



City Research Online

City St George's, University of London

Citation: Sodhi, M. S., Roscoe, S., Ellram, L. M., Tang, C., Sarkis, J., Handfield, R., Roehrich, J. & Schleper, M. (2025). Infiltration, Interdiction, and Other Covert Supply Chain Operations: A Research Agenda. *International Journal of Operations and Production Management*, 45(13), pp. 233-252. doi: 10.1108/ijopm-02-2025-0115

This is the published version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: <https://openaccess.city.ac.uk/id/eprint/35552/>

Link to published version: <https://doi.org/10.1108/ijopm-02-2025-0115>

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to [City Research Online policy](#).

Infiltration, interdiction, and other covert supply chain operations: a research agenda

International
Journal of
Operations &
Production
Management

233

ManMohan S. Sodhi

Bayes Business School, City St George's University of London, London, UK

Samuel Roscoe

*Department of Curriculum and Pedagogy (EDCP), UBC, Vancouver, Canada and
Thompson Rivers University, Kamloops, Canada*

Lisa Marie Ellram

*Department of Management, Farmer School of Business, Miami University, Oxford,
Ohio, USA*

Christopher Tang

*University of California Los Angeles Anderson School of Management, Los Angeles,
California, USA*

Joseph Sarkis

*Foisie Business School, Worcester Polytechnic Institute, Worcester,
Massachusetts, USA and*

Hanken School of Economics, Humlog Institute, Helsinki, Finland

Robert B. Handfield

*Poole College of Management, North Carolina State University, Raleigh,
North Carolina, USA*

Jens K. Roehrich

School of Management, University of Bath, Bath, UK, and

Martin C. Schleper

*Information Systems, Supply Chain Management and Decision Support Department,
NEOMA Business School – Reims Campus, Rouen, France*

Abstract

Purpose – The masterminds behind covert supply chain operations aim to hide their activities from government agencies and society at large, often for illegal gains or to intentionally cause harm. This conceptual article outlines a research agenda for future studies by framing covert supply chain activities and the countermeasures used to disrupt them.

Design/methodology/approach – Secondary data were collected from various news sources (observation) and analyzed to understand the nature of covert supply chain operations and efforts to identify and disrupt them (conceptualization).

Findings – To date, covert supply chain operations and counter-operations categories have been scarcely scrutinized in the supply chain literature, and our framework presents many fruitful avenues for further research.

Practical implications – Policymakers may aim to enhance the visibility of covert supply chains to achieve strategic objectives. Our framework enables logistics providers, network orchestrators, and shippers to identify vulnerabilities and detect covert infiltration by hostile actors within customer supply networks.

© ManMohan S. Sodhi, Samuel Roscoe, Lisa Marie Ellram, Christopher Tang, Joseph Sarkis, Robert B. Handfield, Jens K. Roehrich and Martin C. Schleper. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at [Link to the terms of the CC BY 4.0 licence](https://creativecommons.org/licenses/by/4.0/).



International Journal of Operations &
Production Management
Vol. 45 No. 13, 2025
pp. 233-252
Emerald Publishing Limited
e-ISSN: 1758-6593
p-ISSN: 0144-3577
DOI 10.1108/IJOPM-02-2025-0115

Originality/value – The mainstream supply chain literature has viewed supply chains of illegal goods and disruptive counter-operations as piecemeal. This conceptual article addresses the topic holistically to create a framework for guiding future research.

Keywords Smuggling, Trafficking, Supply chains, Disruption, Infiltration, Interdiction, Counter-operations, Illegitimate supply chains, Research agenda, Security, Counterfeiting

Paper type Conceptual paper

1. Introduction

In September 2024, a coordinated explosion of pagers and walkie-talkies in Beirut, Lebanon, sent hundreds of Hezbollah members, a militant group, to the hospital for emergency treatment and killed at least 12 people, including non-combatants (BBC, 2024a; FT, 2024). Soon after, Israeli Prime Minister Netanyahu took credit, announcing that he had launched the pager operation despite contrary advice from his country's security establishment (CNN, 2024). Later, on the US TV program *60 Minutes*, masked men claiming to be Mossad agents described using a covert supply chain and shell companies, including the Hungary-based BAC, to trick Taiwan-based Gold-Apollo into allowing them to use their brand for over ten years to sell pagers and walkie-talkies to Hezbollah with explosive material under the control of Israeli forces (CBS News, 2024).

The seriousness and covert nature of these actions have caught the attention of the supply chain community, especially regarding the safety of consumer-facing supply chains. While the supply chain risk management (SCRM) literature mainly focuses on natural disasters (Tang, 2006; Sodhi, 2016), financial crises (Blome and Schoenherr, 2011), or geopolitical tensions (Roscoe *et al.*, 2022; Duong *et al.*, 2025), limited focus has been given to covert activities by actors aiming to disrupt supply chains. The supply chain literature discusses covert operations in a fragmented manner across issues like counterfeiting (Stevenson and Busby, 2015), cybercrime (Melnyk *et al.*, 2022), industrial espionage (Carnovale *et al.*, 2022), drug smuggling (Basu, 2013; Skilton and Bernardes, 2022), or wildlife trafficking (Duensing *et al.*, 2023). Media reports highlight that both government and non-government actors conduct covert supply chain operations to cause disruptions, generate illicit profits, or inflict harm. Criminal organizations may operate their own supply chains for illegal drugs or arms trafficking. Alternatively, criminals might infiltrate legally established supply chains to smuggle contraband, conduct surveillance, or engage in cybercrime, often without the knowledge of legitimate supply chain operators. Law enforcement agencies have multiple teams dedicated to detecting and stopping such covert activities by disassembling them and disrupting the flow of materials, products, information, and capital.

Current research on *covert* supply chain activities—whether legally sanctioned or not—is scattered across various fields and lacks a solid foundation for further study despite its increasing importance. Therefore, this paper aims to develop a comprehensive understanding, vocabulary, and framework for these activities, providing supply chain scholars with a strong basis for their research. As a result, we pose the following question: *How can we frame covert supply chain operations?*

We gathered, examined, and cross-checked secondary information on events related to covert supply chain operations from various news outlets, including the BBC, New York Times, Financial Times, CNN, and The Economist. We used the first two stages of the four-stage research process, namely, *observation and conceptualization*, to create a framework that helps us classify observed events (Sodhi and Tang, 2014). Observing events associated with covert supply-chain phenomena is suitable for this emerging research area, as it prompts questions about “what,” “how,” or “why” certain events happen.

In doing so, we contribute to the existing OSCM literature by framing covert supply chain operations and efforts to disrupt them. We also highlight key areas for future research concerning covert supply chain activities and the countermeasures used to disrupt or prevent them.

2. Literature review and conceptual background

Supply chain management (SCM) coordinates material, information, and financial flows through partnerships between organizations, using vertical integration and contractual obligations to manage these flows (Ellram, 1991). An implicit assumption in much of the literature is that a supply chain operates within the legal boundaries, rules, and regulations of all the countries where it functions. However, not all supply chains involve legally sanctioned products or activities. Additionally, not all supply chain activities may be transparent to stakeholders from start to finish (Meehan and Pinnington, 2021), which can enable illegal activities.

Managers seek supply chain visibility to understand the status of upstream operations within their supply chains (Sodhi and Tang, 2019). Modern global supply chains are complex due to the presence of many suppliers worldwide at the first tier or even further upstream, with many involved in subcontracting (Marques *et al.*, 2024a; Meehan and Pinnington, 2021). This complexity, along with supplier reluctance to share information about sub-tier suppliers, creates a barrier for managers trying to gain better supply chain visibility (Sodhi and Tang, 2019). Additionally, companies often hide how they handle illegal activities in their corporate reports (Davenport and Leitch, 2005). For example, many companies do not report cyber-hacking incidents and instead pay ransom to criminals (Handfield *et al.*, 2025). The lack of standardization in reporting, regulations, and implementation further obstructs visibility for downstream buyers and decreases overall supply chain transparency for other stakeholders (Marshall *et al.*, 2016).

Suppliers and focal companies can also disengage — in this sense, “decouple” — from the supply chain, which can disrupt information flow and create conditions and incentives for illicit activities within the supply chain. Under ongoing price pressure from buyers and fluctuating demand, suppliers may claim to have limited control when responding to requests for information about non-compliant or illegal activities (Nath *et al.*, 2020). A focal company may appear to comply with regulations (Marques *et al.*, 2024b) but shift responsibility to suppliers in the event of negative reports, thereby splitting claims in corporate compliance reports from actual operational practices (Meehan and Pinnington, 2021; Marques *et al.*, 2024b). They might also avoid adopting technologies like blockchain, which provide visibility, to maintain deniability about possible illegal upstream activities in the supply chain (Marshall *et al.*, 2016). The consequent limited visibility in the supply chain for downstream buyers and stakeholders creates opportunities for covert activities to occur within legal supply chains.

2.1 Overt and covert supply chain operations

While any supply chain crossing multiple borders is subject to legal obligations from different national laws and enforcement levels, our focus here is on supply chains that attempt to bypass these obligations. A “legitimate supply chain” is designed to produce and deliver products and services from source to end user, with all businesses involved registered with and reporting to their respective regulatory agencies (Mueller *et al.*, 2009). In contrast, an “illegitimate supply chain,” such as one for illegal drugs like fentanyl, operates secretly to avoid detection by legal authorities and law enforcement (Basu, 2014). Although legality and legitimacy are not the same, we are using the terms interchangeably here.

Scholars from different fields have examined legitimate and illegitimate supply chain interference in some depth. These studies include the covert movement of illicit or illegitimate items within legitimate supply chains, and the disruption of supply chain flows to prevent criminal activities or harm (e.g. Basu, 2013; D’Amato and Papadimitriou, 2013; D’Amato *et al.*, 2019; Duensing *et al.*, 2023; Pullman *et al.*, 2024; Sánchez-Pérez *et al.*, 2023; El Baz *et al.*, 2025).

Zsidsin (2024) cautions against using terminology such as “legitimate” or “illegitimate” supply chains, as legitimacy depends on social norms and the perspective from which it is

viewed. He gives the example of the Underground Railway (e.g. [Still, 2019](#)), which helped enslaved people of African origin escape from the Confederacy. While it was considered an illegitimate supply chain by the Confederate government, it was viewed as legitimate by the governments of the Northern states to which they were escaping. Also, institutional logics and social norms change over time or differ across regions, even within the same country, as with the sale of marijuana in the US.

Because of these discrepancies, we categorize operations in supply chains as *either overt or covert*. We characterize these operations in a supply chain as “overt” if they comply with the legal frameworks, rules, and regulations of each country where the supply chain operates; therefore, there is no need to hide these operations, at least not from legal authorities. Overt supply chains are likely to seek legal protection from government authorities to counter external threats such as cybercrime, counterfeiting, or industrial espionage.

Conversely, operations in a supply chain are considered “covert” if they are deliberately hidden or disguised from government authorities, legitimate organizations within the supply chain, and the general public ([Zsidisin, 2024](#)). Such operations can expect to face prosecution by legal authorities unless the authorities themselves are involved in these covert activities. An entire supply chain may be deemed covert if all its operations from source to sale are hidden. However, covert operations can also occur in overt supply chains when there is insufficient visibility for the focal company throughout the supply chain.

We also define *counter-operations* as *actions or strategies used to partially or fully disrupt supply chain operations, whether covert or overt*. The same descriptors, overt and covert, characterize counter-operations, which help us frame real-life supply chain operations and counter-operations within a 2×2 overt-covert framework, as discussed in [Section 3](#). Counter-operations can vary in intensity and duration, such as occasionally intercepting drug shipments. Law enforcement authorities might choose to end or permit the operations of a covert supply chain involved in illegal narcotics using their own overt or covert operations.

2.2 Covert operations in covert and overt supply chains: infiltration

One way to keep covert operations hidden is by piggybacking on overt supply chains. For instance, the supply chain for fentanyl involves secret activities to produce and distribute the drug using visible supply routes. The *precursor* chemicals for fentanyl are usually manufactured in unmarked factories in China and India ([DEA.gov, 2020](#)). These chemicals are then shipped to Mexico, disguised as dog food or motor oil, to avoid detection ([DEA.gov, 2020](#); [FT, 2024](#)). Drug cartels operate hidden labs across Mexico to produce the final product, which they pack alongside pharmaceutical goods or deceptively label as legitimate medicine. This covert method allows cartels to utilize legitimate pharmaceutical supply chains to ship to the US, thus avoiding detection by border patrol, customs agents, and end users ([FT, 2023](#)).

Wildlife trafficking operates in a similar way. Animals are illegally poached, and their bodies or parts are secretly transported through legal supply chains, mostly using maritime container shipping ([South and Wyatt, 2011](#); [TRAFFIC, 2020](#)). An example is traffickers moving elephant tusks, pangolin scales, and animal skulls along with cut timber in containers. Malaysian officials intercepted one such shipment containing illegal items worth over US\$18 million ([The Independent, 2022](#)). Wildlife poaching at the beginning of these hidden supply chains often occurs in areas with weak government oversight or poor legal enforcement ([Duensing et al., 2023](#)).

The term “supply chain infiltration” refers to piggybacking on shipments that move through visible supply chains. D’Amato and Papadimitriou (2013: p. 998) define *supply chain infiltration* as covert actions involving an “unauthorized actor inserting (illegal) products or engaging (illegal) operations into a legitimate supply chain.” Infiltration occurs when actors within the supply chain have inadequate accountability or when government oversight is limited. Such actors have little incentive before the fact and face no accountability afterward to proactively stop illegal activities, despite eventually being impacted as stakeholders

(Duensing *et al.*, 2023). The reputational risk for cargo shipping companies, terminal operators, and logistics providers is minimal when it comes to detecting wildlife trafficking (Duensing *et al.*, 2023). In reality, criminals operating covertly and their enablers within infiltrated supply chains share the motive of ensuring quick and uninterrupted transfer of trafficked animals or their parts for economic reasons (Duensing *et al.*, 2023).

Counterfeiting is another method used by covert actors, driven by financial motives, to exploit supply chains and smuggle illegal goods. It involves trademark infringement and passing off a product as someone else's (Stevenson and Busby, 2015, p. 112). Covert actors produce counterfeit pharmaceutical products that imitate the original manufacturer's trademarks, often using the same contract manufacturers and transportation networks as major pharmaceutical companies (Trott and Hoecht, 2007). Luxury goods, including high-end handbags and clothing, are especially vulnerable to counterfeiting because these items are sometimes produced in the same factories as genuine designer products and travel through the same supply chains, but are ultimately sold at discounted prices (Wang *et al.*, 2020).

While our conceptual article mainly focuses on physical products, supply chain infiltration can also occur in the digital realm through cybersecurity breaches or industrial espionage. In 2020, covert actors hacked into SolarWinds, a major American information technology (IT) company, embedding malicious code (malware) into the company's software system. This code created a backdoor to customer IT systems, which hackers then accessed to install more malware (Melnyk *et al.*, 2022). State-sponsored cyberattacks have also been conducted to steal military secrets or gather sensitive information. In 2024, Chinese government agents reportedly sponsored a cyber actor, known as Volt Typhoon, to breach US government IT systems and compromise multiple critical infrastructure sectors in cyberspace, including communications, energy, transportation, and water (CISA.gov, 2024). Cyber-hijacking is also increasing, with notable incidents including a cyberattack on the shipping company Maersk in 2017, which disrupted shipments, and a fake broker scam in the US in 2020 (Sharp Blue, 2025).

Also in the digital world, companies engage in industrial espionage by exploiting vulnerabilities in a competitor's supply chain to steal intellectual property (IP) and proprietary knowledge (Carnovale *et al.*, 2022). In 2021, Fiat Chrysler accused General Motors of corporate espionage, alleging that GM agents impersonated former Fiat Chrysler employees in emails to gather information about a bribery scandal (Reuters.com, 2022).

There are some empirical studies on supply chain infiltration, but they are rare due to the secretive nature of these activities and the reluctance of perpetrators to self-incriminate (Naylor, 2004). Duensing *et al.* (2023) present a notable exception with interviews involving government officials, NGOs, and shipping companies that unintentionally took part in wildlife trafficking. They introduce the concept of "societal supply chain risk," defined as "hazards that originate from or occur within supply chains, and which mainly affect actors in the supply chain—and possibly even humanity as a whole" (p. 23). A study by Keskin *et al.* (2023) on wildlife trafficking highlights the difficulties in collecting primary data on illegal supply chains due to the fragmented efforts among government agencies and NGOs worldwide. They point out that most data come solely from successful seizures by enforcement agencies, which can lead to biased conclusions. Gathering primary data can be difficult when no detections or seizures occur (Keskin *et al.*, 2023). Consequently, most research relies on secondary data to develop conceptual models (e.g. Basu, 2014) and classify activities (e.g. D'Amato and Papadimitriou, 2013). Therefore, literature reviews on the topic do not provide empirical insights into the infiltration of these networks (e.g. Anzoom *et al.*, 2021).

While useful as a starting point, D'Amato and Papadimitriou's (2013) definition of *supply chain infiltration* is too narrow in our view because it focuses only on covert products or persons operating within overt supply chains. They do not consider *counter-operations* where covert actors operate unseen within covert supply chains, gathering intelligence to disrupt the operation later. For example, law enforcement agencies insert their covert agents or coerce embedded informers into covert drug smuggling or human trafficking rings to collect

intelligence for future disruption. Similarly, secret services like the US Central Intelligence Agency (CIA) and the UK Secret Intelligence Service (MI6) covertly use information systems and satellite imagery to digitally infiltrate the overt supply chains of other countries (Smith, 2022), thereby gathering information about both covert and overt supply chains.

It is therefore essential to consider covert actors who infiltrate: (1) overt supply chain operations to secretly move people, products, or capital; and (2) covert or overt supply chains to gather information, possibly for future disruption. In both cases, the actors' aim is to stay hidden and ensure supply chain continuity, at least in the short or medium term. We can now present a more comprehensive definition.

Supply chain infiltration by covert actors is the insertion of products and actors into a supply chain, whether covert or overt, without the knowledge of its operators. These actors maintain the continuity of the infiltrated supply chain while using it to move their illicit products or collect information without authorization.

While infiltration maintains the continuity of the target supply chain, in the short or medium term, the ultimate aim may be to disrupt the infiltrated supply chain or cause harm to other stakeholders.

2.3 Counter-operations to disrupting covert or overt supply chains: interdiction

The goal for supply chain managers is to maintain supply chain continuity, defined as “the minimization of disruption to the supply of products, services, and information” (Autry and Bobbitt, 2008: p. 57). However, other actors may seek to disrupt this continuity. An example is when explosive devices were hidden inside massage units and shipped internationally via DHL, a third-party logistics provider (WSJ, 2024). Two of these devices detonated during transit at DHL distribution hubs in Germany and the United Kingdom (UK) (WSJ, 2024). Western security officials claimed that these devices were part of a covert Russian government operation intended to disrupt, or at least threaten, transportation routes across the Atlantic, particularly given the ease with which these devices were discovered (WSJ, 2024).

There have also been accusations that certain governments were involved in the explosion of the Russian Nord Stream 1 and 2 gas pipelines supplying Europe (The Atlantic, 2023), following US President Biden's threat to “bring an end” to the second pipeline (NBC, 2022) and Germany's subsequent indictment of some Ukrainian nationals as a minor individual matter (BBC, 2024b). The disruption negatively impacted not only Russian exports but also European imports, leading to higher energy prices in the UK and the European Union (EU) (New York Times, 2022). Russia's share of pipeline gas dropped from over 40%–8%, while the US tripled its gas exports to Europe. As a result, the US became the continent's largest supplier of liquefied natural gas, fulfilling President Biden's goal to reduce European imports of Russian energy (European Council, 2024), albeit at a significantly higher cost for European consumers and industry.

Samsung Electronics provides an example of efforts to prevent the supply chain from being disrupted by competitors. The firm mitigates competitor risk by acquiring a significant stake in sole supplier companies, thereby securing a seat on their boards of directors. This prevents Apple or other competitors from gaining control of the supplier, which could disrupt Samsung's supply chain (Sodhi and Lee, 2007). The Biden (and later, Trump) administration's effort to “impede China's ability” to produce advanced chips and “ability to develop large language models” is another example of interdiction (FT, 2025). Related measures blocked Chinese companies, especially Huawei, from purchasing the latest chip-making equipment from the Dutch firm ASML or advanced chips from Nvidia. However, Nvidia sales restrictions were later eased after China threatened retaliation by withholding supplies of rare earth magnets (Reuters, 2025).

Military analysts use the term “interdiction” to describe delaying, disrupting, or destroying supply lines (Bingham, 1996), as a long-term warfare strategy (Chen and Evers, 2023). In this

context, management scholars define *supply chain interdiction* as “a strategy where an organization competes by taking supply-side actions to prevent rivals from acquiring, moving, or converting critical resources to gain a market advantage” (Bell *et al.*, 2015: p. 90).

This definition of supply chain interdiction as a preemptive strategy carried out by one organization against another to achieve a competitive edge is too narrow in two ways. *First*, it does not account for *counter-operations* aimed at disrupting covert or overt supply chains. Government agents may infiltrate a covert supply chain, maintain supply chain continuity for some time, and then interdict the movement of narcotics across international borders. We refer to this action as “infiltrate to interdict”. Government agencies may also employ surveillance techniques and informants to detect illegal activities and then interdict the offending supply chain by arresting key actors or seizing contraband—an action we term “detect to interdict”.

Second, a revised definition of supply chain interdiction should include both supply- and demand-side disruptions. Examples of supply-side interdiction include arrests of key individuals or seizures of illegal narcotics aimed at disrupting covert drug supply chains. Demand-side interdiction includes government agencies implementing public policy measures, such as awareness campaigns warning users that street drugs may be laced with fentanyl to reduce consumption (Tang and Choi, 2024). In July 2024, the White House issued a memorandum prioritizing the strategic disruption of fentanyl and synthetic opioid supply chains through a coordinated approach (Whitehouse.gov, 2024). We therefore suggest a more comprehensive definition of supply chain interdiction:

Supply chain interdiction is the intentional disruption, either covert or overt, of the movement of materials, products, information, people, or capital by targeting up- or downstream supply chain operations and/or personnel within a supply chain.

This definition includes actions by covert or overt actors, whether private groups or government agencies, aimed at disrupting either upstream or downstream operations of the supply chains of target companies, industries, or countries.

3. Observation and conceptualization

As a first step, we aimed to classify ten examples reported in the mainstream US and UK media (Table 1), some of which we have already discussed in earlier sections. For each example, we identified the operators and counter-operators. Based on the literature and our extended definitions, we also considered whether infiltration or interdiction was used by either party. Finally, we examined the nature of operations and counter-operations—whether covert or overt—drawing from the literature and the conceptual background from the previous section (Table 1).

Synthesizing these examples, we classified each into a 2×2 framework to categorize the nature of the supply chain operations and the counter-operations. The framework shows that counter-operations are conducted by covert or overt actors, ultimately aiming to disrupt material, products, services, or financial flows within overt or covert supply chains. Counter-operations include actions taken in response to or in opposition to supply chain activities. The intensity and duration of these counter-operations depend significantly on the intent and the strategy adopted (Figure 1).

In the four quadrants I–IV, we identify traditional supply chain operations in quadrant I, which could be disrupted by counter-operations from competitors or malicious actors (e.g. cybercriminals). Quadrant II involves covert supply chain activities, such as those involving illegal drugs or counterfeit goods, where legal authorities use overt (and legal) methods to disrupt them through counter-operations. In quadrant III, however, legal authorities or competitors may employ covert agents to infiltrate the supply chain, either for surveillance or with the goal of disruption. Lastly, in quadrant IV, competitors or legal authorities of one country secretly attempt to disrupt the supply chains of a company or those of another country.

Table 1. Examples of observations classified with our framework of operations and counter-operations

#	Observation/Year	Supply chain operators	Counter-operators	Counter-operation	Direct target//others affected indirectly	Nature of supply chain operations	Nature of counter-operations
1	US sanctions on Chinese companies from accessing equipment to produce semi-conductors, 2022	Chinese electronic chip manufacturers	US government	Interdiction	Chinese chip manufacturing//US and other consumers worldwide	Overt	Overt
2	US sanctions of Russian petroleum exports and trade in general, 2023 (ongoing)	Russian exporters of oil	US government	Interdiction	Russian government//Russian exporters of grain and fertilizer, negatively affecting developing countries in Asia and Africa	Overt	Overt
3	US DEA seizure of fentanyl being brought into the US, every year	Private operators in many countries (China, India, Mexico)	US Drug Enforcement Agency (DEA)	Detect to interdict, and Infiltrate to interdict	Private operators//beneficial for preventing fentanyl-related deaths in the US	Covert	Overt Covert
4	Exploding pagers and walkie-talkies in Lebanon, 2024	Israeli secret service agents	Israeli secret service agents	Infiltrate to interdict	Hezbollah fighters//Hezbollah social service workers for infrastructure, health-care facilities, schools, and youth programs	Covert	Covert
5	ANOM network for “secure” communication, 2018–2021	US FBI and the Australian Federal Police (AFP)	US FBI and the Australian Federal Police (AFP)	Infiltrate to Interdict	Criminal drug-running networks	Covert	Covert
6	Blowing up Russian gas pipelines to Europe, 2022	Gazprom (Russian state)	Ukraine, possibly US	Interdiction	Russian economy//UK and EU consumers affected by increased prices; massive impact on the environment	Overt	Covert
7	Ransom cyber-attack on Colonial Pipeline-US, 2021	Colonial pipeline	Russia-based hacker group, DarkSide	Interdiction	Pipeline users//US consumers and downstream companies	Overt	Covert

(continued)

Table 1. Continued

#	Observation/Year	Supply chain operators	Counter-operators	Counter-operation	Direct target//others affected indirectly	Nature of supply chain operations	Nature of counter-operations
8	Planting incendiary devices in message units at DHL centers, 2024	DHL	Russian operatives suspected	Interdiction	US//could cause devastation if successful on a commercial flight	Overt	Covert
9	Blowing up of Iranian centrifuges using a computer virus, 2010–2011	Iranian government	US and Israel joint operations	Interdiction	Iranian nuclear development//other countries using the targeted Siemens equipment (India, Mexico, others)	Overt	Covert
10	Severing internet cables in the Baltic Sea, 2024	Private companies operating these cables	Chinese or Russian ships suspected of anchor-dragging	Interdiction	Telecom users in Europe, particularly in Finland and Germany	Overt	Covert

Source(s): Authors' own creation

— Counter-operations — Covert Overt	IV. Interdict	III. Infiltrate to interdict
	6. Blowing up Russian gas pipelines to Europe, 2022 7. Ransom cyber-attack on Colonial Pipeline-US, 2021 8. Planting incendiary devices in massage units at DHL centers, 2024 9. Blowing up of Iranian centrifuges using a computer virus, 2010-2011 10. Severing internet cables in the Baltic Sea, 2024	3. US DEA seizures of fentanyl being brought into the US, every year 4. Exploding pagers and walkie-talkies in Lebanon, 2024 5. ANOM network for 'secure' communication, 2018–2021
	I - Interdict	II. Detect to interdict
	1. US sanctions on Chinese companies from accessing equipment to produce semi-conductors, 2022 2. US sanctions of Russian petroleum exports and trade, 2023 (ongoing)	3. US DEA seizure of fentanyl being brought into the US
	Overt	Covert
	— Supply chain operations —	

Figure 1. A framework for understanding the type of counter-operations for disruption based on the nature of the supply chain operations and the counter-operations. Infiltration and interdiction can also be cyber-operations. Source: Authors' own creation

The framework in [Figure 1](#) can serve as a starting point for developing a shared understanding of how companies' supply chain operations are vulnerable to infiltration and interdiction. When using this framework, it's helpful to remember that the same party may perform both operations and counter-operations, rather than different ones. For example, joint efforts by Australia, Europol, and the FBI led to the creation of the ANOM network, which infiltrated drug supply chains and also carried out counter-operations, resulting in the arrest of over 800 people worldwide to disrupt these supply chains ([BBC, 2021](#)). In other cases, counter-operations to interdict will necessarily be carried out by the opposing party, in line with interdiction strategies supported by military analysts.

[Table 1](#) also shows the direct target and indirect "collateral damage" in terms of its impact on others or the environment in the rightmost column, indicating potential for expanding the framework. Indeed, we demonstrate these nuances through the interaction between supply chain operations and counter-operations ([Figure 2](#)). [Figure 2](#) illustrates supply chains that have all operations as (A) covert or (C) overt, and also (B) where covert operations infiltrate overt supply chains. Supply chain operations of all three types can be disrupted anywhere in the supply chain by targeting the source, distribution, and demand itself. Harm can also be inflicted on others besides the target of covert supply chain operations or covert counter-operations, resulting in "collateral damage."

4. Avenues for future research

Our observations and evaluations, based on recent supply chain disruptions, suggest that extensive research is still needed to understand both covert and overt operations involving supply chain interdiction and infiltration within both legitimate and illegal supply chains. Most existing literature on covert supply chains and their operations is either theoretical ([Anzoom et al., 2021](#)) or depends on secondary data (for example, [Basu, 2014](#)). Researchers who gathered primary data through stakeholder interviews (e.g. [D'Amato and Papadimitriou, 2013](#); [Duensing et al., 2023](#)) have made valuable contributions, proposed well-informed strategies, and developed hypotheses for preventing illegal infiltration into legitimate supply chain activities.

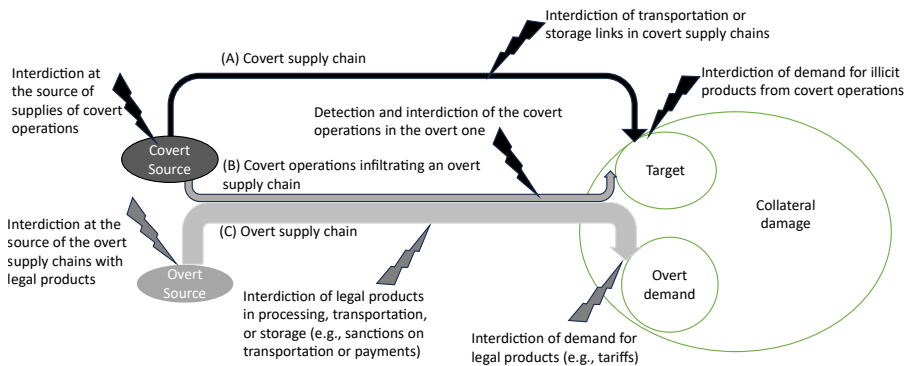


Figure 2. Covert operations in (a) independent covert supply chains and (b) having infiltrated (c) overt supply chains with legal operations and products; interdiction can occur at different points in overt and covert supply chains. Collateral damage can result from covert operations or the interdiction of such operations. Source: Authors' own creation

Although the existing scholarly work and our paper serve as a starting point, further empirical and conceptual research is needed to understand the infiltration and interdiction of supply chain operations and their impact on stakeholders. Our framework, illustrated in Figure 1 and further enhanced by Figure 2, prompts a range of questions that form a research agenda encompassing supply- and demand-side factors, government coordination mechanisms, intermediaries and technology, the motivations of various actors, and methodological approaches. These questions often span across the quadrants of Figure 1 and the relationships within Figure 2. Therefore, we propose a research agenda that examines the nature and dimensions of key concepts (“what and where”) regarding contextual and environmental conditions at locations within the supply chain, the actors (“who”), and the process or development aspects (“how”).

Table 2 provides a comprehensive overview of significant opportunities to deepen our understanding of covert supply chain operations and counter-operations.

4.1 What and where?

We hope that exploring questions of what and where in the future will enhance understanding of different aspects related to supply- and demand-side factors. Reducing consumer demand for illegal goods and strengthening regulatory frameworks are crucial for intercepting illegal supply chains, as is uncovering them through demand-side interdiction. Alternatively, decriminalizing the consumption and distribution of certain goods like drugs could potentially provide better oversight without the collateral damage of negatively affecting communities and individuals. On the supply side, we face a new era where any supply chain operation can be targeted or infiltrated by actors seeking to cause harm. Insights from managing overt supply chains could help guide efforts to disrupt covert ones through governance, visibility, and transparency.

We need to examine the “what” and “where” aspects of supply chain counter-operations. International business scholars have extensively discussed how tariffs and trade barriers can disrupt global trade flows (Beaumier and Cartwright, 2024; Miller, 2022). Global value chain (GVC) theory (Gereffi *et al.*, 2005; Phillips *et al.*, 2022; Roehrich *et al.*, 2025) plays a crucial role in identifying the coordination mechanisms within the supply chain, power asymmetries, and the development of governance structures. GVC theory demonstrates how policy tools (tariffs, trade agreements) and geopolitical tensions (trade wars) can disturb international trade. Global production networks (Coe *et al.*, 2008; Henderson *et al.*, 2002) also provide a

Table 2. A research agenda with potential research-guiding questions for supply chain operations and counter-operations

What and where?	Who?	How?
<p><i>Supply-side</i></p> <ul style="list-style-type: none"> • Are we entering a new era of supply chain threats whereby any supply chain can be weaponized to achieve certain goals? • How can we compare counter-operations for covert and overt supply chains? • Can technologies such as AI and blockchain be used to monitor overt supply chains for visibility into non-conforming or unusual activity that could suggest covert activity? <p><i>Demand-side</i></p> <ul style="list-style-type: none"> • What demand side factors contribute to disrupting and preventing the movement of contraband materials around the world? • What preventive approaches—including visibility and transparency—can supply chain participants use to interdict legitimate vs legitimate supply chain operations? • What approaches can be applied to secure supply chain operations on the demand side as well as the supply side? <p><i>Collateral damage</i></p> <ul style="list-style-type: none"> • Who else gets hurt besides the people targeted? • What is the impact on the environment in general as a result of the conflict? 	<ul style="list-style-type: none"> • How can governments collaborate to disrupt the movement of illicit materials across national boundaries? • What policy levers can governments use to entice international cooperation among private and public sectors in disrupting the movement of illicit items? • How can we encourage visibility and transparency through information sharing between government agencies (nationally and internationally) working to disrupt illegal trade flows? • What is the role of development of standard metrics and terminologies in improving global monitoring of supply chain operations? • What actions and relationships—including visibility and transparency efforts—exist across different levels of analysis (governments, supply chains, lead companies, suppliers, supply chain managers) to mitigate supply chain interdiction and protect supply chain flows? • How can government agencies coordinate and share information internally as well as with other governments, without revealing how they discover covert operations? 	<ul style="list-style-type: none"> • How do security measures have to evolve to address threats to international transportation modes, including air cargo, ocean freight, rail/road networks, and port operators? • How can technology (specifically blockchain, artificial intelligence, forensic science, and big data models) play a role in identifying, tracking, and disrupting the movement of illicit materials across global supply chains? • How can technology tampering prevention—zero trust, visibility, and transparency efforts—be completed on technology products as they move through the supply chain? • Can regulatory standards play a role in effective supply chain risk management for infiltration and interdiction? • Can we make covert supply chains overt by decriminalizing certain products to be able to control them overtly while reducing the inadvertent negative impact on communities and individuals?

Source(s): Authors' own creation

solid framework for analyzing supply chain interdiction and infiltration activities. Based on GVC analysis and actor-network theory, the global production network framework includes relevant actors in the production system (internal and external stakeholders). This perspective helps understand the intentions of actors within a supply network and explains why some actors are motivated to disrupt or infiltrate supply chain operations.

Within these contexts, questions also arise about the acceptance of overt or covert practices in the supply chain. Classifying and assessing covert and overt actions and responses will likely draw on institutional and legitimacy theory (e.g. [Busse et al., 2016](#)). Institutional logics and their dynamism may offer insights into these various interdiction and infiltration activities. These issues also connect to the stakeholders involved, and stakeholder theory can help deepen the understanding and guide responses.

4.2 Who?

Governments can disrupt the movement of illicit materials by promoting international cooperation, using policy incentives, and improving information sharing among relevant agencies. Coordinated efforts across governments, supply chains, and key stakeholders like companies and suppliers (at various levels) are essential for strengthening security, ensuring compliance, and protecting legitimate trade flows.

Examining the questions of “who” from a theoretical perspective, Actor-Network Theory (ANT) extends phenomenology by treating non-human actors (e.g. technology, documents, or policies) as equally important as human actors in shaping outcomes (Hald and Spring, 2023). Incidents in supply chains, for example, are viewed as the result of interactions within a network of actors. Material phenomenology examines how objects, tools, or non-human entities contribute to experiences and results (e.g. how a damaged product “experiences” its journey through the supply network). Systems phenomenology focuses on understanding the interconnectedness and emergent properties of systems (Iliopoulos, 2016). Coordination mechanisms and power relationships are involved in both the “who” and “how” sections. These perspectives can also be analyzed using the relational view (Dyer and Singh, 1998) and resource dependence theory (Pfeffer and Salancik, 1978). These theories have been extensively explored in traditional supply chain research (Handfield, 1993) and can be adapted to this environment. New theoretical insights are likely to emerge for existing theories within this non-traditional supply chain context.

4.3 How?

To address the “how” questions, as noted earlier, modern supply chains are complex and involve many intermediaries. These intermediaries can play a role in using technology to share information. Technology, such as the use of blockchain in supply-chain traceability and transparency (Babich and Tang, 2022), can be crucial in preventing physical infiltration of supply chains.

After conceptualization, the next step is to develop relevant measurement approaches and methodologies. Multiple theories and methods can be used to understand and evaluate supply chain interdiction and infiltration events, leading to the creation of theories, frameworks, and methodologies for effective supply chain interdiction and infiltration.

Data for theory-building and testing. Building and testing theories requires collecting empirical data on covert or illegal supply chain activities. However, gathering primary data is challenging because these activities are secretive and may be illegal. These supply chains are intentionally concealed, often decentralized, and involve actors actively trying to avoid detection, making direct observation or standard data collection methods nearly impossible. Additionally, ethical and legal restrictions limit researchers’ access to sensitive information, and the reliability of available data is often questionable due to its association with criminal or unregulated environments. Despite these obstacles, potential data sources include law enforcement records, court documents, investigative journalism, customs seizure reports, and declassified intelligence. Moreover, reports from NGOs and watchdog organizations—often based on field investigations or whistleblower disclosures—can provide valuable, though partial, insights into illegal supply chain activities. Insider accounts and corporate whistleblowers can also expose hidden practices. Furthermore, dark web scraping and blockchain transaction analysis are emerging methods for tracing illicit trade. While each source has limitations, combining data from multiple sources can provide essential insights into the structure and behavior of covert supply chains.

Methodology. Innovation in approach will likely be crucial, especially in covert supply chain operations. Such innovation could involve how researchers collect information from governments and businesses, sharing their analyses to protect supply chains without revealing insights to malicious actors. Military tactics, approaches, and methods used for interdiction and infiltration might offer valuable insights for examining various non-military supply

chains. Most cases of covert supply chain interdiction and infiltration are complex to evaluate empirically, but scholars should try to do so. Utilizing latent and observational methods could enhance understanding of supply chain interdiction and infiltration activities. Partnering with government counterintelligence agencies could also grant access to proprietary datasets for simulation models, allowing comparison of different interdiction strategies.

We could consider phenomenology, which methodologically emphasizes exploring and understanding lived experiences—especially with those affected, such as the destruction of entire community fabrics through the “war on drugs” (e.g. Reagan, 1990; Boyd, 2002). Although commonly used in fields like healthcare (Neubauer *et al.*, 2019), this approach could be expanded to supply chain research by examining the lived experiences of stakeholders—ranging from customers, including both intended and unintended victims, to manufacturers and suppliers, as shown in case studies (Towers *et al.*, 2020). Additionally, criminology also offers innovative methodological approaches to investigate covert and illegal phenomena in greater detail, including the use of legal documents and other archival data (Gadd *et al.*, 2011).

Another possible area of theory is that illegal actions can stem from criminological theories. An example is Routine Activity Theory (Miró, 2014), which states that a crime happens when three conditions are met: (1) a motivated offender; (2) a suitable target; and (3) a lack of a capable guardian, addressing the questions of who, what, and where. Additionally, drawing from sociology and criminology, Rational Choice Theory can be a useful perspective for analyzing illicit behavior (e.g. Gul, 2009; Carson *et al.*, 2020).

Another aspect to consider when studying supply chain interdiction and infiltration is the intersection of political science and global trade policy. Political scientists argue that supply chains can be weaponized to disrupt international trade, especially when governments control critical resources or the means of transforming resources into essential products (Farrell and Newman, 2022). For example, the US government has required American companies to block the sale of high-bandwidth memory chips and chipmaking tools to Chinese firms (Drezner, 2024; FT, 2025). Political scientists use concepts such as economic coercion and statecraft (related to institutional theory) to analyze how sanctions can prevent a major power from accessing advanced technologies. A game-theoretic approach can reveal the intentions of supply chain operators and intervention actors during interdiction and infiltration, as well as their responses to these actions. An example is modeling how governments could disrupt terrorist activities through subsidies (Shan and Zhuang, 2014).

Finally, when examining “how” from a theoretical standpoint, resource- or knowledge-based views and resource orchestration theory can be used to understand which resources within a supply chain are most vulnerable and to identify ways to detect and prevent counter-operations in the supply chain. These views can also determine who controls specific resources and how these resources can be managed in both open and covert supply chain activities.

5. Conclusion

The existing OSCM literature mainly focuses on producing and transporting “normal” goods through overt supply chains that follow the regulatory and legislative frameworks of the countries where the operations take place. These overt supply chains aim to either “maximize profit” in commercial activities or “maximize service” when providing public goods. In contrast, limited research has explored the structure of covert supply chains and the roles of governments and other stakeholders in combating such illegal activities. Notably, incidents like the “exploding pagers and walkie-talkies” have set concerning precedents that could encourage other covert actors. As geopolitical tensions rise, international agreements weaken, and malicious parties gain more resources and become more sophisticated, studying covert operations in supply chains will become even more essential.

Acknowledgments

This paper is an invited contribution that has undergone a thorough peer-review process. The discussion was started in September 2024 after the events of the pager and walkie-talkie explosion in Beirut, Lebanon. Based on a lively LinkedIn discussion started by Martin C. Schleper, this joint project was started and eventually resulted in this paper.

References

- Anzoom, R., Nagi, R. and Vogiatzis, C. (2021), "A review of research in illicit supply-chain networks and new directions to thwart them", *IISE Transactions*, Vol. 54 No. 2, pp. 134-158, doi: [10.1080/24725854.2021.1939466](https://doi.org/10.1080/24725854.2021.1939466).
- Autry, C.W. and Bobbitt, M.L. (2008), "Supply chain security orientation: conceptual development and a proposed framework", *International Journal of Logistics Management*, Vol. 19 No. 1, pp. 42-64, doi: [10.1108/09574090810872596](https://doi.org/10.1108/09574090810872596).
- Babich, V. and Tang, C.S. (2022), "How the U.S. can use technology to catch Chinese exporters trying to avoid tariffs", *Wall Street Journal*, No. 22 July 2022, available at: <https://www.wsj.com/articles/technology-catch-chinese-avoiding-tariffs-11658151476> (accessed 15 January 2025).
- Basu, G. (2013), "The role of transnational smuggling operations in illicit supply chains", *Journal of Transport Security*, Vol. 6 No. 4, pp. 315-328, doi: [10.1007/s12198-013-0118-y](https://doi.org/10.1007/s12198-013-0118-y).
- Basu, G. (2014), "Concealment, corruption, and evasion: a transaction cost and case analysis of illicit supply chain activity", *Journal of Transportation Security*, Vol. 7 No. 3, pp. 209-226, doi: [10.1007/s12198-014-0140-8](https://doi.org/10.1007/s12198-014-0140-8).
- BBC (2021), *ANOM: Hundreds Arrested in Massive Global Crime Sting Using Messaging App*, BBC, (8 June 2021), available at: <https://www.bbc.co.uk/news/world-57394831> (accessed 19 July 2025).
- BBC (2024a), *What We Know about the Hezbollah Device Explosions*, BBC, (20 September 2024), available at: <https://www.bbc.com/news/articles/cz04m913m49o> (accessed 17 January 2025).
- BBC (2024b), "German arrest warrant over Nord Stream blast mystery", 14 August 2024, available at: <https://www.bbc.co.uk/news/articles/cnvyz1472rpo> (accessed 11 February 2025).
- Beaumier, G. and Cartwright, M. (2024), "Cross-network weaponization in the semiconductor supply chain", *International Studies Quarterly*, Vol. 68 No. 1, sqae003, doi: [10.1093/isq/sqae003](https://doi.org/10.1093/isq/sqae003).
- Bell, J.E., Autry, C.W. and Griffis, S.E. (2015), "Supply chain interdiction as a competitive weapon", *Transportation Journal*, Vol. 54 No. 1, pp. 89-103, doi: [10.5325/transportationj.54.1.0089](https://doi.org/10.5325/transportationj.54.1.0089).
- Bingham, P.T. (1996), "Revolutionizing warfare through interdiction", *Airpower Journal*, pp. 1-6, available at: <https://apps.dtic.mil/sti/tr/pdf/ADA529681.pdf> (accessed 3 February 2025).
- Blome, C. and Schoenherr, T. (2011), "Supply chain risk management in financial crises—a multiple case-study approach", *International Journal of Production Economics*, Vol. 134 No. 1, pp. 43-57, doi: [10.1016/j.ijpe.2011.01.002](https://doi.org/10.1016/j.ijpe.2011.01.002).
- Boyd, G. (2002), "Collateral damage in the war on drugs", *Villanova Law Review*, Vol. 47, pp. 839-850.
- Busse, C., Kach, A.P. and Bode, C. (2016), "Sustainability and the false sense of legitimacy: how institutional distance augments risk in global supply chains", *Journal of Business Logistics*, Vol. 37 No. 4, pp. 312-328, doi: [10.1111/jbl.12143](https://doi.org/10.1111/jbl.12143).
- Carnovale, S., Carnovale, J., Strub, D., Szalwinski, A. and Marek, J. (2022), "Guardians of intellectual property in the 21st century: the global supply chain industry", *Rutgers Business Review*, Vol. 7 No. 1, pp. 1-21.
- Carson, J.V., Dugan, L. and Yang, S.M. (2020), "A comprehensive application of rational choice theory: how costs imposed by, and benefits derived from, the U.S. Federal Government affect incidents perpetrated by the radical eco-movement", *Journal of Quantitative Criminology*, Vol. 6 No. 3, pp. 701-724, doi: [10.1007/s10940-019-09427-8](https://doi.org/10.1007/s10940-019-09427-8).
- CBS News (2024), *Former Agents from Israel's Mossad Detail How They Built and Sold Explosive Pagers to Hezbollah Terrorists*, CBS News - 60 Minutes, (22 December 2024), available at:

- <https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript/> (accessed 17 January 2025).
- Chen, L.S. and Evers, M.M. (2023), “‘Wars without gun smoke’: global supply chains, power transitions, and economic statecraft”, *International Security*, Vol. 48 No. 2, pp. 164-204, doi: [10.1162/isec_a_00473](https://doi.org/10.1162/isec_a_00473).
- CISA.gov (2024), “U.S. and international partners publish cybersecurity advisory on People’s Republic of China State-sponsored hacking of U.S. Critical infrastructure | CISA. Feb 24th, 2024”, available at: <https://www.cisa.gov/news-events/news/us-and-international-partners-publish-cybersecurity-advisory-peoples-republic-china-state-sponsored> (accessed 24 April 2025).
- CNN (2024), “Israel’s Netanyahu acknowledges pager attack, says he sees ‘eye-to-eye’ with Trump on Iran”, *CNN*, (10 November 2024), available at: <https://edition.cnn.com/2024/11/10/middleeast/israel-netanyahu-pager-trump-intl-latam/index.html> (accessed 17 January 2025).
- Coe, N.M., Dicken, P. and Hess, M. (2008), “Global production networks: realizing the potential”, *Journal of Economic Geography*, Vol. 8 No. 3, pp. 271-295, doi: [10.1093/jeg/lbn002](https://doi.org/10.1093/jeg/lbn002).
- Davenport, S. and Leitch, S. (2005), “Circuits of power in practice: strategic ambiguity as delegation of authority”, *Organization Studies*, Vol. 26 No. 11, pp. 1603-1623, doi: [10.1177/0170840605054627](https://doi.org/10.1177/0170840605054627).
- DEA.gov (2020), “Fentanyl flow to the United States”, *DEA Intelligence Report*, available at: https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf (accessed 17 January 2025).
- Drezner, D.W. (2024), “Global economic sanctions”, *Annual Review of Political Science*, Vol. 27 No. 1, pp. 9-24, doi: [10.1146/annurev-polisci-041322-032240](https://doi.org/10.1146/annurev-polisci-041322-032240).
- Duensing, S., Schleper, M.C. and Busse, C. (2023), “Wildlife trafficking as a societal supply chain risk: removing the parasite without damaging the host?”, *Journal of Supply Chain Management*, Vol. 59 No. 2, pp. 3-32, doi: [10.1111/jscm.12297](https://doi.org/10.1111/jscm.12297).
- Duong, L., Sanderson, H., Phillips, W., Roehrich, J.R. and Uwalaka, V. (2025), “Creating agile and resilient supply chains: the supply of critical healthcare products in the face of geopolitical disruption”, *International Journal of Operations and Production Management*, Vol. 45 No. 5, pp. 1090-1118, doi: [10.1108/ijopm-03-2024-0243](https://doi.org/10.1108/ijopm-03-2024-0243).
- Dyer, J.H. and Singh, H. (1998), “The relational view: cooperative strategy and sources of interorganizational competitive advantage”, *Academy of Management Review*, Vol. 23 No. 4, pp. 660-679, doi: [10.2307/259056](https://doi.org/10.2307/259056).
- D’Amato, I. and Papadimitriou, T. (2013), “Legitimate vs illegitimate: the luxury supply chain and its doppelganger”, *International Journal of Retail and Distribution Management*, Vol. 41 Nos 11/12, pp. 986-1007, doi: [10.1108/IJRDM-01-2013-0015](https://doi.org/10.1108/IJRDM-01-2013-0015).
- D’Amato, I., Belvedere, V. and Papadimitriou, T. (2019), “Illegitimate trade in the fashion industry: relevance and counterstrategies in the Italian context”, *The Journal of Business and Industrial Marketing*, Vol. 34 No. 8, pp. 1654-1667, doi: [10.1108/JBIM-05-2018-0178](https://doi.org/10.1108/JBIM-05-2018-0178).
- El Baz, J., Evangelista, P., Jebli, F. and Sweeney, E. (2025), “Towards an understanding of illegal supply chain design in conflict areas: the case of the grain supply chain in Ukraine”, *International Journal of Operations and Production Management*, Vol. 45 No. 5, pp. 1148-1177, doi: [10.1108/IJOPM-03-2024-0264](https://doi.org/10.1108/IJOPM-03-2024-0264).
- Ellram, L.M. (1991), “Supply-chain management: the industrial organisation perspective”, *International Journal of Physical Distribution and Logistics Management*, Vol. 21 No. 1, pp. 13-22, doi: [10.1108/09600039110137082](https://doi.org/10.1108/09600039110137082).
- European Council (2024), “Where does the EU’s gas come from?”, *European Council*, (21 March 2024), available at: <https://www.consilium.europa.eu/en/infographics/eu-gas-supply/> (accessed 25 January 2025).
- Farrell, H. and Newman, A.L. (2022), “Weak links in finance and supply chains are easily weaponized”, *Nature*, Vol. 605 No. 7909, pp. 219-222.
- FT (2023), “The global network behind the fentanyl crisis”, *Financial Times*, (8 November 2023), available at: <https://ig.ft.com/fentanyl-crisis/> (accessed 17 January 2025).

- FT (2024), "From Taipei to Budapest: the mysterious trail of exploding pager", *Financial Times*, (18 September 2024), available at: <https://www.ft.com/content/72edfec6-a691-4969-a8e8-45781a227c71> (accessed 19 November 2024).
- FT (2025), "'We've impeded China': departing official defends US export controls", 20 January 2025. available at: <https://www.ft.com/content/8ba7df25-1d91-46f9-a1f7-6814343c7884> (accessed 11 February 2025).
- Gadd, D., Messner, S.F. and Karstedt, S. (2011), *The SAGE Handbook of Criminological Research Methods*, Sage, London.
- Gereffi, G., Humphrey, J. and Sturgeon, T. (2005), "The governance of global value chains", *Review of International Political Economy*, Vol. 12 No. 1, pp. 78-104, doi: [10.1080/09692290500049805](https://doi.org/10.1080/09692290500049805).
- Gul, S. (2009), "An evaluation of rational choice theory in criminology", *Sociology and Applied Science*, Vol. 4 No. 8, pp. 36-44.
- Hald, K.S. and Spring, M. (2023), "Actor-network theory: a novel approach to supply chain management theory development", *Journal of Supply Chain Management*, Vol. 59 No. 2, pp. 87-105, doi: [10.1111/jscm.12296](https://doi.org/10.1111/jscm.12296).
- Handfield, R. (1993), "A resource dependence perspective of just-in-time purchasing", *Journal of Operations Management*, Vol. 11 No. 4, pp. 289-311, doi: [10.1016/0272-6963\(93\)90005-A](https://doi.org/10.1016/0272-6963(93)90005-A).
- Handfield, R., Earp, J. and Sadeghi, A. (2025), "Reducing cybersecurity vulnerability in the supply base: insights from cyber experts", *Technology in Society*, Vol. 2, doi: [10.1016/j.techsoc.2025.102947](https://doi.org/10.1016/j.techsoc.2025.102947).
- Henderson, J., Dicken, P., Hess, M., Coe, N. and Yeung, H.W.C. (2002), "Global production networks and the analysis of economic development", *Review of International Political Economy*, Vol. 9 No. 3, pp. 436-464, doi: [10.1080/09692290210150842](https://doi.org/10.1080/09692290210150842).
- Iliopoulos, A.C. (2016), "Complex systems: phenomenology, modeling, analysis", *International Journal of Applied and Experimental Mathematics*, Vol. 1, p. 105, doi: [10.15344/2456-8155/2016/105](https://doi.org/10.15344/2456-8155/2016/105).
- Keskin, B.B., Griffin, E.C., Prell, J.O., Dilkina, B., Ferber, A., MacDonald, J., Hilend, R., Griffis, S. and Gore, M.L. (2023), "Quantitative investigation of wildlife trafficking supply chains: a review", *Omega*, Vol. 115, 102780.
- Marques, L., Erthal, A. and Crane, A. (2024a), "Impact pathways: follow the labour: the labour supply chain and its impact on decent work in product supply chains", *International Journal of Operations and Production Management*, Vol. 45 No. 7, pp. 1395-1401, doi: [10.1108/ijopm-06-2024-0470](https://doi.org/10.1108/ijopm-06-2024-0470).
- Marques, L., Morais, D. and Terra, A. (2024b), "More than meets the eye: misconduct and decoupling against blockchain for supply chain transparency", *Production and Operations Management*, Vol. 34 No. 5, pp. 1-19, doi: [10.1177/10591478231224928](https://doi.org/10.1177/10591478231224928).
- Marshall, D., McCarthy, L., McGrath, P. and Harrigan, F. (2016), "What is your strategy for supply chain disclosure", *MIT Sloan Management Review*, Vol. 57 No. 2, pp. 37-45.
- Meehan, J. and Pinnington, B.D. (2021), "Modern slavery in supply chains: insights through strategic ambiguity", *International Journal of Operations and Production Management*, Vol. 41 No. 2, pp. 77-101, doi: [10.1108/ijopm-05-2020-0292](https://doi.org/10.1108/ijopm-05-2020-0292).
- Melnyk, S.A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J.F. and Friday, D. (2022), "New challenges in supply chain management: cybersecurity across the supply chain", *International Journal of Production Research*, Vol. 60 No. 1, pp. 162-183, doi: [10.1080/00207543.2021.1984606](https://doi.org/10.1080/00207543.2021.1984606).
- Miller, C. (2022), *Chip War: the Fight for the World's Most Critical Technology*, Simon & Schuster, London.
- Miró, F. (2014), *Routine Activity Theory. The Encyclopedia of Theoretical Criminology*, Blackwell Publishing, Oxford, pp. 1-7.

- Mueller, M., dos Santos, V.G. and Seuring, S. (2009), "The contribution of environmental and social standards towards ensuring legitimacy in supply chain governance", *Journal of Business Ethics*, Vol. 89 No. 4, pp. 509-523, doi: [10.1007/s10551-008-0013-9](https://doi.org/10.1007/s10551-008-0013-9).
- Nath, S.D., Eweje, G. and Sajjad, A. (2020), "The hidden side of sub-supplier firms' sustainability – an empirical analysis", *International Journal of Operations and Production Management*, Vol. 40 No. 12, pp. 1771-1799, doi: [10.1108/ijopm-05-2019-0403](https://doi.org/10.1108/ijopm-05-2019-0403).
- Naylor, R.T. (2004), *Wages of Crime: Black Markets, Illegal Finance, and Underworld Economy*, Cornell University Press.
- NBC (2022), "Biden vows U.S. will 'bring an end' to Nord Stream 2 pipeline if Russia invades Ukraine", Feb. 7, 2022, available at: <https://www.nbcnews.com/politics/biden-meet-german-chancellor-russia-ukraine-tesnions-rcna15190> (accessed 11 February 2025).
- Neubauer, B.E., Witkop, C.T. and Varpio, L. (2019), "How phenomenology can help us learn from the experiences of others", *Perspectives on Medical Education*, Vol. 8 No. 2, pp. 90-97, doi: [10.1007/s40037-019-0509-2](https://doi.org/10.1007/s40037-019-0509-2).
- New York Times (2022), "'Act of sabotage' hits Europe's energy and stocks markets", *New York Times*, (28 September 2022), available at: <https://www.nytimes.com/2022/09/28/business/dealbook/sabotage-nordstream-europe-russia-gas-stocks.html> (accessed 25 January 2025).
- Pfeffer, J. and Salancik, G.R. (1978), *The External Control of Organizations: A Resource Dependence Perspective*, Harper & Row, New York.
- Phillips, W., Roehrich, J.K., Kapletia, D. and Alexander, E. (2022), "Global value chain reconfiguration and COVID-19: investigating the case for more resilient redistributed models of production", *California Management Review*, Vol. 64 No. 2, pp. 71-96, doi: [10.1177/00081256211068545](https://doi.org/10.1177/00081256211068545).
- Pullman, M., McCarthy, L. and Mena, C. (2024), "Breaking bad: how can supply chain management better address illegal supply chains?", *International Journal of Operations and Production Management*, Vol. 44 No. 1, pp. 298-314, doi: [10.1108/IJOPM-02-2023-0079](https://doi.org/10.1108/IJOPM-02-2023-0079).
- Reagan, B. (1990), "The war on drugs: a war against women", *Berkeley Women's Law Journal*, Vol. 6, pp. 203-214.
- Reuters (2022), "U.S. appeals court rejects GM racketeering suit against Fiat Chrysler August 11th, 2022", available at: <https://www.reuters.com/legal/us-appeals-court-rejects-gm-racketeering-suit-against-fiat-chrysler-2022-08-11/> (accessed 24 April 2025).
- Reuters (2025), "Nvidia's resumption of AI chips to China is part of rare earths talks, says US. 16 July, 2025", available at: <https://www.reuters.com/technology/nvidia-resume-h20-gpu-sales-china-2025-07-15/> (accessed 19 July 2025).
- Roehrich, J.K., Sarafan, M., Squire, B., Lawson, B. and Bouazzaoui, M. (2025), "Conflict and contract use in cross-cultural buyer-supplier relationships: the roles of cultural context", *Production and Operations Management*, Vol. 34 No. 5, pp. 974-992, doi: [10.1177/10591478241265481](https://doi.org/10.1177/10591478241265481).
- Roscoe, S., Aktas, E., Petersen, K.J., Skipworth, H.D., Handfield, R.B. and Habib, F. (2022), "Redesigning global supply chains during compounding geopolitical disruptions: the role of supply chain logics", *International Journal of Operations and Production Management*, Vol. 42 No. 9, pp. 1407-1434, doi: [10.1108/ijopm-12-2021-0777](https://doi.org/10.1108/ijopm-12-2021-0777).
- Sánchez-Pérez, M., Marín-Carrillo, M.B., Illescas-Manzano, M.D. and Souilim, Z. (2023), "Understanding the illegal drug supply chain structure: a value chain analysis of the supply of hashish to Europe", *Humanities and Social Sciences Communication*, Vol. 10 No. 1, p. 276, doi: [10.1057/s41599-023-01770-3](https://doi.org/10.1057/s41599-023-01770-3).
- Shan, X. and Zhuang, J. (2014), "Subsidizing to disrupt a terrorism supply chain—a four-player game", *Journal of the Operational Research Society*, Vol. 65 No. 7, pp. 1108-1119, doi: [10.1057/jors.2013.53](https://doi.org/10.1057/jors.2013.53).
- Sharp Blue (2025), "The rise of cargo pirates 2.0: cyber-hijacking of shipments in the digital age, Sharp Blue: 26 March", available at: <https://www.sharp-blue.com.au/the-rise-of-cargo-pirates-2-0-cyber-hijacking-of-shipments-in-the-digital-age/> (accessed 21 July 2025).

- Skilton, P.F. and Bernardes, E. (2022), "Normal misconduct in the prescription opioid supply chain", *Journal of Supply Chain Management*, Vol. 58 No. 4, pp. 6-29, doi: [10.1111/jscm.12286](https://doi.org/10.1111/jscm.12286).
- Smith, M. (2022), *The Real Special Relationship: the True Story of How the British and US Secret Services Work Together*, Simon & Schuster, London.
- Sodhi, M.S. (2016), "Natural disasters, the economy and population vulnerability as a vicious cycle with exogenous hazards", *Journal of Operations Management*, Vol. 45 No. 1, pp. 101-113, doi: [10.1016/j.jom.2016.05.010](https://doi.org/10.1016/j.jom.2016.05.010).
- Sodhi, M.S. and Lee, S. (2007), "An analysis of sources of risk in the consumer electronics industry", *Journal of the Operational Research Society*, Vol. 58 No. 11, pp. 1430-1439, doi: [10.1057/palgrave.jors.2602410](https://doi.org/10.1057/palgrave.jors.2602410).
- Sodhi, M.S. and Tang, C.S. (2014), "Guiding the next generation of doctoral students in operations management", *International Journal of Production Economics*, Vol. 150, pp. 28-36, doi: [10.1016/j.ijpe.2013.11.016](https://doi.org/10.1016/j.ijpe.2013.11.016).
- Sodhi, M.S. and Tang, C.S. (2019), "Research opportunities in supply chain transparency", *Production and Operations Management*, Vol. 28 No. 12, pp. 2946-2959, doi: [10.1111/poms.13115](https://doi.org/10.1111/poms.13115).
- South, N. and Wyatt, T. (2011), "Comparing illicit trades in wildlife and drugs: an exploratory study", *Deviant Behavior*, Vol. 32 No. 6, pp. 538-561, doi: [10.1080/01639625.2010.483162](https://doi.org/10.1080/01639625.2010.483162).
- Stevenson, M. and Busby, J. (2015), "An exploratory analysis of counterfeiting strategies: towards counterfeit-resilient supply chains", *International Journal of Operations and Production Management*, Vol. 35 No. 1, pp. 110-144, doi: [10.1108/ijopm-04-2012-0174](https://doi.org/10.1108/ijopm-04-2012-0174).
- Still, W. (2019), *The Underground Railroad Records: Narrating the Hardships, Hair-Breadth Escapes, and Death Struggles of the Slaves in Their Efforts for Freedom*, Penguin Randomhouse LLC, New York.
- Tang, C.S. (2006), "Perspectives in supply chain risk management", *International Journal of Production Economics*, Vol. 103 No. 2, pp. 451-488, doi: [10.1016/j.ijpe.2005.12.006](https://doi.org/10.1016/j.ijpe.2005.12.006).
- Tang, C.S. and Choi, T. (2024), "To combat the fentanyl crisis, the US should further target the supply chain", *Chicago Tribune*, 9 January 2024, available at: <https://www.chicagotribune.com/2024/01/09/christopher-tang-and-thomas-choi-to-combat-the-fentanyl-crisis-the-us-should-further-target-the-supply-chain/> (accessed 17 January 2025).
- The Atlantic (2023), "The most consequential act of sabotage in modern times", *The Atlantic*, (13 December 2023), available at: <https://www.theatlantic.com/international/archive/2023/12/nord-stream-pipeline-attack-theories-suspects-investigation/676320/> (accessed 18 December 2024).
- The Independent (2022), "Malaysia seizes African tusks, pangolin scales worth \$18M", *The Independent*, (18 July 2022), available at: <https://www.independent.co.uk/news/african-ap-malaysia-asia-b2125530.html> (accessed 3 February 2025).
- Towers, N., Abushaikha, I., Ritchie, J. and Holter, A. (2020), "The impact of phenomenological methodology development in supply chain management research", *Supply Chain Management: An International Journal*, Vol. 25 No. 4, pp. 443-456.
- TRAFFIC (2020), "Countering wildlife trafficking through Kenya's seaports: workshop proceedings", available at: <https://www.traffic.org/site/assets/files/12732/kenyas-ports-proceedings-web-final.pdf> (accessed 3 February 2025).
- Trott, P. and Hoecht, A. (2007), "Product counterfeiting, non-consensual acquisition of technology and new product development: an innovation perspective", *European Journal of Innovation Management*, Vol. 10 No. 1, pp. 126-143, doi: [10.1108/14601060710720582](https://doi.org/10.1108/14601060710720582).
- Wang, Y., Lin, J. and Choi, T.M. (2020), "Gray market and counterfeiting in supply chains: a review of the operations literature and implications to luxury industries", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 133, 101823, doi: [10.1016/j.tre.2019.101823](https://doi.org/10.1016/j.tre.2019.101823).
- Whitehouse.gov (2024), "Memorandum on prioritizing the strategic disruption of the supply chain for illicit fentanyl and synthetic opioids through a coordinated, whole-of-government, information-driven effort", Whitehouse.gov, (31 July 2024), available at: <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/07/31/memorandum-on-prioritizing-the-strategic->

[disruption-of-the-supply-chain-for-illicit-fentanyl-and-synthetic-opioids-through-a-coordinated-whole-of-government-information-driven-effort/](#) (accessed 3 February 2025).

- WSJ (2024), “Russia is accused of terrorism in alleged incendiary device plot”, *The Wall Street Journal*, (5 November 2024), available at: <https://www.wsj.com/world/europe/russia-is-accused-of-terrorism-in-alleged-incendiary-device-plot-e90ab67b?msoclid=28bd52b6a53c672e37304734a485664f> (accessed 3 February 2025).
- Zsidisin, G.A. (2024), “Defining covert supply chains”, available at: <https://ssrn.com/abstract=4855774> (accessed 25 January 2025).

Further reading

- FT (2019), “WhatsApp voice calls used to inject Israeli spyware on phones”, *Financial Times*, (13 May 2019), available at: <https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab> (accessed 26 January 2025).
- New York Times (2019), “The secret history of the push to strike Iran”, *New York Times*, (4 September 2019, updated 23 May 2021), available at: <https://www.nytimes.com/2019/09/04/magazine/iran-strike-israel-america.html> (accessed 3 February 2025).
- Reuters (2024), “Chamber of Commerce sees new US export crackdown on China, email says”, 22 November, available at: <https://www.reuters.com/technology/chamber-commerce-sees-new-us-export-crackdown-china-email-says-2024-11-22/> (accessed 17 January 2025).
- State.gov (2023), *United States Sanctions Additional Sinaloa Cartel Network of Fentanyl Suppliers*, State.gov, (9 March 2023), available at: <https://www.state.gov/united-states-sanctions-additional-sinaloa-cartel-network-of-fentanyl-suppliers/> (accessed 20 November 2024).
- Washington Post (2012), “Stuxnet was work of U.S. and Israeli experts, officials say”, *Washington Post* (2 June 2012), available at: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAInEy6U_story.html (accessed 3 February 2025).

Corresponding author

Samuel Roscoe can be contacted at: s.roscoe@ubc.ca