Organised criminal groups’ use of corruption and physical threats against customs officials

Various customs administrations have reported that their officials are physically threatened by organised criminal groups to abuse their power and facilitate illicit activities, such as drug trafficking. This Helpdesk Answer conceptually analyses how organised criminal groups use corruption and physical threats to influence customs officials and enable their profit-making activities, before describing how applying certain integrity measures could potentially prevent and counter the emergence of such threats.
Query

Which integrity measures can customs institutions take to increase their resilience to organised criminal groups’ use of corruption and physical threats?

Contents

1. Introduction
2. A conceptual understanding of physical threat, corruption and organised crime
   a. The interplay between corruption and physical threat
   b. Organised criminal groups’ use of corruption and physical threats
3. Organised criminal groups’ use of corruption and physical threats against customs officials
   a. Organised criminal groups’ interests in the customs sector
   b. Organised criminal groups’ corruption of customs officials
   c. Organised criminal groups’ use of physical threats against customs officials
4. Exploring the potential of integrity measures to address organised criminal groups’ use of corruption and physical threats against customs officials
   a. Scoping interventions
   b. Assessing risks
   c. Public integrity measures
   d. Holistic approach
5. References

MAIN POINTS

— There is general agreement within the literature that organised criminal groups use corruption and physical threat as tactics to enable their profit-making activities, but less agreement on what makes them select one tactic over the other given the influence of many contextual variables.

— Both of these tactics are used against customs officials to facilitate their profit-making activities. While their use of physical threat has been comparatively less studied, it presents serious risks to the integrity of customs administrations.

— Customs administrations are best placed to take internally orientated measures to prevent and respond to the infiltration of organised criminal groups and the emergence of physical threats.

— Enhanced integrity measures have the potential to make a positive contribution in this regard. These measures include safe and secure whistleblowing mechanisms, lifestyle checks, staff rotation policies and integrity training of officials.
Caveat

This Helpdesk Answer is based on desk research and as such relies on literature published by others. No primary research was undertaken.

The paper attempts to shed light on a problem faced by customs administrations that has been, so far, relatively understudied. In some cases, this paper relies on a degree of inference when, for example, exploring possible applications of findings from one field to another.

Introduction

According to Chapter 2 of the Revised Kyoto Convention, “customs” means the Government Service which is responsible for the administration of Customs law and the collection of duties and taxes and which also has the responsibility for the application of other laws and regulations relating to the importation, exportation, movement or storage of goods (WCO 2006).

Corruption affects the work of customs administrations in several ways and can obstruct their ability to fulfil their organisational mandate and objectives. Estimates suggest that 30% or more of customs revenues, generated through trade taxes, are lost to corruption (World Bank no date).

Corruption can be perpetrated by different actors in this sector. Customs officials themselves can be a source of corruption given that they often enjoy discretionary powers over important decisions. Cases have been reported in which customs officials have extorted traders, for example, threatening them with spurious fees or tariffs (World Bank no date).

In addition to this insider threat, integrity issues can arise as a result of organised criminal groups (OCGs) trying to influence customs officials to facilitate their illicit activities. These activities might include, for example, the smuggling of drugs and weapons or other illegal goods (World Bank no date).

OCGs employ different tactics in this regard. They may develop corrupt relations with customs officials and bribe them to allow illegal goods to be smuggled across borders (World Bank no date).

While it is not a noted issue at every border, there have also been reports of customs officials being threatened with physical violence by OCGs to allow them to conduct their illicit activities unimpeded.1 When faced with physical threat, targeting themselves or their family members, customs officials may have no choice but to comply with the demands of criminal groups. This can inadvertently facilitate corruption by providing OCGs with the entry point to exert greater influence over customs officials and their operations.

Protecting customs officials from such threats of violence from OCGs is a complex issue, which requires comprehensive and coordinated responses from different agencies. For example, national (and international) law enforcement agencies are in general primarily responsible for investigating OCGs and responding to threats of violence when they arise. At the same time, there

---

1 Such incidents have been reported by some members of the World Customs Organisation (WCO).
are a number of internal integrity measures that customs administrations can take to reduce the exposure of their staff to threats from criminal groups.

The first section of this Helpdesk Answer addresses the relationship between physical threat and corruption as practiced by OCGs. It then draws on literature and open media sources to explore to what extent these threats are present in the customs sector.

Based on the findings, the third section summarises and analyses the potential of public sector integrity measures to prevent and respond to corruption and physical threats faced by customs officials. These integrity measures can be implemented internally by customs administrations and include safe and secure reporting and whistleblowing mechanisms, staff rotation policies, training of customs officials, and ethical leadership.

A conceptual understanding of physical threat, corruption and organised crime

The interplay between corruption and physical threat

This paper interprets physical threat as the intent - whether stated or implied - to inflict bodily harm. The relationship between physical threat and corruption is a complex one. Indeed, conceptually, it is not clear whether abuses of power committed by officials to comply with demands backed by physical threats can be considered to be acts of corruption. Corruption is defined as “the abuse of entrusted power for private gain” (Transparency International no date). If we consider a scenario in which an individual abuses their entrusted power in response to being physically threatened, it would be problematic to say they have done so “for private gain” in the traditional understanding of these words.

The United Nations Convention against Corruption (UNCAC) does not address if the presence of physical threat affects whether or not a corruption offence has been committed. However, the US Department of Justice (2020) has produced a resource guide on the Foreign Corrupt Practices Act (FCPA), which states:

“situations involving extortion or duress will not give rise to FCPA liability because a payment made in response to true extortionate demands under imminent threat of physical harm cannot be said to have been made with corrupt intent or for the purpose of obtaining or retaining business.”

This guidance is noteworthy on two points. First the reference to threat of physical harm suggests the scope of the duress defence covers only physical coercion as opposed to other forms of coercion. Secondly, it points to a common recognition that the threat of physical harm negates the “private gain” element within the definition of corruption. In criminal jurisprudence, the defence of duress is normally available to anyone who is accused of having committed a crime (The Law Dictionary, No Date). Successfully raising the defence of duress amounts to demonstrating that the accused party lacked the intent to commit the crime due to the presence of coercion, physical or otherwise.

In this sense, if a public official such as a customs official abuses their power in response to being physically threatened – for example, accepting a bribe to ensure narcotics are not controlled at the border – that customs official may be able to
successfully defend themselves against prosecution for acts of corruption by arguing they acted under duress.

Nevertheless, this would not change the fact that the bribe has been accepted and the illicit activity facilitated, causing similar damaging effects on the operations of border control and wider society that a case of bona fide corruption would have.

This creates a somewhat complex situation in which the behaviour or actions of the individual customs agent may not qualify as corruption, but such behaviour or actions contribute to an increase in the aggregate level of corruption within that official’s institution. As an example, in an organisation where it is perceived that others are engaging in corrupt behaviour or misconduct (even if it is not legally considered corruption as it has been caused by duress), this behaviour may be normalised across the group. Indeed, a common rationalisation for corruption is that people perceive that “everyone else is doing it”, so therefore engage in corrupt behaviour or misconduct (even if it is not legally considered corruption as it has been caused by duress), this behaviour may be normalised across the group.

On this basis, this paper addresses reported physical threats made against custom officials that may have similar outcomes to corruption and lead to an increase of aggregate corruption in the sector. Nonetheless, the author acknowledges that, in many jurisdictions, officials confronted with physical threats may not be considered to be guilty of corrupt offences.

Organised criminal groups’ use of corruption and physical threat

Despite the growing international recognition of the challenges posed by organised crime and its main perpetrators – organised criminal groups – as exemplified by the 2000 adoption of the United Nations Convention Against Transnational Organised Crime, there is no universally-accepted definition of OCGs. Scholars normally attempt to distinguish organised crime from other forms of criminal behaviour through focusing on OCGs’ modus operandi. Albanese (2021: 431) describes how academic definitions of organised crime often coalesce around similar elements:

- Planned, rational acts committed by groups of individuals
- The crimes committed often respond to public demand for illicit goods and services
- The objective of the crimes is financial or material gain
- Corruption and intimidation are used to protect ongoing criminal enterprises

Reed (2009:11) argues that OCGs use corruption and intimidation as “enabling activities” to facilitate other profit-making activities. Similarly, Hauck and Peterke (2010) list corruption and the threat of violence as OCGs’ primary enabling activities. They are not necessarily the only enabling activities OCGs rely on, but considering others in detail is beyond the scope of this paper. In this vein, the paper focuses on how OCGs use corruption and physical threat as “tactics” in response to different needs and environments. These
dynamics are explored in greater detail in the rest of this section.

The forms of corruption OCGs engage in can be varied. Europol (2021: 27) identified bribery, influence peddling, nepotism and abuse of authority as the main forms criminal groups availed of within the EU. Similarly, violent acts OCGs deploy can include “threats, intimidation, vandalism and assaults, to kidnapping, torture, mutilation and murder” (2021: 21).

OCGs are diverse in their nature, and not all of these groups have been recorded using corruption and physical threats. Europol (2021) carried out a serious and organised crime threat assessment based on data provided in response to over 4,000 questionnaires by European Union (EU) member states and partners. The assessment found that almost 60% of the criminal groups identified engaged in corruption and that also 60% of them used violence to some extent (2021: 19).

Despite challenges that necessarily arise in directly studying OCGs, the literature has attempted to shed light on the conditions under which an OCG will choose to employ one tactic over another. Bailey and Taylor (2009: 11) describe how OCGs rely on three tactics in their interactions with the state: evasion, corruption and confrontation. In the most basic scenario, an organised criminal group intending to conduct illicit business will first try to avoid state detection (evasion); when this is impossible, they may attempt to co-opt state actors (corruption); and finally, they may seek to intimidate state actors (confrontation), although this is the least employed tactic due to its costs and difficulty to execute. According to this model, once evasion fails and the illicit activities of an OCG cannot escape detection, the preference is corruption rather than physical threat.

This kind of model—one depicting a progression-like structure in which OCGs substitute one tactic for another under certain conditions—points to an initial conclusion that OCGs are more likely to resort to confrontation when their use of corruption is restricted. Gillies (2023) warns that interventions that seek to dismantle corrupt structures may inadvertently serve to heighten the risk of state actors facing violence.

Nevertheless, this model is not without its limitations. OCGs do not always make use of physical threat and corruption for the same purpose. For example, Europol (2021) stated that violence may be used by a group to strengthen their reputation in the criminal environment. This means the reasons why an organised criminal group resorts to threatening violence may have nothing to do with whether their use of corruption was restricted or not. Rather, different tactics in this case are used for different objectives.

Reed (2009) highlights that there is a strong variation between countries in how and why OCGs use corruption. Buscaglia and van Dijk (2003: 23) list five levels of infiltration of the public sector by OCGs, ranging from sporadic acts of bribery at low levels of government agencies to capture of the state’s policies. While the broader aim might be to enable profit-

---

2 Bailey and Taylor (2009: 11) give the following examples of such costs: “(1) external costs such as greater public awareness of the organised criminal groups’ existence and activities, higher levels of government repression, and public repudiation; and (2) internal costs, such as members’ defection, declining business, and risks to members’ personal security.”
making activities, as OCGs move between these levels, their intermediate aims can be varied.

Similarly, there are a wide range of contextual variables determining the conditions under which OCGs employ physical threat. There is a strong variation in the structures and sizes of OCGs; Kotzé et al. (2022) found that violence is used more readily by smaller organised criminal group in comparison to larger, established ones. Some scholars also treat the illicit commodity being trafficked by the OCGs as a significant determinant of violence – for example, when a high demand for a commodity develops (Kenny et al. 2020). However, Williams (2009: 324) found that the type of commodity is not as significant a determining factor for the level of violence as the political, social and cultural context in which the OCG operates, especially whether there are serious capacity gaps and legitimacy deficits across state institutions.

Lastly, it is not always possible to disentangle corruption and physical threat as isolated tactics occurring in separate stages of a progressive escalation. For example, in the situation where an OCG approaches a public official with a proposal to engage in corruption, the official, knowing how OCGs operate, may still perceive a physical threat even when it has not been expressed. Gounev and Bezlov (2010:78) found this is the case at the local level in Portugal where “corrupt exchanges ‘offered’ by organised criminals to politicians are accompanied by an implicit degree of intimidation which determines the outcome of the proposal made”.

Indeed, Fukumi (2005:90) describes how for the Medellín cartel in Colombia during the 1980s, corruption and intimidation were used in tandem against public officials, essentially becoming “two sides of the same coin”.

Smith et al. (2018: 3) found that one of the ways OCGs interacted with Australian public servants was through “threats of violence intended to intimidate those who have been corrupted”. This suggests the existence of a process where corruption originally unaccompanied by physical threat then transformed to a situation where corrupt behaviour is maintained by physical threat.

Williams (2009: 329) concludes that “although it is tempting to see corruption and violence as alternative strategies of criminal organisations – the infamous choice between silver and lead – in [Mexico and Iraq] corruption and violence are mutually reinforcing”. In these two countries, Williams demonstrates how OCGs pursue simultaneous strategies of confrontation and collusion with the state rather than having one strategy to replace the other.

Similarly, Morris (2012) in his analysis of drug trafficking gangs’ use of corruption in Mexico found that, while corruption may have once contributed to lower levels of drug-related violence in the past, corruption takes shifting patterns and may have also played a role in fuelling the drug-related violence in the 2000s; for example, the corruption of law enforcement and judiciary actors may have led to greater impunity for OCGs, thus lowering the potential costs they face in using violence (Morris 2012: 33).

In conclusion, the literature paints a complex picture on OCGs’ use of physical threat and corruption. It emerges that, depending on a range of contextual variables, these tactics may be used in some scenarios as substitutes for each other, while they can be mutually reinforcing in others. This finding has important implications not only for determining how OCGs use these tactics against customs officials but also as an important consideration when designing any
measures to address physical threat and corruption respectively.

Organised criminal groups’ use of corruption and physical threats against customs officials

Organised criminal groups’ interests in the customs sector

Having established some of the contextual variables that may lead to physical threat or corruption being used as tactics by OCGs, this section will explore the unique attributes of the customs sector to consider how OCGs deploy these tactics specifically against customs officials.

Buscaglia and van Dijk (2003:11) describe key role and vulnerability of customs institutions to OCGs:

“Customs bureaux are responsible for allowing for access of goods and services into a country and play a key role in preventing both trafficking in persons and drugs and smuggling of goods and services in general. As a result, customs are well worth being ‘captured’ by organised crime.”

Therefore, OCGs have an interest in influencing customs officials to secure profits from crimes that have a cross-border element. This exposes customs officials to organised crime to a greater degree than many other public servants (Fjeldstad and Raballand 2020:123)

There are different ways that customs officials can facilitate greater profits for OCGs. Customs officials may participate directly in smuggling or help OCGs avoid the detection of illicit goods. OCGs may rely on corrupt custom officials to mis-declare or undervalue their shipments of licit goods through legitimate import/export companies (Chêne 2008: 2). According to Europol (2023: 4), OCGs coordinate networks of corrupt actors at the ports (including port workers, freight agents and customs) to gain key intelligence on logistical processes to avoid detection.

Furthermore, OCGs ultimately strive to secure arrangements at border crossings that they can rely on for their illicit activities (UNODC no date). This means they are not pressing for short-term abuses of powers, but rather a sustainable relationship with customs officials so that the abuse of power occurs for a prolonged period.3

Indeed, due to the magnitude of the profits available, a compromised customs administration that fails to prevent illicit activities from taking place will by default indirectly contribute to the sustained growth of the OCG via the latter’s accumulation of resources.

3 Experts consulted when drafting this paper suggested that OCGs may have a preference for using corruption as a tactic to influence customs officials, because using violence generates additional business risks and may trigger law enforcement crackdowns, thus undermining such a sustainable relationship.
Organised criminal groups’ corruption of customs officials

As outlined in the previous section, OCGs rely on corrupting customs officials as a tactic to fulfil their interests. However, there are also contextual factors specific to the customs sector at play, which affect not only the propensity of OCGs to use corruption but also how likely customs officials are to engage in corruption.

Velkova and Georgievski (2004: 284) carried out a cross-case analysis of corruption among customs officials across south-eastern European countries, and found the factors that made the officials susceptible to corruption included their low salaries, ineffective penal policies, poor human resource management systems and the low level of supervision of their activities.

Additional reasons cited by the World Customs Organisation (2021:14) for why customs officials are targeted for corruption include the monopoly power they have over customs functions, as well as the fact that clearance of many goods is time sensitive, creating additional incentives to circumvent customs procedures.

One might infer that lower-ranking officials working onsite at border control are OCGs’ main target for corruption, but corruption in the customs sector occurs across the hierarchy. Dormaels and Walle (2011) carried out a study interviewing 707 customs officials in Belgium, finding that both high and low-level customs officials did not report significantly different rates of being approached to engage in corrupt acts. This is typically the case where the scale and scope of criminal activities become more complex and high-level facilitation becomes necessary (US AID, 2019). For example, an Organized Crime and Corruption Reporting Project (OCCRP, 2019) investigation detailed how an individual used bribes to infiltrate a large network of high and low-level Kyrgyz customs officials to launder up to US$700 million out of Kyrgyzstan on behalf of a locally powerful family.

Therefore, one can infer that the customs sector is not only particularly susceptible to corruption, but also to OCGs’ use of corruption. Jancsics (2019:4) introduces a standalone concept of “border corruption”, defined as an “illegal exchange of different resources between two or more actors – border official(s) (bribe taker) and client(s) (bribe giver) – who may be individuals, firms, or organised crime groups”. Since one of the primary duties of customs is to prevent the cross-border movement of illegal goods, which can be a highly profitable activity, Jancsics finds that “border corruption, more than any other form of corruption, can be linked directly to the activities of crime syndicates”.

Jancsics provides a typology of border corruption, with the overarching categories of “collusive corruption” and “coercive corruption”. Whereas collusion broadly refers to cases where both actors on each side of the corrupt transaction are equal players who benefit, coercion is a dependency-based unequal social relationship. This includes cases where an informal group such as an OCG coerces customs officials to facilitate illegal activity. The forms of coercion which Jancsics elaborates on in this regard are organised criminal group’s exploitation of a customs officials’ alcohol or drug abuse or blackmail following exposed infidelities (2019: 9).

Jancsics’ typology places a strong emphasis on the role of social norms and local networks in driving border corruption. In a later publication, the author (2020: 220) describes how social bonds and a level of trust between the customs
official and the organised criminal group have often already been established before corruption occurs. Under this interpretation, infiltration help create the space for corruption.

Jancsics elaborates that customs work, especially at remote locations, demonstrates strong group features, in which employees’ work, residence and leisure often overlap, meaning tight local networks can form within and outside the workplace (2020: 218-19). Customs officials may also come under pressure to engage in corruption from within informal traditional systems, such as family members relying on them for financial sustenance (Fjeldstad and Raballand 2020:123).

Influence may also come from local political networks. The Global Initiative Against Transnational Crime (2019:11) quotes a police official who claimed that custom officials routinely receive orders and rewards from their superiors to turn off the cameras at a border crossing between Albania and North Macedonia to allow trucks to pass through unobstructed; the spoils of this activity are then reportedly shared between local OCGs and political parties.

This touches on an important point; OCGs can use intermediaries to corrupt customs officials. Meaning, customs officials may not be approached directly by members of OCGs, but rather by third parties; for example, police officers who themselves have been corrupted by OCGs.

It can be inferred from the important role of networks and social norms that corruption can easily become entrenched within the customs sector, and with that, customs officials’ interaction with OCGs becomes more frequent.

Organised criminal groups’ use of physical threats against customs officials

Compared to the use of corruption, there is a general lack of literature on OCGs’ use of physical threats against customs officials. The topic has not been studied systematically and much of the evidence available is anecdotal and outdated in nature.

Korsell et al. (2007) carried out a study measuring to what extent public officials working in the regulatory and law enforcement sector in Sweden face forms of what they call “unlawful influence”, an umbrella term of serious forms of influence and pressure that includes corruption and physical threat. They received 4,538 responses to a questionnaire from public officials, including 938 customs officials, and they analytically compare the experience of different occupational groups.

For example, 13.4 % of responding customs officials reported having been exposed to harassment, threats and/or violence, in comparison to 14.8 % of prosecutors and 12.2 % of police officials, but only 3.2 % of tax auditors. They highlighted that the forms of violent threats faced by the actors vary; for example, police officials meet all kinds of people in their work who might physically threaten them, but that in “contrast to other occupational groups, customs officials are to a high degree confronted by organised crime, mostly in connection with drug trafficking”. They explain that customs officials can be exposed to violence by OCGs who become more desperate in their exercise of unlawful influence (2007: 352).

Several of the customs officials responding to the questionnaire revealed that they are exposed to a
form of “subtle harassment” which does not amount to full violence but nevertheless can have the effect of paralysing the official and institution; in spite of this, the officials reported the support they received from their employer against this harassment as insufficient (2007: 354). While they do not define this term “subtle harassment”, it is reminiscent of the insight gained in the previous section that not all physical threats are enunciated, and that corruption and physical threat cannot be easily disentangled.

In 2020, Reportedly cited one Governor Waheed Qatali from Heart Province, Afghanistan who claimed that customs officials working in the border town of Islam Qala were being physically threatened by drug cartels with weapons such as knives, rifles and rocket launchers, coercing them to sign illegal documents to facilitate smuggling and the evasion of excise duties. The Special Inspector General for Afghanistan Reconstruction (2014:3) described reports that Afghan customs officials were being intimidated and, in some cases, kidnapped by criminal and patronage networks in retaliation for collecting customs duties.

Incidents do not always remain at the threat level and customs official may be violently attacked and in extreme cases murdered. In 2003, Trinidad and Tobago News reported how a customs official was shot and killed by unknown perpetrators in what police believed was a retribution attack for his refusal to bow to the “demands of several unscrupulous persons”. Similarly, in 2020, a customs official in Antigua and Barbuda was kidnapped and murdered by unknown perpetrators; the official had been investigating a customs fraud case involving up to US$3.3 million (Dominica News Online: 2020). In 2022, after customs officials operating in Kwara State, Nigeria seized their goods (parboiled rice and fuel), a smuggling ring laid in ambush, killing one official and injuring three others (Daily Trust 2022)

Case study: Baja California, Mexico

Baja California is a Mexican state in the northwest of the country that shares a border with Arizona and California in the United States. There is a high rate of customs activity around this border area, centred in the urban areas of Tijuana, Tecate and Mexicali.

Rival drug cartels have a strong presence in Baja California, notably the Sinaloa, Arellano-Félix and the New Generation Jalisco cartels, who engage in violent clashes one another.

These cartels try to influence customs officials primarily to facilitate the smuggling of narcotics into the US but they are also suspected of being involved in human trafficking, and the smuggling of huachicol, an adulterated alcoholic drink. Infobae (2020) reports that low-ranking customs officials in Baja California are routinely threatened by OCGs or have taken bribes from them.

These threats also reach high-ranking customs officials. In October 2020, Mexican maritime customs took part in an operation to confiscate 28kgs of precursor chemicals used to manufacture fentanyl and methamphetamine from a ship arriving from Japan at Ensenada port; police believed the chemicals were being trafficked by the Sinaloa cartel. Shortly after the operation, a cloth or a so-called “narcomanta” was discovered at the port with an intimidating message directed at the administrator of maritime customs in Ensenada.

In 2021, widespread corruption was identified by the financial intelligence unit (FIU) within the Baja California customs administration, in addition to other state-level customs administrations. The institution was suspected of facilitating several corrupt practices, including
fraud to avoid excise duties on the export and import of cars; in some cases, this was reportedly done in collusion with organised criminal groups. The FIU filed criminal complaints against several high-ranking customs administrators, who were removed from their posts.

It is not possible to clearly identify links between all the developments described above, but these examples point to OCGs using both corruption and physical threats against customs operations in Baja California.

Sources: San Diego Union Tribunal 2023; Animal Político 2021; Infobae 2020; Border Hub 2021.

Analysing these cases, possible overlaps with OCGs’ use of corruption emerge. As with corruption, OCGs deploy physical threats against both high and low-ranking customs officials. The role of remote locations and local networks appears to be significant in both. These may be especially important in determining the use of physical threat because they can be linked to the lack of a sufficient law enforcement response to violence.

There are also apparent idiosyncrasies. While OCGs use corruption primarily towards the facilitation of illicit activities, there may be additional reasons to use physical threat or violence such as retaliation against uncooperative officials. While physical threat seems to succeed as a tactic in pressuring customs officials to facilitate these activities, it is less clear if it helps OCGs to infiltrate customs sectors to the extent that corruption does.

Finally, these cases suggest that OCGs rely on a mixture of tactics over the same period of time rather than one over another. Nevertheless, this does not exclude that violence can be used as a “substitute” for corruption, in cases when customs officials carry out their duties and interrupt the illicit activities or, it seems, also when they themselves attempt to address corruption within the sector.

Exploring the potential of integrity measures to address organised criminal groups’ use of corruption and physical threats against customs officials

Scoping interventions

One of the main reasons for the attention given in previous sections to understanding the conditions under which OCGs use corruption and physical threats against customs officials was to provide a conceptual framework for understanding which interventions can be effective.

First, there are a number of contextual variables determining how and why OCGs use corruption and physical threat. Each of these contextual variables could be explored in much further detail than this paper allows, but they paint a complex picture of when and how OCGs elect to rely on physical threat and corruption, meaning that a one-size fits all approach is unsuitable.

Second, there are factors unique to the customs sector which heighten the risk of both corruption and physical threat. These factors broadly pertain to the nature of customs officials’ work, their proximity to OCGs, and to prevailing social norms. Interventions should consider these factors in order to be effective.
The interventions addressing physical threat can be divided into two categories. Preventive measures aim to stop physical threats from emerging in the first place. In contrast, reactive interventions consist of measures that respond to a manifested threat of violence and thus are primarily aimed at securing the safety of the threatened individual and, in some cases, holding the organised criminal group accountable.

In terms of preventive measures, customs administrations can seek to establish internal policies that can reduce the emergence of the physical threats, with a focus on managing interaction with external parties and targeting potential vectors of OCG infiltration. This may entail minimising instances in which OCGs (and their intermediaries) come into contact with customs officials, and thus prevent OCGs from seizing opportunities to influence the behaviour of officials through the use of corruption and physical threats. One could also describe this as a process of making customs administrations more “resilient” at the institutional level to these threats.

Reactive measures such as physical protection programmes typically fall within the mandate of law enforcement agencies. Unless the relevant law enforcement powers have been delegated to them, customs administrations acting on their own may be limited in their ability to react to physical threats that have emerged. Yet there are certain integrity measures customs administrations can take to protect their staff after the emergence of a threat, such as establishing robust whistleblowing mechanisms.

For these reasons, and in line with the expertise of the Anti-Corruption Helpdesk, this section focuses primarily on those preventive and reactive measures that can be taken by customs administrations themselves.

**Assessing risks**

Assessing risks is an important step to take before planning and implementing any policy intervention.

In the first section, a model was considered that presents physical threat as a substitute tactic used by OCGs when their use of corruption is restricted. This model was shown to be limited in many respects, with other voices within the literature pointing to the face that both tactics are used in tandem by OCGs or as supplementary to each other.

Nevertheless, it not possible to dismiss the possibility that under certain circumstances, OCGs may consider corruption and physical threats as substitute tactics. If so, this can present a serious risk: interventions that target corruption in the customs sector and make it more difficult for OCGs to corrupt customs officials to serve their interests may inadvertently lead OCGs to deploy the substitute tactic of physical threat.

On the other hand, it was found in previous sections that corruption rather than physical threat is typically an OCG’s first means of infiltrating an institution. This infiltration creates more points of contact between members of organised criminal groups and public sector officials. It was described how corruption can become entrenched in the customs sector, implying that, in the long run, there will be a greater likelihood of situations arising that OCGs would respond to with physical threat or violence. In addition, corruption within the customs sector could hinder the effectiveness of
measures intended to address and deter physical threat. Therefore, passively allowing corruption to occur in this instance would amount to failing to prevent the emergence of physical threat.

While targeting corruption in the customs sector is a necessary action to reduce the risk of physical threat in the long term, it must be carried out in a way that does not bring unacceptable risks to customs officials in the short term.

This touches on an important debate within the anti-corruption field – namely, sequencing. For example, there is a discussion about whether anti-corruption interventions can be effective in fragile contexts where a certain threshold of security and criminal justice standards has not been met (GIZ 2020: 27). In such a case, it could make more sense to prioritise security and criminal justice reforms, before embarking on anti-corruption interventions. There is no one-size-fits-all approach for sequencing, but it is important to have a clear understanding of the local context (Fagan 2011).

Considering all of this, an initial step for customs administrations developing measures to build resilience against the influence of OCGs could be to undertake a robust risk assessment of the environment in which those measures will be implemented.

The most relevant tool in this case could be the organised crime threat assessment, which aims to “gather relevant data and present it in a systematic way to determine current and future trends in organised criminal activity” (Shaw 2011: 1). These assessments can be carried out at the transnational, national or local level and work best when gathering insights from a wide range of stakeholders, especially law enforcement and intelligence actors.

Conducting such an exercise before interventions are implemented could help customs administrations measure and mitigate risks associated with OGCs, including their potential use of violence. It can also create a better understanding of the place of these interventions within a sequence of other necessary interventions.

Public integrity measures

The preventive measures that customs administrations can take are largely internal in nature, meaning, they are geared towards their own employees rather than clients such as businesses involved in cross-border trade. These measures should build resilience at both the individual and institutional levels. To meet these criteria, this Answer explores measures which are grouped under the rubric of “public integrity”. It is informed by the Organisation for Economic Co-operation and Development’s (2020) definition of public integrity as the “the consistent alignment of, and adherence to, shared ethical values, principles and norms for upholding and prioritising the public interest over private interests in the public sector.”

The public integrity approach offers advantages for the purposes of this paper. First, public integrity requires public sector institutions to go beyond the aim of negating corruption to actually developing a positive set of attitudes and values across the organisation (WCO 2021: 13). This means it also targets behaviour that can lead to the development of contact with OCGs, although it might not constitute corruption.

Public integrity has already been applied to the customs sector. The World Customs Organisation has embraced integrity
programming and its member states adopted the Revised Arusha Declaration in 2003, which declared that effective national customs integrity programmes must address ten core considerations. The WCO maintains a periodically revised integrity development guide, which acts as a “comprehensive tool that addresses all aspects of an integrity development initiative undertaken by Customs administrations” (WCO 2021: 10). The OECD (2016) has also emphasised the centrality of an integrity approach to customs agencies to prevent the facilitation of illicit trade and smuggling.

It should be emphasised it appears from a review of the literature that no research has to date been undertaken on the application of public integrity measures to preventing physical threat. Therefore, this section relies on a degree of inference to interpret how such measures could be effective against physical threat.

**Safe and secure whistleblowing mechanisms**

Whistleblowing is defined as the disclosure of information about suspected wrongdoing to individuals or entities believed to be able to effect action (Terracol 2022). Internal whistleblowing systems are operated by organisations to facilitate disclosures about wrongdoing within their organisation.

It is not difficult to imagine how promoting whistleblowing can prevent the emergence of physical threats. The risks of interaction with OCGs can be flagged and employees can be encouraged to disclose any suspected cases of officials having been corrupted by OCGs. This can also be done at the point of interaction where corruption has not yet materialised. An advantage of this measure is that due to the local nature of their work, customs officials may have prior knowledge of who could be members of OCGs or their intermediaries. Therefore, an effective reporting system can provide some of the data necessary to operate an early warning system for the emergence of physical threats.

Employees can be encouraged to disclose risks and breaches, but they can also be mandated to do so. For example, the Australian Customs and Border Protection Service (ACBPS) makes it a legal requirement for all employees to report serious misconduct, including corrupt conduct and criminal behaviour, to its Integrity and Professional Standards Branch (Grant 2013: 128). Furthermore, there are indications that complicit employees may be encouraged to self-report their misconduct where their employing organisation promises to respond with leniency (Lambsdorff and Nell 2007).

Regardless, it is necessary to create an environment that enables whistleblowing. Part of this is ensuring procedures are clear and easy to follow (OECD 2015). Organisations such as customs administration should make information about their internal whistleblowing systems highly visible and accessible via a wide range of channels (Terracol 2022: 12).

Individuals who disclose breaches may face additional risks once they have made a

---

4 The ten key factors are: leadership and commitment; regulatory framework; transparency; automation; reform and modernisation; audit and investigation; code of conduct; human resource management; morale and organisational culture; relationship with the private sector.
disclosure. This includes not only retaliation from the employer or co-worker but where they report a matter implicating OCGs, it may increase their vulnerability to physical threats and violence (Maslen 2023: 3).

The most important protective measure to overcome these risks is to ensure that confidentiality is guaranteed. There are different ways of doing this, including making use of open-source software solutions and removing any personal identifying information in reports made through physical complaint boxes and hotlines (Maslen 2023: 15). If the whistleblower’s identity and any third party is mentioned in the report, access to that information should be strictly controlled (Terracol 2022: 26).

In the event that it is not possible to entirely protect the identity of the employee, further protections may need to be in place. In some jurisdictions, whistleblowers are entitled to protective measures such as enhanced security actions, such as regular patrolling and installation of security devices and electronic warning devices (Maslen 2023: 16). Additionally, if a case goes to court, the official may be eligible for witness protection. (Maslen 2023: 14). While witness protection may not come under the mandate of the customs administration, responsible staff can be aware of these protective measures and which external agencies to contact if the threat escalates.

Employees should be able to rely on a systematic and professional follow up of reports by qualified and internal control units. It is possible that high-level customs officials are involved with OCGs. In such a situation, the customs administration’s ability to respond to the report will be compromised (OECD 2016:52-3). The responsibility for operating the internal whistleblowing system should be given to an impartial person or department that is independent and free from conflict of interest and is accorded adequate resources and powers (Terracol 2022: 11).

This can increase the trust customs officials have in the whistleblowing mechanism and assuage their fears about facing any fallout after reporting. Indeed, the customs administration should take proactive measures to protect any persons reporting suspected wrongdoing with the reasonable belief that the information reported was true at the time of reporting – as well as third parties at risk of detrimental conduct (Terracol 2022: 17).

Lifestyle checks

France (2021: 2) defines a lifestyle check, also sometimes called lifestyle audit, as “an accountability tool that measures a person’s lifestyle – property and assets owned, spending habits, and way of living.”

Lifestyle checks could be used by employers to uncover cases of illicit enrichment within their workforce as well as to identify behaviour which threatens the integrity of the institution.

This can be carried out already at the recruitment phase through employee-vetting procedures or security checks; for example, many customs administrations check candidates’ police records (OECD 2016: 55). The OECD recommends that customs officials are subject to comprehensive and ongoing security checks including “reinvestigations in employees background, behavioural checks, psychometric checks, management checks, elaboration of risk profiles and random auditing; particularly for positions that are highly vulnerable to corruption and other integrity risks” (2016: 62). Such checks
can help identify members of OCGs or individuals with personal connections to them that have or are aspiring to join the customs workforce.

In the previous sections, it was found that lifestyle factors and local relationships can increase customs officials' vulnerability to being targeted by OCGs. Therefore, lifestyle checks can uncover any potentially compromising relationships an employee or candidate may have.

For example, Jancsics (2019) identifies substance abuse as a lifestyle factor that can be exploited to establish “dependency-based unequal social relations” between a customs official and an OCG. The official becomes inherently vulnerable to the influence of OCGs and exposed to their tactics, including the possible use of physical threat. If a lifestyle check identifies that a customs official engages in substance abuse, the customs administration can explore taking steps to mitigate the risks this poses. For example, Australian Customs and Border Protection Service (ACBPS) introduced a mandatory drug and alcohol testing programme for customs officials (Grant 2013: 129).

Furthermore, customs administrations can carry out social media monitoring to check for suspicious behaviour relating to corruption (Smith et al. 2018: 94). Such measures may also support identifying any existing personal connections between employees or candidates and OCGs and their intermediaries.

Lastly, many public sector agencies mandate their employees to comply with so-called financial auditing measures such as submitting declarations of assets, interests and income (France 2021: 5). If unexplained wealth is identified in an employee’s account, the employee will have to justify its legitimate origins. Therefore, proactive financial auditing measures can identify and prevent OCGs from bribing officials as a means of infiltrating the customs sector.

Concerns are often raised about the compatibility of lifestyle checks with privacy rights (France 2021: 2). Therefore, it is critical that this measure is carried out in full respect of the local law and in accordance with the powers accorded to the customs administration.

**Monitoring and control**

The OECD (2013) recommends that public sector organisations operate an effective integrity risk management and control system to safeguard integrity. Similarly, the Revised Arusha Declaration recognises that the “prevention and control of corruption in customs can be assisted by the implementation of a range of appropriate monitoring and control mechanisms such as internal check programmes, internal and external auditing and investigation and prosecution regimes.”

It was established in the previous section that a lack of supervision facilitates corruption and interactions between OCGs and officials, especially when customs officials work at remote land borders and have a high degree of discretion to make decisions (Jancsics 2019: 10).

Therefore, monitoring and control mechanisms may be used to prevent the emergence of physical threat by addressing this unique character of customs work. There are several good practices to draw on in this respect. France, Belgium and Slovenia highlighted the use of mobile units that carry out unannounced inspections of customs officials at work as an effective measure (Gounev and Bezlov 2010: 3).
Access to information such as inspection schedules should be restricted to the minimum number of staff responsible for spot checks and inspections. Good practice suggests that inspections should be carried out in teams, rather than by individual inspectors. Indeed, in several countries, including Estonia, the so-called four eyes system makes it compulsory for at least two officials to be present during key customs work processes (Velkova and Georgievski 2004: 287). In the Philippines, customs officials are obliged to wear body cameras and record events during all regular operations (Kusumawardhani and Diokno 2022: 139). Customs officials may also be prohibited from using private mobile phones while on duty (Jancsics 2021: 223). Such measures do not rely on a centralised monitoring entity and therefore can be well-suited to support the detection of any organised crime risks, while at the same time deterring customs officials from interacting with OCGs.

Relevant literature recommends that monitoring and control measures be accompanied by effective systems to respond to any risks that are flagged. WCO recommends that administrations set up internal control units to collect and analyse risks from different sources (2021: 44). Furthermore, customs administrations should have a designated office that leads internal investigations where necessary; however, the OECD (2016: 48) recommends appointing an external, independent third party to conduct the investigations when the misconduct involves high-ranking officials.

Potential limitations of this measure include that it is more focused on detecting risks present onsite during working times, whereas interactions between OCGs and customs officials may originate and mature outside of working life (Jancsics 2019).

### Staff rotation

Gounev and Bezlov (2010: 102) differentiate between three kinds of staff rotation policies in the customs sector. Customs officials may be periodically transferred to other locations within a country to carry out customs work. Second, their work shifts may be rotated frequently and randomly with other officials. Finally, there can be randomised schedules so that which customs official inspects which object (for example, a shipment) is not predetermined.

All of these, at varying levels, aim to disrupt the regular patterns that can facilitate corruption. For example, rotation of staff across locations can help address the risk of customs officials falling under the influence of local networks. If an official has been compromised, the disruption of their regular work shift may make it more difficult for them to facilitate smuggling. As established in the previous section, OCGs aim to develop sustainable relationships with customs officials, which depends in part on the customs officials being based in a specific geographical area.

Rotation can also be used to protect people from physical threat by relocating an individual away from the source of the threat (Maslen 2023: 17). While recognising OCGs can have a wide geographical reach, if the relocation is strategically considered, it may be possible to reduce the risk.

There are certain limitations to this measure. For example, in Czech Republic, it was found to be ineffective because of the geographical proximity between the various locations of customs offices in that country (Velkova and Georgievski 2004: 287). Furthermore, Jancsics (2019: 11) notes that preexisting social arrangements and networks can persist across different locations.
Training

According to Resimić (2022: 1), the aim of integrity training for public officials is “to raise awareness about integrity standards and corruption prevention in the public sector.” The OECD recommends that integrity training is provided on an ongoing basis to customs officials (OECD 2016: 54). For example, the Dutch Tax and Customs Administration, carries out introductory and ongoing integrity training for staff and appoints integrity counsellors who offer guidance on integrity standards (Van Blijswijk et al 2004: 723).

Training can touch on a wide range of topics pertaining to integrity. The OECD recommends that the integrity training curriculum is specialised and tailored to the needs of the job (OECD 2016: 54). For customs officials then, training could have an important role in raising awareness of the threats posed by organised crime. It is likely that not all staff are aware of how OCGs infiltrate the customs sector and, indeed, the chain of events that can lead to the emergence of physical threat.

Training can also address behaviour that may make officials more easily identifiable and vulnerable. For example, it has been found that OCGs increasingly rely on information made available via social media to identify potential public sector officials to approach, either with illicit inducements or physical threats (Smith et al. 2018: 88). Therefore, a tailored training on responsible social media use could act as an important mitigating factor. Trainings can also familiarise officials with polices that may help to conceal their identities, such as an organisational policy on officials’ use of social media, or protocols such as not wearing uniforms off duty or disclosing work details with external actors. Such policies can be set out in the customs administration’s code of conduct.

Existing evidence suggests that the most effective training combines theory and practical case examples (Resimić 2022: 2). In Belgium, roleplaying featured in the training of customs officials, including how to properly communicate in vulnerable situations as well as using neutralisation techniques (Dormaels and Walle 2011: 37). It may be beneficial to explore the potential of using training to simulate interactions between customs officials and organised criminal groups, so that officials have an enhanced understanding of the risks and threats, as well as to learn about appropriate ways to react.

There are no obvious limitations to a well-executed training. However, a common obstacle is having sufficient resources in place to hold comprehensive and regular integrity trainings (Resimić 2022: 3).

Ethical leadership

One of the key steps in mainstreaming integrity across an institution is ensuring that people in leadership roles at different organisational levels act ethically. People look to authority figures for social cues, meaning that authority figures are in an opportune position to influence behaviour (Jenkins 2022: 11). For example, leaders can set the message that corruption is no longer tolerated (Fjeldstad and Raballand 2020:128). Leadership is furthermore a key element in designing and effectively implementing strategies to this effect (OECD 2016: 17).

OCGs use corruption and physical threat as tactics against both high and low-ranking customs officials. Therefore, if leaders set an example of non-tolerance of unsanctioned contact with external actors, there could be a trickle-down effect to lower ranking customs officials. Furthermore, in light of the study by
Korsell et al. (2007), which revealed that public sector employees facing subtle forms of harassment often did not feel that their employer acknowledged this, there should be processes in place to ensure that employees’ concerns are escalated to leadership and dealt with appropriately.

However, the influence of ethical leadership on the part of top-level officials can be limited. As OECD (2020) states, public sector leaders tend to head large organisations that are distributed across different locations, leading to communication challenges. This is especially the case for the customs sector. Therefore, it is important to apply a broad understanding of the leadership concept and underline the role of middle managers.

**Automation**

Customs automation can broadly be understood as the application of information and communication technologies for accomplishing the mission of customs (UNECE 2012). There has been a turn towards automating key customs processes in recent years as an anti-corruption measure (Fjeldstad and Rogaland 2020:129), as recognised under the Revised Arusha Declaration. Crucially, automation can reduce the high level of discretion customs officials are typically accorded to carry out their duties.

For example, between 2004 and 2019 the Afghan customs administration led a process to computerise customs clearance operations to increase efficiency and reduce opportunities for corruption. Despite capacity and security constraints, the administration recorded increased revenue collection from customs clearance. (Fjeldstad and Raballand 2020:140).

Additionally, numerous countries make use of a single automated system to collect customs fees to prevent customs officials from soliciting bribes before the clearance phase (OECD 2016: 34).

Automation can not only reduce the emergence of physical threats by targeting corruption, it also uniquely has the potential to prevent physical threat or potential violence from occurring at all. This is because the automation of certain customs process can minimise face-to-face interactions between the officials and members of OCGs. This could be especially effective in remote and unsupervised locations where officials are more vulnerable to OCGs.

There are limitations to automation. It should be emphasised that not all customs processes can be automated: for example, cargo examination (OECD 2016: 31). Secondly, automated systems can be vulnerable to forms of external manipulation (WCO 2021: 38). There is a further risk of an OCG attempting to corrupt the customs officials who have access to an automated system to use it for their own advantage.

**Holistic approach**

The integrity measures outlined above are internal measures that customs administrations can adopt of their own accord. However, the intended effect of such measures may be limited if carried out in isolation from each other and from wider anti-corruption interventions (Jenkins 2022: 1).

The impact of integrity measures may also be limited without complementary measures from other sectors. Fjeldstad and Raballand (2020:132) argue that integrity in customs requires a whole-of-government approach with “the commitment of other external control...”
authorities (such as the police, prosecutors and judicial power)”.

Considering their central role in implementing reactive measures, an adequate law enforcement response is essential. Indeed, to mitigate against any risk of violence, law enforcement should have the capacity to protect people targeted by OCGs, including through witness protection schemes, and cooperate duly with customs administrations in this regard.

This holistic approach can be taken even further. The WCO (2021: 30) calls for engagement with the private sector and society as a whole to address integrity risks in customs. An example of this approach in action is the reported plans of the Dutch government to address the violence posed by OCGs who have infiltrated Rotterdam port to smuggle drugs. Among other measures, the government aims to offer alternative pathways to vulnerable young people who may turn to a life of crime (Boztas, 2022).
References


Albanese, J.S. 2021. Organized crime as financial crime: The nature of organized crime as reflected in prosecutions and research. Victims & Offenders, 16(3)


Border Hub. 2021. Denuncian penalmente a aduanales de Tamaulipas y Baja California


Campbell, W and Chee Hing, K. 2003. Businessman held for Customs official’s murder Trinidad and Tobago News


Chêne, M. 2013. Literature review on corruption at ports and border points in Southern Africa.


Organised criminal groups’ use of corruption and physical threats against customs officials


Gillies, A. 2023. Narco-political corruption: Damaging democracy while reducing violence?

Global Organized Crime Index. No date. Mexico.


Global Initiative on Transnational Organized Crime. 2019. Hotspots of organized crime in the Western Balkans: Local vulnerabilities in a regional context


Jenkins, M. 2022. The effectiveness of integrity led anti-corruption interventions.


The Law Dictionary. No Date. What is duress?


OCCRP. 2019. Plunder And Patronage In The Heart Of Central Asia.


Resimić, Miloš. 2022. Integrity training for public officials.


Special Inspector General for Afghanistan Reconstruction. 2014. Afghan customs: US programs have had some successes, but challenges will limit customs revenue as a sustainable source of income for Afghanistan (SIGAR 14-47 Audit Report).


Transparency International. ND. What is corruption?

UNODC. No date. Causes of private sector corruption.

UNODC. No date. Links between organised crime and corruption.

UNODC. 2002. Results of a pilot survey of forty selected OCGs in sixteen countries.


World Bank. No date. Customs Administrations

World Customs Organisation. 2006. The Revised Kyoto Convention.

DISCLAIMER
All views in this text are the author(s)’ and may differ from the U4 partner agencies’ policies.

PARTNER AGENCIES
GIZ/BMZ (Germany), Global Affairs Canada, Ministry for Foreign Affairs of Finland, Danida (Denmark), Sida (Sweden), SDC (Switzerland), Norad (Norway), UK Aid/FCDO.

ABOUT U4
The U4 anti-corruption helpdesk is a free research service exclusively for staff from U4 partner agencies. This service is a collaboration between U4 and Transparency International (TI) in Berlin, Germany. Researchers at TI run the helpdesk.

The U4 Anti-Corruption Resource Centre shares research and evidence to help international development actors get sustainable results. The centre is part of Chr. Michelsen Institute (CMI) in Bergen, Norway – a research institute on global development and human rights.

www.U4.no
U4@cmi.no

KEYWORDS
Customs – integrity – organised crime – security

OPEN ACCESS
We apply a Creative Commons licence to our publications: CC BY-NC-ND 4.0.