary roads or alternative national jurisdictions without leaving the broader corridor.

This commercial function generates the same dual-use dynamic at the corridor level that containerisation generates at the port level. Transit facilitation agreements, simplified customs procedures for frequent commercial carriers, and the operational pressure to

maintain throughput at major border crossings all reduce the depth of inspection in ways that are commercially necessary but structurally exploitable. Synthetic drugs, particularly amphetamine-type stimulants produced in Western Balkans clandestine laboratories or transiting from further east, are concealed within legitimate commercial consignments, personal vehicles, coach luggage and freight shipments in ways that are functionally comparable to the concealment methods documented at Antwerp-Bruges: the licit logistics infrastructure provides the cover, the volume and the routing logic that illicit flows exploit (Europol 2025; EMCDDA and Europol 2024a; GI-TOC 2025).

This matters particularly for synthetic drug supply chains because production and distribution are more geographically flexible than in plant-based drug markets, while precursor chemicals can move through licit or semi-licit commercial channels before diversion. The corridor therefore does not merely transport finished illicit products. It also links production capacity, precursor availability, commercial freight flows and EU consumer markets. Its relevance for this thesis lies precisely in this dual role: it functions both as a transit space for illicit commodities and as a governance seam through which licit, grey-zone and illicit flows can be recombined.

The corridor's infrastructure vulnerability has a specific geographic dimension that distinguishes it from port-based cases. Unlike a port, which is a discrete node with defined perimeters, the Western Balkans corridor is a diffuse network of crossing points, secondary roads, mountain passes and informal pathways.

Frontex risk analyses consistently document how enforcement pressure at major crossing points displaces trafficking flows toward less monitored secondary routes, resulting in a displacement dynamic that is geographically extensive and operationally flexible in ways that port-based enforcement cannot replicate (Frontex 2024). The corridor therefore embodies a version of the dual-use paradox that is less about inspection architecture and more about territorial scope: the EU's external border governance system is designed around designated crossing points, while the corridor's geography provides abundant alternatives.

7.2 Governance Vulnerabilities: Fragmentation Across the EU External Border Architecture

7.2.1 The Multi-Level Coordination Problem

The border-management system responsible for managing the Western Balkans corridor involves an exceptional degree of institutional layering. At the EU level, Frontex conducts joint border operations, deploys standing corps officers to EU member state borders, and coordinates intelligence sharing through its risk analysis framework. Europol provides criminal intelligence support and maintains liaison channels with Western Balkans partner authorities. The EU's enlargement and neighbourhood policy instruments, IPA funding, CEPOL training programmes, and bilateral cooperation agreements, provide capacity-building support to Western Balkans authorities. At the national level, the border forces, customs authorities and police of EU member states on the corridor's EU-side frontier, especially Croatia, Slovenia, Hungary, Bulgaria and Romania, exercise primary operational responsibility for enforcement. And at the partner-country level, the border and customs authorities of Western Balkans states operate under their own legal frameworks, with varying degrees of integration into EU coordination mechanisms and varying levels of institutional capacity (Frontex 2024; UNODC 2024).

No single actor in this architecture has the mandate or the data access to govern the corridor as a unified system. Frontex's operational mandate is bounded by the external borders of EU member states, meaning that it has no direct enforcement authority within Western Balkans partner countries. Europol's intelligence function is effective where national law enforcement agencies share information proactively, but information-sharing between EU member state police and Western Balkans partner authorities remains structurally uneven, constrained by legal framework differences, data protection concerns and institutional trust deficits. The capacity gap between well-resourced EU member state border forces and the often under-equipped, underpaid border authorities of Western Balkans partner countries creates asymmetries that trafficking networks exploit systematically: consignments intercepted at EU entry points frequently originate from border crossings earlier in the corridor where detection probability is lower (Europol 2025; GI-TOC 2025).

7.2.2 Route Adaptation as Evidence of Governance Fragmentation

The most analytically significant evidence of governance vulnerability in the Western Balkans corridor is the documented pattern of route adaptation in response to enforcement pressure. That pattern exhibits how governance fragmentation enables supply-chain integrated criminal adaptation. When enforcement intensity increases at a

specific crossing point or along a specific route segment, trafficking networks show a capacity to shift flows toward alternative pathways within the corridor network.

This adaptation can take several forms, including shifts from major motorway crossings to secondary border points, rerouting consignments between the Serbia-Hungary, Croatia-Slovenia, Bulgaria-Romania, and Adriatic branches of the corridor, movement of smaller quantities through private vehicles or coach routes, and changes to documentation and cargo descriptions designed to exploit differences in customs attention across jurisdictions. The crucial point is not that every route displacement follows the same pattern, but that the corridor provides enough geographic and institutional redundancy for displacement to remain a rational response to enforcement pressure. Frontex and Europol reporting repeatedly document this broader displacement logic: intensified controls at formal crossings can redirect flows toward neighbouring entry points, secondary roads or less visible informal routes, while capacity-building at selected nodes may improve local detection without producing corridor-level control (Frontex 2024; Europol 2025). For example, reporting on the Western Balkans route repeatedly notes that intensified controls at major official crossings can be accompanied by increased use of secondary crossings, informal routes and neighbouring border segments, illustrating how enforcement pressure may displace rather than suppress flows.

This adaptation dynamic is not primarily a function of criminal sophistication, but is rather a function of institutional segmentation. A corridor-integrated enforcement response, in which all crossing points along a given route segment were simultaneously subject to the same enhanced scrutiny, would reduce the displacement opportunity. Such a response is not available within the current cross-border enforcement structure because it would require simultaneous, coordinated enforcement action across multiple national jurisdictions and partner-country territories. That is precisely the cross-mandate, cross-border coordination that the existing framework cannot reliably produce. The route adaptation dynamic therefore serves as a diagnostic indicator of governance fragmentation as an operative mechanism: criminal networks adapt not because they are necessarily more capable than enforcement actors, but because the multi-jurisdictional enforcement chain gives them more degrees of freedom.

7.3 Integrity Vulnerabilities and the Political-Criminal Nexus

The Western Balkans corridor presents an integrity vulnerability profile that is qualitatively different from, and analytically more complex than, the port corruption documented in Case 1. At Antwerp-Bruges, integrity vulnerabilities are primarily socio-economic: port workers are recruited through social networks and economic incentives that exploit wage differentials and information asymmetries. In parts of the Western Balkans, the integrity challenge is more systemic. GI-TOC's Organized Crime Index identifies several states in the region as environments where criminal markets intersect with political patronage, weak institutional oversight and corruption vulnerabilities (GI-TOC 2025). The issue is not uniform state capture, but uneven institutional resilience across agencies, border segments and jurisdictions (GI-TOC 2025; Europol 2025).

Border integrity along the corridor is spatially uneven, characterised by localised pockets of institutional vulnerability rather than uniform state capture. In practical terms, these asymmetries may involve bribery of individual border or customs officials, document fraud, selective non-enforcement, leakage of operational information, political protection of trafficking intermediaries, or uneven willingness to share intelligence with EU partners. Integrity vulnerability in this case is therefore best understood as variable and spatially uneven rather than region-wide or uniform.

This political-criminal nexus has direct implications for border governance. Where border officials are embedded in networks of political patronage that overlap with criminal networks, integrity measures of the kind deployed at Antwerp-Bruges, as in background screening, lifestyle auditing, anonymous reporting, are insufficient, because the problem is not individual susceptibility to criminal recruitment but institutional capture at the structural level. Intelligence sharing with partner-country authorities is also constrained by this dynamic: EU agencies cannot reliably share operational intelligence about trafficking networks with border authorities whose institutional integrity cannot be guaranteed, creating a structural information asymmetry that benefits trafficking networks directly.

It is this dimension, the overlap between governance fragmentation and political-criminal entanglement in some Western Balkans states, that positions Case 2 analytically between the hybrid effects dominant in Case 1 and the hybrid entanglement dominant in Case 3. The Western Balkans corridor does not exhibit hybrid entanglement in the full sense

developed for the Captagon case: there is no conflict economy, no sanctions architecture and no state-level production involvement. The case should therefore not be read as a weaker version of the Captagon model, but as an intermediate form in which ordinary border-governance vulnerabilities are intensified by uneven integrity conditions and selective state-crime linkages. At the same time, in the specific sense of state-crime linkages that blur the boundary between public authority and criminal protection, and thereby generate security effects that transcend individual criminal acts, parts of the Western Balkans corridor exhibit dynamics that are closer to hybrid entanglement than to the purely structural hybrid effects of Case 1. This is consistent with the theoretical framework's positioning of the Western Balkans case as sitting between the two hybrid modes.

7.4 Synthesis: Governance Fragmentation, Adaptive Pressure and Hybrid Security Implications

The Western Balkans case shows that the dual-use paradox operates at the corridor level through a mechanism that is distinct from, but structurally analogous to, its operation at the port level. Where Antwerp-Bruges generates exploitability through the tension between commercial throughput and inspection depth, the Western Balkans corridor generates exploitability through the tension between transit facilitation and enforcement depth across a multi-jurisdictional enforcement chain. In both cases, the logic of the licit system, port efficiency at Antwerp-Bruges, and partial regulatory integration through enlargement and neighbourhood policy in the Western Balkans, creates governance conditions that illicit networks can exploit.

The route adaptation dynamic, analysed in Section 7.2.2, is the empirical signature of this mechanism at the corridor level. It demonstrates that governance fragmentation is an operational resource for trafficking networks, not just an institutional inconvenience. The multi-jurisdictional character of the cross-border enforcement chain is the structural condition that makes route adaptation consistently available as a criminal response to enforcement pressure. Addressing this dynamic requires not incremental improvement of individual crossing-point enforcement, the dominant modality of current EU capacity-building efforts, but a structural redesign of the cross-border coordination environment to produce corridor-level governance responses that match the corridor-level operational logic of the networks being targeted.

In hybrid security terms, the Western Balkans case primarily generates hybrid effects within the EU's internal security space: the systematic exploitation of external border governance seams degrades the EU's border integrity, undermines the effectiveness of Frontex and Europol mandates, and contributes to the sustained penetration of synthetic drug supply chains into Schengen territory. But the integrity dimension analysed in Section 7.3, the political-criminal nexus in parts of the corridor, introduces a partial hybrid entanglement dimension that the purely structural account of Case 1 does not capture. This positioning between the two hybrid modes is analytically valuable: it shows that hybrid effects and hybrid entanglement are not binary categories but points on a continuum, and that the same corridor can exhibit both dynamics simultaneously in different institutional and geographic sub-contexts.

Three governance implications follow from this case. First, corridor-level enforcement requires corridor-level governance architecture since the current EU external border system is designed around crossing-point management rather than network-level coordination, and this design mismatch is the primary structural source of the route adaptation dynamic. Second, capacity-building efforts in Western Balkans partner countries must explicitly address institutional integrity at the structural level, not only individual corruption, if they are to produce reliable enforcement partners rather than intelligence risks. Third, the EU's enlargement and neighbourhood policy instruments represent an underutilised governance lever: the conditionality architecture of the accession process creates incentives for institutional reform in Western Balkans states that border security capacity-building alone cannot generate, and aligning relevant security-governance reforms with rule-of-law and accession conditionality more explicitly would address the political-criminal nexus dimension in ways that operational enforcement cannot reach.

8. Case 3: The Captagon Economy of the Levant: Precursor Diversion, Conflict Economy and Hybrid Entanglement at the European Security Perimeter

Cases 1 and 2 demonstrate the dual-use paradox operating through infrastructure design and governance fragmentation within and at the borders of the EU's regulatory space. Case 3 demonstrates it operating upstream: in the political economy of production, the diversion of globally traded precursor chemicals, and the structural entanglement of a

synthetic drug economy with a conflict, a sanctions regime and state-crime linkages that extend to the Eastern Mediterranean interface with European security governance. Unlike Cases 1 and 2, which primarily show cross-domain security effects generated through the structural exploitation of licit systems, Case 3 shows the constitutive integration of a drug economy into a war economy, a sanctions-evasion architecture and a state-crime nexus that cannot be disaggregated from the political order of the producing region. This is why the Captagon economy of the Levant represents the clearest case of what this thesis terms hybrid entanglement.

The analytical value of this distinction is clearest in Case 3. In Cases 1 and 2, the dual-use paradox arises because licit systems are structurally exploitable, that is, ports, corridors, inspection architectures create the conditions of exploitability independently of any political entanglement. In Case 3, the licit system that is exploited is the global chemical trade, and the political entanglement is constitutive rather than contextual: the precursor diversion, the production networks and the export infrastructure cannot be understood as criminal phenomena operating within an otherwise stable political environment. They are embedded in the political economy of a fragmented and reconstituting state, sustained by actors whose involvement in the drug economy is inseparable from their role in the conflict, the sanctions regime and the regional power competition that defines the Levant's post-2011 political landscape. Governing this supply chain requires not only border control and chemical regulation but diplomatic engagement, sanctions enforcement and geopolitical analysis, resulting in a governance register that lies beyond the normal operating logic of the EU’s internal security architecture.

The chapter does not attempt a comprehensive history of the Syrian conflict, Gulf demand for Captagon or sanctions law. Its analytical focus is narrower: how precursor diversion, conflict-linked production, sanctions-evasion incentives and maritime or land-border interfaces combine to produce hybrid entanglement relevant to European security governance.

Because the Captagon economy is highly opaque and reporting on Syria's political and territorial fragmentation remains uneven, the chapter treats recent claims about production shifts cautiously and relies on convergent institutional, analytical and investigative sources where available.

The chapter proceeds as follows. Section 8.1 analyses precursor diversion as the upstream vulnerability connecting global chemical trade to Captagon production. Section 8.2 examines the state-crime entanglement and conflict economy dynamics that define hybrid entanglement in the Levantine context, with specific attention to reported fragmentation and decentralisation of production networks under conditions of weakened central authority. Section 8.3 analyses Jordan and the Eastern Mediterranean as the governance interface at which hybrid entanglement encounters the European security perimeter. Section 8.4 synthesises the findings, establishes the comparative position of Case 3 within the thesis's vulnerability typology and hybrid framework, and draws the governance implications.

8.1 Precursor Diversion: The Upstream Dual-Use Paradox

8.1.1 The Global Chemical Trade as Structural Vulnerability

The production of Captagon, the colloquial term for fenethylline and, increasingly, for a range of amphetamine-type stimulants produced and marketed under that name in the Middle East and Gulf, requires chemical inputs that are globally traded, commercially essential and deeply embedded in licit pharmaceutical, agricultural and industrial supply chains. Relevant precursor and pre-precursor chemicals include ephedrine, pseudoephedrine, phenylacetic acid and other controlled or non-controlled chemical inputs, depending on the production pathway and tablet composition. Their availability is governed by the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and operationalised through the INCB's pre-export notification system and import authorisation mechanisms, as well as through the EU's own precursor control regime under Regulation (EC) No 273/2004 and its implementing instruments (INCB 2024; UNODC 2024).

This regulatory architecture embodies the upstream version of the dual-use paradox in its most structurally exposed form. The same chemicals required for illicit synthetic drug production are required for legal pharmaceutical manufacturing: pseudoephedrine for cold and flu medication, ephedrine for asthma treatment, phenylacetic acid for a range of industrial applications. The global chemical trade cannot be restricted to the point of eliminating diversion without dismantling the supply chains that legal pharmaceutical production depends on. The regulatory response is therefore necessarily risk-based: pre-export notifications, import authorisation requirements, and suspicious transaction

reporting create a monitoring architecture that can detect anomalous flows but cannot prevent diversion by state or quasi-state actors with the institutional capacity to produce legitimate documentation, exploit bilateral trade relationships or operate through jurisdictions with weak enforcement capacity (INCB 2024; Steenkamp 2025, 485–486).

The specifically Syrian dimension of precursor vulnerability operates through multiple channels. During the Assad period, Syrian state and military-affiliated actors exploited Syria's formal participation in international chemical trade frameworks to acquire precursors through ostensibly legitimate import channels, as well as through diversion from domestic pharmaceutical stocks and through procurement via third-country intermediaries in jurisdictions where export controls were weakly enforced (Steenkamp 2025, 485–486; UNODC 2024). INCB precursor reporting has identified suspicious transaction patterns, anomalous chemical flows and diversion risks involving Syrian-linked entities and regional supply chains during this period, but the architecture of the pre-export notification system, dependent on the good faith of exporting state authorities and the reliability of import documentation, was structurally unable to prevent diversion where state-linked actors in the importing jurisdiction were themselves implicated in the illicit production system (INCB 2024).

8.1.2 Fragmentation of Production Networks and the Persistence of Precursor Vulnerability

Recent reporting suggests that the weakening and fragmentation of centralised regime control over parts of Syrian territory has transformed rather than resolved the precursor diversion problem**.** Where the Assad-era Captagon economy was characterised by relatively centralised production linked to military and security structures, particularly the Fourth Armoured Division under Maher al-Assad, recent assessments suggest a more fragmented landscape of smaller, more dispersed production networks involving former regime affiliates, militia networks, tribal intermediaries and opportunistic criminal entrepreneurs (GI-TOC 2025; Steenkamp 2025, 478–479, 488–489). This fragmentation complicates rather than reduces the precursor diversion problem. Centralised production is in principle more visible to intelligence monitoring and more amenable to diplomatic pressure than dispersed, decentralised networks. The fragmentation of production networks reduces the leverage points available to governance actors while maintaining, and potentially expanding, production capacity distributed across the territory.

The precursor vulnerability of this fragmented environment is further amplified by the weakening of whatever residual regulatory capacity Syrian state institutions maintained over chemical imports and pharmaceutical stocks. In an environment where state authority is fragmented among competing armed factions and the formal institutional architecture of chemical regulation is weakened, uneven or contested, precursor diversion is no longer a matter of state actors exploiting regulatory frameworks. It also becomes a matter of armed actors controlling territory on which chemical stocks and production infrastructure are physically present. The governance implication is significant: the INCB monitoring architecture, the EU's export control regime and bilateral diplomatic engagement are all designed to interact with state actors. Where state authority is fragmented or contested, these instruments lose much of their practical leverage.

8.2 State-Crime Entanglement and the Conflict Economy: Why This Is Hybrid Entanglement

The defining characteristic of Case 3, the feature that distinguishes it analytically from Cases 1 and 2 and justifies its classification as hybrid entanglement rather than hybrid effects, is the constitutive integration of the Captagon economy into the political economy of the Syrian conflict. This integration operated at multiple levels simultaneously during the Assad period and appears to have reconfigured under conditions of weakened and fragmented central authority.

Under the Assad regime, the Captagon economy was actively organised and protected by elements of the Syrian military and security apparatus. Steenkamp's (2025, 4) analysis of the Syria-Jordan corridor, drawing on 35 interviews with regional analysts, security officials and civil society actors, documents how the Fourth Armoured Division and associated militias functioned as production and export infrastructure, using military logistics networks, border checkpoints and protected transport channels to move Captagon shipments through Jordan toward Gulf markets and Eastern Mediterranean export routes. The revenues generated constituted a significant funding stream for armed actors whose operational capacity depended on income independent of the formal state budget. The drug economy and the conflict economy were not parallel phenomena. They were the same phenomenon operating through overlapping networks of actors, infrastructure and political protection.

This constitutive integration is what distinguishes hybrid entanglement from the hybrid effects of Cases 1 and 2. At Antwerp-Bruges, criminal networks generate cross-domain security effects by exploiting logistics infrastructure that was designed for commercial purposes. In the Western Balkans, trafficking networks exploit governance fragmentation across a multi-jurisdictional border architecture. In both cases, the licit system creates the conditions of exploitability, but the political order remains external to the drug economy: governance actors are trying to control a criminal phenomenon operating within a recognisable state environment. In the Levantine case, the political order is not external to the drug economy but constitutively embedded in it: the actors producing and exporting Captagon are simultaneously the actors exercising territorial control, managing border crossings, providing political protection to trafficking networks and evading international sanctions. Governing the supply chain therefore requires governing the political order: a task that lies beyond any drug control or border security mandate.

The sanctions dimension amplifies this hybrid entanglement in a specific and analytically important way. The international sanctions regime targeting the Assad government and associated actors, including EU, US and Arab League measures, created a financial isolation architecture that simultaneously attempted to constrain the regime's revenue sources and incentivised the development of sanctions-evasion mechanisms. The Captagon economy functioned as one such mechanism: it generated hard currency revenues through export markets in the Gulf that were outside the formal financial system, thereby providing a sanctions-resistant income stream that partially offset the regime's financial isolation. The drug economy was thus not merely a by-product of the conflict, but also an adaptive response to the incentives created by financial isolation and sanctions pressure, resulting in an unintended dilemma created by instruments designed to constrain the regime. This dynamic shows why the Captagon case cannot be governed through drug-control instruments alone: the supply chain is embedded in a geopolitical and sanctions architecture that shapes the incentive structures of the producing actors in ways that border control and chemical regulation cannot address.

8.3 Jordan and the Eastern Mediterranean: The Governance Interface

The point at which the Levantine hybrid entanglement encounters the European security perimeter is not the Syrian border but the network of transit and export interfaces that connect Levantine production zones to regional and international markets. Jordan

constitutes the primary land-border interface: it is simultaneously one of the most affected transit states for Captagon moving toward Gulf markets and a frontline interdiction actor whose border forces have conducted some of the most substantial seizure operations documented in the Levantine corridor (Steenkamp 2025; UNODC 2024). Jordan's position is structurally paradoxical: its geographic location and relatively functional border governance make it both a critical interdiction node and a potential transit corridor for consignments that successfully evade Jordanian controls.

The Eastern Mediterranean maritime dimension connects the Levantine production system to European markets through a set of shipping routes and port interfaces that run from Lebanese, Syrian and Turkish coastal areas toward Southern European ports, primarily in Greece, Italy and Cyprus, and onward into Northern European distribution networks. Institutional reporting has documented repeated attempts to move Captagon through Mediterranean maritime routes, demonstrating that the European interface is relevant even when Gulf markets remain the principal destination. Reported seizures in Southern European ports illustrate that Mediterranean routes can connect Levantine production systems to European logistics infrastructure, even where Gulf markets remain the principal destination.

These maritime routes exploit the same containerised logistics vulnerabilities documented in Case 1: Levantine shipments are concealed within legitimate commercial consignments, routed through intermediary ports in lower-risk jurisdictions, and targeted using insider access and documentation manipulation techniques that mirror those documented at Antwerp-Bruges. The difference is that the supply chain originates in a hybrid entanglement environment, meaning that the producing region is a conflict economy with state-crime linkages, while the entry infrastructure is the same European logistics system analysed in Cases 1 and 2. The Eastern Mediterranean interface therefore represents the point at which hybrid entanglement and hybrid effects meet: the entangled upstream production system connects to the structurally exploitable downstream logistics infrastructure, generating a supply chain that combines both modes of hybrid security challenge simultaneously. The primary consumer markets for Captagon remain outside the EU, particularly in the Gulf, but the case remains relevant to European security because the precursor flows, maritime interfaces, sanctions-evasion dynamics and

regional instability effects intersect with European governance instruments and the EU's wider security perimeter.

The governance challenge at this interface is compounded by the fragmented institutional architecture of the Eastern Mediterranean security environment. EU member states in Southern Europe, first and foremost Greece, Italy, Cyprus, exercise primary jurisdiction over their maritime borders and port entry points, but lack the intelligence resources and regional partnership infrastructure to systematically monitor Levantine trafficking networks whose operational centres are in Syria, Lebanon and Jordan.

Frontex's maritime surveillance operations in the Eastern Mediterranean are heavily shaped by irregular migration management and the mandate and operational culture of these missions is not optimised for synthetic drug and precursor trafficking. Europol's engagement with Levantine networks is constrained by the absence of functioning law enforcement partners in Syria and the limited bilateral cooperation architecture with Jordan and Lebanon. The UNODC's regional programmes provide some operational support and capacity-building, but the gap between the scale of the governance challenge and the institutional resources available to address it is substantial (UNODC 2024; Steenkamp 2025).

8.4 Synthesis: Hybrid Entanglement, Comparative Position and Governance Implications

Case 3 completes the three-level application of the dual-use paradox developed in this thesis. Case 1 demonstrates the paradox in containerised port infrastructure, where throughput optimisation and selective inspection generate residual vulnerability. Case 2 demonstrates it in transit facilitation and land-border governance, where corridor openness and multi-jurisdictional enforcement create route-adaptation opportunities. Case 3 demonstrates it upstream in global chemical trade and conflict-linked production, where commercially necessary precursor flows become embedded in a war economy, sanctions-evasion environment and state-crime nexus.

The vulnerability typology applies to Case 3 with a different weighting than in Cases 1 and 2. Infrastructure vulnerability is present since the Eastern Mediterranean maritime interface exploits the same containerised logistics vulnerabilities as Antwerp-Bruges but it is not the dominant category. Governance vulnerability is also present since the

institutional fragmentation of the Eastern Mediterranean security architecture mirrors the corridor governance failures of Case 2 but again it is not the primary analytical contribution of this case. At the upstream level, precursor vulnerability and integrity vulnerability converge in hybrid entanglement: the problem is not the individual corruption of port workers or the political-criminal linkages of border officials, but the structural implication of state-linked actors, military networks and criminal-political intermediaries in a conflict economy. This form of integrity failure cannot be addressed through anti-corruption measures, background screening or accession conditionality alone. It requires political and diplomatic instruments aimed at restoring legitimate governance capacity, disrupting protected production networks and rebuilding credible regulatory authority.

The hybrid entanglement classification of Case 3 is analytically justified on three grounds that distinguish it clearly from the hybrid effects of Cases 1 and 2. First, the actors generating the security effects are political-military actors for whom the drug economy is a constitutive element of their power base and resource structure, not criminal networks exploiting a licit system from outside. Second, the governance instruments required to address the supply chain include diplomatic engagement, sanctions enforcement, conflict resolution support and state-building assistance and none of these falls within the mandate of the EU's internal security architecture or the drug-control institutions whose primary remit is the downstream end of the supply chain. Third, the security effects produced by the Captagon economy extend beyond the drug trafficking domain into regional stability, sanctions regime integrity and the political order of a strategically significant neighbourhood, resulting in effects that are hybrid in the analytically precise sense of operating across multiple security domains simultaneously and below the threshold of any single governance response.

Three governance implications follow from Case 3 that are distinct from those generated by Cases 1 and 2. First, upstream precursor governance requires a geopolitical dimension that existing regulatory frameworks cannot provide: the INCB monitoring architecture and EU export control regime must be connected to diplomatic and sanctions enforcement instruments if they are to function in environments where state-linked actors are implicated in precursor diversion. Second, the Eastern Mediterranean interface requires dedicated institutional attention that neither Frontex's migration-focused

maritime mandate nor Europol's partner-constrained intelligence function currently provides. Closing this gap requires clearer institutional mechanisms for cross-domain engagement, whether through mandate adaptation, stronger liaison structures or dedicated regional coordination arrangements. Third, the reported fragmentation of Captagon production networks under conditions of weakened central authority represents both a challenge and an opportunity: disruption efforts may be more effective before decentralised production networks consolidate, but engagement with emerging or reconstituted Syrian authorities must be conditioned on credible evidence of their willingness and capacity to address precursor diversion and drug production.

The EU's external action instruments, the European Neighbourhood Policy, the EEAS and engagement with regional partners including Jordan, therefore represent relevant leverage points if deployed with explicit attention to the precursor and drug-economy dimensions of Syria's evolving political environment.

9. Conclusion: The Structural Persistence of Exploitability and the Governance Challenge Ahead

This thesis set out to answer a specific and consequential puzzle: why have synthetic drug supply chains been able to evolve into hybrid security challenges within the European security perimeter despite increasingly sophisticated border governance and control technologies?

The answer this thesis has developed is not that European institutions have failed, that criminal networks are unusually smart, or that political will has been insufficient. The answer is structural. Synthetic drug supply chains persist and evolve as hybrid security challenges because the logistics infrastructure, border governance architecture and chemical trade systems that European security depends on are constitutively dual-use: the same design features that make them maximally efficient for licit commerce also make them structurally exploitable by illicit supply chains. This exploitability is not simply a correctable deficiency. It is a feature of systems that must simultaneously maximise commercial throughput and maintain security enforcement.

Governance reform can reduce and redistribute this vulnerability, but it cannot eliminate the underlying tension entirely. It can only manage it more or less effectively. Managing it

better than current architectures allow requires a fundamentally different understanding of what the governance problem is.

9.1 Answering the Research Question

The thesis has argued that the persistence of synthetic drug supply chains as hybrid security challenges is produced by three categories of structural vulnerability, namely infrastructure, governance and integrity, that operate simultaneously across the European security perimeter and reinforce one another in ways that single-sector governance responses consistently fail to disrupt. These vulnerability categories are not independent pathologies. They form an interlocking architecture in which each creates and sustains the conditions under which the others are amplified.

Infrastructure vulnerabilities derive from the design properties of logistics systems, including throughput optimisation, selective inspection, containerisation opacity, and node dependence. These features cause residual exploitability as an irreducible by-product of commercial efficiency. As McLay and Dreiding (2012) set out in the context of risk-based screening, and as the Antwerp-Bruges case confirms empirically, detection probability and throughput efficiency are in irreducible tension under any resource-constrained regime. Risk-based inspection architectures will always contain exploitable residual vulnerabilities for actors who comprehend the targeting logic and the scale of the synthetic drug economy creates the resources to acquire that understanding systematically.

Governance vulnerabilities derive from the institutional architecture of the European security response: its mandate fragmentation, coordination frictions, capability asymmetries and the legitimacy tensions inherent in risk-based border regimes. No single institution has a comprehensive mandate or data access across synthetic drug supply chains as an integrated system. Frontex operates at external borders, Europol conducts criminal intelligence, national customs authorities manage commercial flows, and port authorities govern terminal operations. Criminal networks, on the contrary, operate across all of these institutional boundaries at the same time. The Western Balkans corridor case demonstrates this with particular clarity: the route adaptation dynamic that characterises the corridor is evidence that the multi-jurisdictional enforcement chain provides more degrees of freedom to trafficking networks than the governance architecture can systematically close rather than evidence of criminal sophistication.

Integrity vulnerabilities arise from the susceptibility of human and institutional nodes in the governance architecture to corruption, capture and insider facilitation and the conditions that generate this susceptibility are structural, not individual. At Antwerp-Bruges, the information asymmetry created by risk-based inspection makes insider knowledge extraordinarily valuable, and the wage structures of port labour markets make corruption economically rational. In the Western Balkans, the political-criminal nexus in parts of the corridor creates integrity vulnerabilities that anti-corruption measures cannot reach. In the Levantine case, state institutions were not individually corrupted but structurally captured: the drug economy was constitutively integrated into the conflict economy, and the actors producing Captagon were concurrently the actors exercising territorial control. These three integrity profiles are qualitatively distinct, and they call for qualitatively distinct governance responses.

The three supporting sub-questions posed in the Introduction are answered by this analysis in sequence. Why do structural characteristics of logistical nodes, precursor regimes and trade facilitation systems render them systematically exploitable? Because they are designed to maximise commercial efficiency in ways that necessarily limit security depth. Therefore, the dual-use paradox is not incidental to their design but constitutive of it. Why do intelligence-led border control technologies and risk-based governance practices generate adaptation, displacement and recurring vulnerabilities rather than durable deterrence? Because they operate within institutional boundaries that criminal networks cross freely, producing enforcement pressure that displaces rather than eliminates trafficking flows. Why do existing EU and international security governance frameworks struggle to integrate border security, organised crime control and societal resilience in a strategically coherent manner? Because the governance architecture was not designed around the supply-chain integration of the threat it is now confronted with. Rather, its mandates, legal frameworks and operational cultures were developed for specific institutional purposes, and the seams between them are the primary exploitation pathways available to illicit supply chains.

A possible counterargument is that rising seizures and expanded institutional cooperation demonstrate governance success rather than structural failure. This thesis does not deny such successes. Its argument is narrower: enforcement can raise costs, disrupt routes and improve detection, but these gains do not eliminate the residual

exploitability generated by risk-based logistics systems, fragmented mandates and adaptive illicit markets. The puzzle is therefore not whether governance works at all, but why governance success at specific nodes does not translate into durable reduction of supply-chain exploitability. The displacement dynamics documented across all three cases, between Antwerp-Bruges and Rotterdam, across Western Balkans corridor crossing points, and between centralised and fragmented Captagon production networks, are precisely the empirical evidence that this residual exploitability persists despite significant enforcement investment.

The dual-use paradox framework would be disconfirmed if evidence showed that risk-based logistics systems can be redesigned to eliminate residual exploitability without reducing commercial throughput. In other words, disconfirmation would require evidence that a port or border governance system can achieve maximal inspection depth and maximal commercial efficiency simultaneously and durably. It would also be disconfirmed if enforcement investment at specific nodes produced durable supply-chain-level reductions rather than displacement to adjacent nodes.

The absence of such evidence across all three cases, and the consistent documentation of displacement dynamics in Europol, Frontex and GI-TOC reporting, supports rather than proves the structural argument. The framework does not claim that governance is irrelevant. It claims that governance operating within existing institutional architectures cannot resolve the underlying infrastructure tension.

9.2 The Comparative Finding: What the Three Cases Prove Together

The comparative architecture of this thesis, three cases selected to represent distinct governance environments across the production-transit-entry geography of the European security perimeter, generates a finding that no single case could produce. Across Antwerp-Bruges, the Western Balkans corridor, and the Captagon economy of the Levant, the dual-use paradox operates at every level of the supply chain through the same structural logic, but with a different dominant vulnerability and a different governance register required to address it.

At the entry level, the port ecosystem of Antwerp-Bruges, infrastructure vulnerability is dominant. The dual-use paradox operates through the tension between commercial throughput and inspection depth. The governance challenge is first and foremost

technical and institutional: how to manage the residual exploitability of containerised logistics without dismantling the commercial architecture that makes the port economically viable. The Stroomplan shows that integrated governance responses can reduce governance and integrity vulnerabilities meaningfully, but cannot resolve the infrastructure constraint.

At the transit level, the Western Balkans corridor, governance vulnerability is dominant. The dual-use paradox operates through the tension between transit facilitation and enforcement depth across a multi-jurisdictional architecture. The governance challenge is primarily institutional and diplomatic: how to produce corridor-level coordination answers that match the corridor-level operational logic of trafficking networks, and how to address the integrity conditions in partner countries that make intelligence sharing structurally unreliable. Rule-of-law and accession conditionality within EU enlargement policy represents an underutilised instrument for structural governance reform that operational enforcement cannot produce.

At the upstream level, the Captagon economy of the Levant, precursor vulnerability and integrity vulnerability converge in hybrid entanglement. The dual-use paradox operates through the tension between internationally indispensable chemical trade and the diversion of precursors into conflict-linked production networks. The governance challenge is primarily geopolitical and diplomatic: how to connect chemical regulation and border control to sanctions enforcement, conflict resolution support and state-building assistance in ways that address the political economy of production rather than merely its downstream consequences. The Eastern Mediterranean interface is the point at which this upstream hybrid entanglement connects to the EU's own logistics infrastructure and it represents a governance gap that neither Frontex's migration mandate nor Europol's partner-constrained intelligence function is currently equipped to close.

The cross-case finding is this: the dual-use paradox is not a discrete vulnerability with a single governance solution. It is a structural property of the European security perimeter that manifests differently at various supply chain levels, requires different governance instruments at each level, and cannot be addressed by any single-sector institutional response.

The vulnerability typology developed in this thesis, infrastructure, governance and integrity vulnerabilities, provides the analytical instrument for identifying which category is dominant in any given governance environment and therefore which response is most likely to be effective.

9.3 Theoretical Contributions

This thesis makes three theoretical contributions that extend beyond its empirical cases. The first is the formalisation of the dual-use paradox of logistics infrastructure as an explanatory concept in security studies and border governance research. The paradox reframes the governance problem: exploitability is not a correctable flaw but a structural condition generated by the commercial success of the same systems that security actors are trying to protect. This reframing has direct implications for policy expectations, as in the goal of governance should be the managed reduction of exploitability, not its elimination, and for institutional design, which must explicitly acknowledge the infrastructure constraint rather than treating it as a problem that additional resources or better coordination will eventually resolve.

The second contribution is the analytical distinction between hybrid effects and hybrid entanglement as two distinct modes through which synthetic drug supply chains cause hybrid security challenges. Hybrid effects, the cross-domain security consequences produced within the EU's internal security space through structural exploitation of licit systems, call for integrity-focused, coordination-centred governance responses.

Hybrid entanglement, the constitutive integration of drug economies into conflict dynamics, war economies and state-crime linkages, calls for geopolitically engaged, diplomatically active responses that address the political economy of production. This differentiation prevents the conceptual inflation of applying the hybrid label to all organised crime while preserving its analytical utility for the genuinely cross-domain security challenges that synthetic drug supply chains generate. It offers a systematic application of the hybrid threat framework to the upstream political economy of synthetic drug production, an area that remains underdeveloped in the existing literature.

The third contribution is the vulnerability typology itself: the distinction between infrastructure, governance and integrity vulnerabilities as analytically distinct categories

that operationalise the dual-use paradox across distinct governance environments and enable systematic cross-case comparison.

The typology is not a descriptive classification scheme: it is a theoretically grounded analytical instrument that makes the dual-use paradox tractable, comparatively portable and policy-relevant in ways that existing single-sector frameworks cannot achieve. Its application across three empirical cases with different dominant vulnerabilities demonstrates its comparative leverage and supports its value as an analytical contribution to the field.

9.4 Policy Implications

The case studies developed several governance implications. This conclusion draws from them five cross-cutting implications that address the governance architecture holistically rather than any single institutional context.

The first implication is that governance reform must be explicitly oriented toward the managed reduction of exploitability rather than its elimination. Policy frameworks that set the elimination of drug trafficking as their operational standard will inevitably fail to meet their own stated objectives, misallocate resources toward unachievable targets, and fail to acknowledge the structural trade-off between commercial throughput and security depth that the dual-use paradox makes irreducible. An honest governance framework acknowledges this trade-off, sets realistic reduction targets derived from it, and evaluates success against those targets rather than against an impossible baseline of zero exploitability.

A second implication is that supply-chain integrated governance responses require supply-chain integrated institutional architectures. The current European security response is organised around mandates designed for distinct institutional purposes such as border management, criminal intelligence, customs compliance, and port administration rather than around the integrated supply-chain logic of the threat. Producing corridor-level or supply-chain-level governance responses requires either mandate redesign or new coordination mechanisms that bridge existing mandates with explicit supply-chain scope. The Stroomplan points in the right direction at the national level. Extending its logic to the European level, treating Antwerp-Bruges and Rotterdam,

and the Western Balkans corridor and its EU entry points, as interconnected governance problems, is the structural reform most urgently needed.

A third implication regarding integrity vulnerability requires structural analysis rather than individual-level responses. Anti-corruption measures, background screening, and awareness campaigns address the individual dimension of insider facilitation and border corruption. What they cannot do is alter the structural conditions that make corruption rational, such as information asymmetries, wage differentials, oversight gaps, and political-criminal linkages, because those conditions are features of the port ecosystem, the labour market, and the political economy of transit states that extend far beyond the institutional mandate of any security actor. Combatting integrity vulnerabilities structurally requires connecting security governance to labour market policy, port employment conditions, political reform conditionality, and the broader governance of the environments in which border officials and port workers operate.

A fourth implication is that the upstream precursor and conflict-economy dimensions of synthetic drug supply chains require governance instruments that the EU's internal security architecture does not yet command. Diplomatic engagement, sanctions enforcement, conflict resolution support, state-building assistance, and the conditionality architecture of the European Neighbourhood Policy are the instruments adequate to the Levantine case and, partially, to the Western Balkans political-criminal nexus. Connecting these external action instruments to the security governance framework that addresses the downstream end of the supply chain is not currently institutionalised in a sufficiently integrated way. The EEAS, the EU's enlargement policy apparatus, and its drug-control institutions operate in parallel rather than in integration. This institutional disconnect is itself a governance vulnerability that the thesis's framework identifies as structurally significant.

Fifth, technology is a governance tool, not a governance solution. Scanning systems, data analytics, as well as risk profiling and artificial intelligence-enabled targeting are key components of modern border control, and continued investment in them is warranted. But they do not resolve the dual-use paradox. Instead, they shift its terms. More sophisticated targeting raises the cost of conventional concealment methods and incentivises adaptation toward insider facilitation, documentation fraud, cyber-physical exploitation, and route displacement.

Treating technology as the primary answer to a structural governance problem produces a technological arms race in which criminal adaptation consistently maintains an advantage, because it is not constrained by institutional mandates, procurement cycles, or democratic accountability. Technology must be embedded in a governance framework that explicitly acknowledges what it can and cannot do.

9.5 Limitations and Future Research

This thesis operates under a few limitations that future research should address. First, the empirical analysis is based primarily on institutional reports, academic literature, and open-source material rather than direct field research or original expert interviews. The findings are grounded in the best available public evidence and are analytically defensible, but they should be understood as working conclusions subject to revision as more granular empirical data becomes available.

A second limitation concerns the use of Antwerp-Bruges as a port case in a thesis focused on synthetic drug supply chains. The empirical record on Antwerp-Bruges is strongest for cocaine trafficking, and this thesis does not treat cocaine and synthetic drugs as interchangeable markets. The case is used for a narrower methodological purpose: to analyse the structural exploitability of high-volume containerised logistics systems, including selective inspection, documentation opacity, terminal complexity, and insider access. These vulnerabilities are relevant to synthetic drug and precursor flows because they concern the logistics architecture itself rather than the specific commodity being transported.

Third, the thesis's focus on three specific cases, however analytically productive, leaves unexplored dimensions of the European synthetic drug supply chain that merit dedicated attention. The role of free trade zones within the EU and its neighbourhood as governance seams exploitable by illicit supply chains is documented in institutional reporting but not systematically analysed here. The financial architecture of synthetic drug supply chains, as in money laundering, hawala networks, cryptocurrency use, and the role of professional intermediaries in reinvesting criminal proceeds, constitutes an integrity vulnerability dimension that this thesis acknowledges but does not fully develop.

Fourth, the evolving political and territorial situation in Syria introduces empirical uncertainty into the Captagon case that no analysis based on currently available evidence

can fully resolve. The fragmentation of production networks, the emergence of new armed actors with economic interests in the drug trade, and the relationship between emerging authorities and territorial control structures in Syria and the international community are developments whose governance implications will take years to clarify. Future research should track these developments explicitly and assess whether the hybrid entanglement framework developed here requires refinement as the Syrian political landscape reconstitutes itself.

A further limitation concerns the exclusion of air cargo, postal parcels, and express courier infrastructure from the primary empirical analysis. These channels are highly relevant for some synthetic substances, especially low-volume, high-potency drugs and new psychoactive substances. The thesis nevertheless focuses on maritime and land-border systems because its central concern is the macro-logistical exploitability of industrial-scale synthetic drug and precursor supply chains, particularly Captagon, amphetamine-type stimulants, and bulk chemical inputs. Future research could extend the framework developed here to air cargo and parcel-based distribution systems, where the dual-use tension between speed, volume, and selective control operates in a different but related form.

Several avenues for future research follow directly from the thesis's analytical framework. The vulnerability typology could be applied systematically to other European port ecosystems, especially Hamburg, Valencia and Piraeus, to test whether the interlocking vulnerability architecture documented at Antwerp-Bruges and Rotterdam is structurally recurrent or partially context-specific. The hybrid effects/entanglement distinction could be applied to other conflict-linked drug economies, for example, Afghan heroin production networks and West African cocaine transit economies, to assess its analytical portability beyond the Levantine case. And the governance implication that supply-chain integrated institutional architectures are required to address supply-chain integrated threats could be operationalised as a comparative research programme examining institutional reform trajectories at Frontex, Europol and the EU Security Union against the analytical standard the thesis has established.

The broader significance of this thesis lies not only in what it says about synthetic drug supply chains but in what it demonstrates about the limits of governance in systems designed for purposes other than security. The dual-use paradox is not unique to logistics

infrastructure: it operates wherever commercially necessary openness creates structurally exploitable vulnerability such as in financial systems, in digital infrastructure, in the energy networks that sustain modern economies. Understanding how to govern the irreducible tension between openness and security is one of the defining institutional challenges of the contemporary international order. This thesis provides one analytically grounded contribution to that challenge, in one domain where it is particularly visible: the ports, corridors and chemical trade networks that simultaneously sustain and expose the European security perimeter.

10. Bibliography

10.1 Academic Literature

Acciaro, Michele, and Patrizia Serra. 2013. "Maritime Supply Chain Security: A Critical Review." In *Proceedings of the International Forum on Shipping, Ports and Airports*

(IFSPA) 2013: Trade, Supply Chain Activities and Transport - Contemporary Logistics and Maritime Issues, 636-651. Hong Kong: Hong Kong Polytechnic University.

Andreas, Peter. 2013. *Smuggler Nation: How Illicit Trade Made America*. Oxford: Oxford University Press.

Barnes, Paul, and Richard Oloruntoba. 2005. "Assurance of Security in Maritime Supply Chains: Conceptual Issues of Vulnerability and Crisis Management." *Journal of International Management* 11 (4): 519–540. https://doi.org/10.1016/j.intman.2005.09.008.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

Dinchel, Eva-Katharina, and Marleen Easton. 2020. "Going with the Flow: Comparative Research on Transnational Port Security." In *Policing Transnational Crime: Law Enforcement of Criminal Flows*, edited by Saskia Hufnagel and Anton Moiseienko, 29–47. London: Routledge. https://doi.org/10.4324/9781351132275-3.

Easton, Marleen. 2020. "Policing Flows of Drugs in the Harbor of Antwerp: A Nodal-Network Analysis." In *Maritime Supply Chains*, edited by Thierry Vanelslander and Christa Sys, 115–134. Amsterdam: Elsevier. https://doi.org/10.1016/B978-0-12-818421-9.00007-0.

Ekwall, Daniel. 2009. *Managing the Risk for Antagonistic Threats against the Transport Network*. PhD dissertation, Chalmers University of Technology, Gothenburg.

Ekwall, Daniel, and Björn Lantz. 2018. *Theft of Goods in Ports: A Review of TAPA EMEA IIS Statistics*. HAZARD Publication Series. University of Turku. http://hdl.handle.net/10227/211991.

Eski, Yarin, and Romano Buijt. 2017. "Dockers in Drugs: Policing the Illegal Drug Trade and Port Employee Corruption in the Port of Rotterdam." *Policing: A Journal of Policy and Practice* 11 (4): 371–86. https://doi.org/10.1093/police/paw044.

Hintsa, Juha, Ximena Gutierrez, Philip Wieser, and Ari-Pekka Hameri. 2009. "Supply Chain Security Management: An Overview." *International Journal of Logistics Systems and Management* 5 (3–4): 344–55. https://doi.org/10.1504/IJLSM.2009.022501.

Kaldor, Mary. 2012. *New and Old Wars: Organized Violence in a Global Era*. 3rd ed. Polity Press.

McLay, Laura A., and Rebecca Dreiding. 2012. "Multilevel, Threshold-Based Policies for Cargo Container Security Screening Systems." *European Journal of Operational Research* 220 (2): 522–29. https://doi.org/10.1016/j.ejor.2012.01.060.

Naylor, R. T. 2005. *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*. Rev. ed. Cornell University Press.

Notteboom, Theo, Athanasios Pallis, and Jean-Paul Rodrigue. 2026. *Port Economics, Management and Policy*. 2nd ed. New York: Routledge. https://doi.org/10.4324/9781003585367.

Roks, Robby, Lieselot Bisschop, and Richard Staring. 2021. "Getting a Foot in the Door: Spaces of Cocaine Trafficking in the Port of Rotterdam." *Trends in Organized Crime* 24 (2): 171–88. https://doi.org/10.1007/s12117-020-09394-8.

Sergi, Anna, Alexandria Reid, Luca Storti, and Marleen Easton. 2021. *Ports, Crime and Security: Governing and Policing Seaports in a Changing World*. Bristol University Press. https://doi.org/10.51952/9781529217735.

Shelley, Louise I. 2014. *Dirty Entanglements: Corruption, Crime, and Terrorism*. Cambridge University Press.

Steenkamp, Christina. 2025. "Captagon and Conflict: Drugs and War on the Border between Jordan and Syria." *Mediterranean Politics* 30 (3): 478–502. https://doi.org/10.1080/13629395.2023.2297121.

Sullivan, John P., and Nathan P. Jones. 2024. "Hybrid Threats: Cartel and Gang Links to Illicit Global Networks." *International Journal on Criminology* 11 (2): 13–38. https://doi.org/10.18278/ijc.11.2.1.

Walker, Jeremy, and Melinda Cooper. 2011. "Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation." *Security Dialogue* 42 (2): 143–60. https://doi.org/10.1177/0967010611399616.

Williams, Phil. 2023. "Transnational Organized Crime." In *Security Studies: An Introduction*, 4th ed., edited by Paul D. Williams and Matt McDonald. Routledge.

10.2 Institutional and Policy Sources

Council of the European Union. 2023. *EU Maritime Security Strategy (EUMSS) and Its Action Plan*. Brussels: Council of the European Union, 24 October 2023.

European Union Drugs Agency (EUDA). 2025. *European Drug Report 2025: Trends and Developments*. Lisbon: EUDA.

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). 2023a. *Captagon Trafficking and the Role of Europe*. Lisbon: EMCDDA.

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol. 2024a. *EU Drug Markets Analysis*. Lisbon: EMCDDA.

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). 2023b. *European Drug Report 2023: Trends and Developments*. Lisbon: EMCDDA.

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). 2024b. *European Drug Report 2024: Trends and Developments*. Lisbon: EMCDDA.

European Commission. 2020. *EU Security Union Strategy*. COM (2020) 605 final. Brussels: European Commission.

European External Action Service (EEAS). 2022. *A Strategic Compass for Security and Defence*. Brussels: EEAS.

Europol. 2023. *Criminal Networks in EU Ports: Risks and Challenges for Law Enforcement*. The Hague: Europol.

Europol. 2025. *EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025: The Changing DNA of Serious and Organised Crime*. The Hague: Europol.

Frontex. 2023. Annual *Risk Analysis for 2023/2024*. Warsaw: European Border and Coast Guard Agency. https://doi.org/10.2819/920282.

Frontex. 2024. *Annual Risk Analysis for 2024/2025.* Warsaw: European Border and Coast Guard Agency. https://www.frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2024-2025.pdf.

Frontex. 2025. *Annual Risk Analysis 2025/2026*. Warsaw: European Border and Coast Guard Agency. https://doi.org/10.2819/7710468.

Global Initiative Against Transnational Organized Crime. 2025. *Global Organized Crime Index 2025: Crime at a Crossroads*. Geneva: Global Initiative Against Transnational Organized Crime. https://ocindex.net.

Global Initiative Against Transnational Organized Crime. 2024. *Building Blocks of a Global Strategy Against Organized Crime*. Geneva: Global Initiative Against Transnational Organized Crime.

International Narcotics Control Board. 2024. *Precursors and Chemicals Frequently Used in the Illicit Manufacture of Narcotic Drugs and Psychotropic Substances: Report of the International Narcotics Control Board for 2023 on the Implementation of Article 12 of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988*. Vienna: United Nations.

NATO. 2022. *NATO 2022 Strategic Concept*. Brussels: NATO.

Organization for Security and Co-operation in Europe. 2024. *OSCE Approach to Preventing and Combating Organized Crime*. Vienna: Organization for Security and Co-operation in Europe.

OECD. 2025. *Report on the Implementation of the OECD Recommendation on Countering Illicit Trade: Enhancing Transparency in Free Trade Zones*. Paris: OECD.

Port of Antwerp-Bruges. 2023. *Facts & Figures 2023*. Antwerp: Port of Antwerp-Bruges.

Port of Antwerp-Bruges. 2025. *Factsheet Throughput Figures 2024*. Antwerp: Port of Antwerp-Bruges.

Port of Antwerp-Bruges. 2026. *Factsheet Throughput Figures 2025*. Antwerp: Port of Antwerp-Bruges.

UNCTAD. 2023. *Review of Maritime Transport 2023: Towards a Green and Just Transition*. Geneva: United Nations Conference on Trade and Development. https://unctad.org/rmt2023.

United Nations Office on Drugs and Crime. 2020. *Global Synthetic Drugs Assessment 2020*. Vienna: United Nations.

United Nations Office on Drugs and Crime. 2021. *UNODC Synthetic Drug Strategy*. Vienna: United Nations Office on Drugs and Crime.

United Nations Office on Drugs and Crime. 2026. "UN Toolkit on Synthetic Drugs." Accessed June 5, 2026. https://syntheticdrugs.unodc.org/syntheticdrugs/en/frontpage.html

United Nations Office on Drugs and Crime, World Customs Organization, INTERPOL, and International Civil Aviation Organization. 2025. "UNODC Passenger and Cargo Control Programme Annual Report 2024: Strengthening a Global Network Against Transnational Crime." Vienna: United Nations Office on Drugs and Crime.

United Nations Office on Drugs and Crime, World Customs Organization, INTERPOL, and International Civil Aviation Organization. 2026. "UNODC Passenger and Cargo Control Programme Annual Report 2025: Enhancing Global Connectivity through Secure Borders." Vienna: United Nations Office on Drugs and Crime.

United Nations Office on Drugs and Crime. 2024. *World Drug Report 2024*. Vienna: United Nations Office on Drugs and Crime.

United Nations Office on Drugs and Crime. 2025. *World Drug Report 2025.* Vienna: United Nations Office on Drugs and Crime.

United States Department of State. 2025. *2025 International Narcotics Control Strategy Report*. Washington, DC: United States Department of State.