Romsom, Etienne

Working Paper

Countering global oil theft: Responses and solutions

WIDER Working Paper, No. 2022/35

Provided in Cooperation with:
United Nations University (UNU), World Institute for Development Economics Research (WIDER)

Suggested Citation: Romsom, Etienne (2022) : Countering global oil theft: Responses and solutions, WIDER Working Paper, No. 2022/35, ISBN 978-92-9267-166-2, The United Nations University World Institute for Development Economics Research (UNU-WIDER), Helsinki, https://doi.org/10.35188/UNU-WIDER/2022/166-2

This Version is available at:
https://hdl.handle.net/10419/259391

WIDER Working Paper 2022/35

Countering global oil theft: responses and solutions

Etienne Romsom*

March 2022

United Nations University World Institute for Development Economics Research

wider.unu.edu

Abstract: This second of two papers on global oil theft discusses ways to reduce oil theft, misappropriation, and fraud. At US$133 billion per year, oil is the largest stolen natural resource globally, while fuel is the most smuggled natural resource. Oil theft equates to 5–7 per cent of the global market for crude oil and petroleum fuels. It is so engrained in the energy supply chain that thefts are priced in by traders and tolerated by many shipping companies as petty theft. Oil theft and related insecurity have substantial negative economic effects on developing countries, whether they produce oil or not. In 2012, non-oil-producing Benin saw a 28 per cent drop in taxable income after a spate of oil tanker hijacking incidents in the Gulf of Guinea in 2011. In Nigeria, the oil capacity shut-in and amount of oil deferred is more than twice the amount estimated as stolen, with a US$20 billion annual loss in petroleum profit tax—63 per cent of total government tax revenue in 2019. Organized oil crime syndicates are often transnational and conduct theft and fraud professionally, exploiting gaps in jurisdiction and adapting their practices when law enforcement becomes more effective. They evolve from ship piracy to stealing tanker cargoes to kidnapping tanker crews; from physical ransom of assets to digital hijacking via ransomware. The proceeds of oil theft often finance other organized crime, and it triggers violence against the community and in crime-on-crime activities. Twelve commonalities in oil theft and fraud have been identified that can direct international solutions, in three target areas: stolen oil volumes, stolen oil transport, and stolen oil money. Prosecution for acts of bribery offers opportunities for action: transport of or payment for illegal oil could constitute a bribe under the US Foreign Corrupt Practice Act if government officials were involved in the transaction or shipment. Bribe charges could be raised for paid 'services' that facilitate oil theft (through action or non-action).

Key words: oil, fuel, theft, corruption, transnational crime, tax evasion and avoidance, piracy, digital ransomware

JEL classification: H2, K42, Q3, Q5

Acknowledgements: The author would like to thank Tony Addison, Alan Roe, and Kathryn McPhail for reading and commenting on an earlier version of this paper.

Related publication:

Romsom, E. (2022). 'Global Oil Theft: Impact and Policy Responses'. UNU-WIDER Working Paper 2022/16. Helsinki: UNU-WIDER. https://doi.org/10.35188/UNU-WIDER/2022/147-1

* EnergyCC, Singapore, er@energycc.com

This study has been prepared within the UNU-WIDER project Extractives for development (E4D)—risks and opportunities, part of the Domestic Revenue Mobilization programme, which is financed by the Norwegian Agency for Development Cooperation (Norad).

Information and requests: publications@wider.unu.edu

ISSN 1798-7237 ISBN 978-92-9267-166-2

https://doi.org/10.35188/UNU-WIDER/2022/166-2

Typescript prepared by Luke Finley.

United Nations University World Institute for Development Economics Research provides economic analysis and policy advice with the aim of promoting sustainable and equitable development. The Institute began operations in 1985 in Helsinki, Finland, as the first research and training centre of the United Nations University. Today it is a unique blend of think tank, research institute, and UN agency—providing a range of services from policy advice to governments as well as freely available original research.

The Institute is funded through income from an endowment fund with additional contributions to its work programme from Finland, Sweden, and the United Kingdom as well as earmarked contributions for specific projects from a variety of donors.

Katajanokanlaituri 6 B, 00160 Helsinki, Finland

1 Introduction

This working paper is the second of two addressing global oil theft and fraud. The first paper primarily explored the impact of oil theft in terms of domestic resource utilization, transnational economic impact, regional insecurity, community impact, and interlinkages with other organized crime (Romsom 2022). This second paper focuses on recent oil theft trends and enforcement successes, as well as commonalities in oil theft and how these can direct countermeasures and solutions.

The paper focuses on criminal oil theft as a commercial activity. The following definitions have been adopted:

- Oil theft is theft of crude oil or oil that has been refined into fuel.
- Crude theft is theft of unrefined crude oil.
- Fuel theft is theft of oil products derived from refining crude oil.

This paper thus defines 'oil theft' widely. In addition to physical theft of oil, it includes theft of oil-related money in illegal transactions through (tax) fraud, misappropriation, and other malpractice, including also digital hijacking of oil infrastructure with ransomware. These all have in common that oil value is stolen from its rightful owners.

As the global oil supply chains are transnational and have a global reach, so too do the syndicates that commit organized oil theft. Individual acts of oil theft may have started as small scale, local, and opportunistic. However, relatively low risks, high profit margins, the opportunities to upscale thefts, and the ability to combine multiple elements of the oil supply chain provide many incentives for oil theft criminals to expand and professionalize their activities and networks. This is why legitimate oil companies, their senior officers, and their employees are increasingly at risk of getting embroiled in oil theft. Some theft syndicates are formed by aligning theft activities by companies or their employees (see Section 2.2). In other circumstances, existing crime organizations diversify their activities to include oil theft.

Global oil theft is estimated at US$133 bn per year (Bonnier and Bonnier 2019; Desjardins 2017). This equates to some 5–7 per cent of all crude oil and refined fuels produced. The first oil theft working paper demonstrates the prevalence of commercial oil theft across the supply chain (see Figure 1) and across geographies. Oil theft is a large-scale global problem, not limited to developing countries. However, developing countries are disproportionately impacted by the resulting loss of business confidence, loss of tax income, lawlessness, and armed criminals expanding their activities into kidnapping and other crime. The criminal syndicates responsible for oil theft are highly diversified. For some of them, their tentacles reach into many areas of the energy system and infrastructure, as well as into security and political organizations.

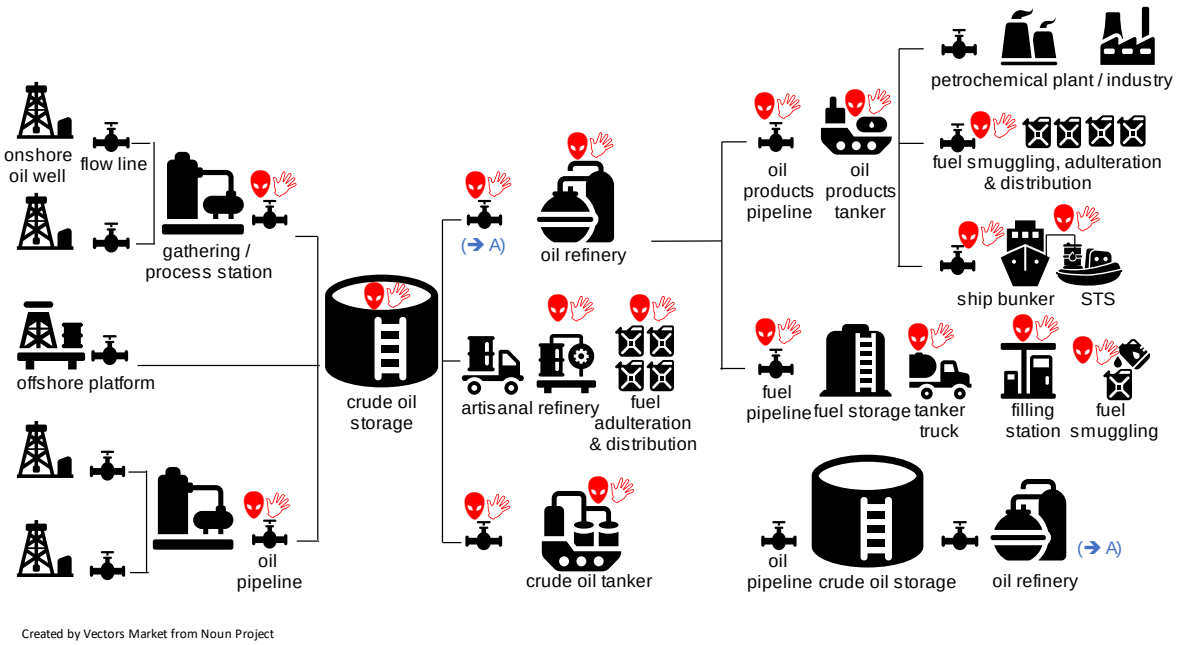
The paper is organized as follows. The remainder of this first section explains why oil theft is such a significant problem and discusses some of the difficulties involved in studying the topic. Section 2 focuses on *maritime oil theft*, which has several aspects, including oil piracy, syndicated theft from storage facilities, fuel adulteration, and manipulation of metering during fuel bunkering: it includes examples from both Asia and West Africa. Section 3 turns to the thorny question of *cyberattacks* on oil supplies and especially the attacks directed at the infrastructure of the oil industry. Section 4 examines the various gaps that are apparent in the battle to wipe out oil theft, with particular attention given to examples from Nigeria and Mexico. Section 5 examines the type of multidimensional approach needed to break the economy of oil theft. Finally, Section 6 drills down

into this broad approach and explains three specific high-impact opportunities to remedy the problem of oil theft. Section 7 concludes. A list of abbreviations and units used in the text follows the References section.

1.1 Why is oil theft a problem?

The impact of oil theft is multifaceted. Domestic resource mobilization (DRM), a strategic priority for developing countries, suffers from reduced tax yield due to oil being stolen and smuggled. In reference to a recent International Monetary Fund (IMF) study on tax revenues for developing countries (Balima et al. 2020), oil-producing countries impacted by oil theft have a tax yield of 9.2 per cent of GDP compared with the IMF's benchmark of 14.7 per cent for commodity-exporting developing countries. For oil-importing countries exposed to oil theft, the tax yield is 15.0 per cent compared with the IMFs estimate of 16.2 per cent for non-commodity-exporting developing countries (Romsom 2022). The impact of oil theft for producing countries is worse, as the value lost is a combination of loss of the physical resource and of associated government revenues. Although a wide range of potential factors can cause the negative correlation between oil theft and the tax yield of developing countries, the analysis illustrates that governments of developing countries dependent on oil revenues are particularly exposed to oil theft, if they are not well diversified by other sources of (tax) income. Government tax yield benchmarks are important for maintaining access to developing countries' principal sources of external financing, as well as in achieving countries' sustainable development goals (SDGs). A 'green recovery' post-COVID-19 through the promotion of carbon tax and other environmental taxes is at risk in countries with endemic/systemic oil theft. Increases in the price premiums for legitimate fuels over those for black-market fuels further incentivize oil thieves and cross-border smugglers.

Figure 1: Oil theft can occur at many points in the total supply chain



Note: oil supply-chain elements particularly exposed to oil theft and discussed in these oil theft papers are highlighted by .

Source: author's illustration; icons created by Vectors Market from the Noun Project: https://thenounproject.com.

Oil theft not only deprives governments of tax and other sources of public revenues: it also has direct and indirect impacts on the economic development of neighbouring countries. It erodes

regional business confidence, investment, and domestic development. A common pathway for oil theft's transnational impact is through cross-border fuel smuggling. Another pathway is through regional insecurity caused by violent oil theft operations that, for instance, disrupt maritime trade (notably in the Gulf of Guinea).

Fuel subsidies have particularly significant cross-border impacts when fuel smuggling effectively extends a country's subsidies into neighbouring countries. The volume leakage due to smuggling limits the benefits that such subsidies are intended to have for the poor or other targeted groups in the subsidizing country.[1] Instead, they profit the wealthy oil crime syndicates. The cost to the country from which the oil is stolen and smuggled is not only the loss of a valuable resource but also adverse macroeconomic impacts, including a raised fiscal deficit (via loss of revenue), accelerated inflation, and currency depreciation. By keeping domestic fuel prices fixed, the effective degree of subsidization increases and hence so do the price differentials with neighbouring countries. This increases the profitability of smuggling, providing further opportunity to grow the illegal market (Wang 1994). In the country that is the recipient of smuggling, these black-market fuels undercut legal retail outlets and thereby erode the government tax base (Soud et al. 2020). Smuggling can be driven by cross-border price arbitrage even if the originating country does not subsidize oil. Cross-border differences in taxation levels can be sufficient to create illicit flows of oil between states. Differential taxation or tax exemptions for certain fuel products, such as kerosene or light cycle oil (LCO), can be an incentive for fraudsters to adulterate fuels. Selling adulterated fuels on the black market, or blending them into legitimate supplies, compromises fuel combustion quality and has negative impacts on performance, assets (engines), and the environment (increasing air pollution, in particular).

Local communities are particularly adversely impacted by oil theft practices which exert a high and lasting toll on those most vulnerable and living off the land and waters. Oil spills from illegal pipeline taps and artisanal refineries cause permanent damage to communities and to the natural resources (water, soils etc.) upon which their livelihoods depend. Oil theft has disastrous consequences for communities when casual neglect of safety causes illegally tapped pipelines to explode. It also attracts and aggravates organized crime and local violence, through armed militias and crime-on-crime activities.

Environmental damage (from spills and artisanal refineries) compounds the detrimental economic impact of oil theft on oil-producing countries (see Figure 2). Furthermore, oil theft activities compromise the integrity and security of oil facilities, causing significant deferment of oil and government income. For example, while Nigerian oil theft is estimated at 400,000 bpd, shut-in oil production capacity is 1 m bpd, causing an annual tax deferment loss of US$20 bn in addition to US$12 bn loss in stolen product (Romsom 2022).

Oil theft often coincides with acts of violence that occur between law enforcement and organized crime syndicates, between organized crime syndicates themselves (i.e. crime-on-crime activities), between organized crime syndicates and members of the community (including employees of oil companies), and sometimes even between law enforcement and members of the community. Although not all acts of violence are directed towards the community, they almost always occur within the community. Leaving oil theft unchecked has destabilizing consequences for local communities and countries as a whole. Attacks against oil facilities and companies weaken existing governments and economies. Oil theft is both a symptom of violent conflict and a source of such

[1] Although we note that such subsidies are generally an inefficient way of targeting poor households as compared with, for instance, social protection. Non-poor subsidies disproportionately benefit wealthier households, as they consume more fuel.

conflict, particularly when competing criminal gangs attack each other for 'market share' or start their own extortion schemes towards these syndicates and towards their communities.

Figure 2: An example of an artisanal refinery in Nigeria

Source: images by Stakeholder Democracy, taken on 21 and 27 November 2012, reproduced from Flickr.com under CC BY-NC-ND 2.0.

Perhaps the most worrying impact of oil theft, beyond the loss of stolen resources and the destruction of the environment that results from oil spills and artisanal refineries, is the impairment of governments' ability to take care of their people and stimulate local development. In several countries, oil theft syndicates are winning the 'hearts and minds' of local communities, by offering employment and cheap or free fuel and providing gifts and community services such as paying for healthcare. In such countries, oil theft is portrayed as a legitimate (if not legal) part of a 'moral economy'. Some oil theft criminal groups describe their own activities as economically rational, politically necessary, morally defensible, and socially productive (Katsouris and Sayne 2013).

1.2 Why is solving oil theft a problem?

Oil theft is common, yet it is also by its nature mostly covert. Because of insiders' involvement, bribery, extortion, the threat of violence, and fear of persecution, there is a significant and systemic lack of practical information on oil theft activities. Basic data are limited on how much oil is stolen, what the stolen oil movements are, and how illicit oil transactions are conducted. Oil theft syndicates show great flexibility in adjusting their theft execution strategies and business models. They know how to exploit gaps in transnational jurisdictions and the limited capacity in law enforcement to move to new targets and methods. Individual oil theft networks are pervasive, diverse, overlapping, and secretive. Opportunistic allegiances complicate legal investigations into their activities, as there are no formal hierarchical structures to target. To hide oil theft, lines are blurred between legal and illegal oil supplies and activities (Figure 3). Much stolen oil finds its way into global commercial markets. This contaminates the legal oil trade with illegal product flows. Under-reporting of theft causes the scale and severity of oil theft problems to be underestimated. Oil theft countermeasures should address both the risk of occurrence (prevention) and the consequences to peoples' lives and the environment.

It is a misconception that oil thieves and smugglers always evade authorities and that corruption is caused by individual officers taking ad hoc bribes. Most fuel smuggling occurs through controlled border posts, where smugglers often pay a flat fee to the authorities in charge for unhindered passage. Smugglers and authorities have informal yet detailed agreements on what goods can be smuggled, how the levels of bribes are determined, and who should be paid. These arrangements benefit both smugglers and authorities. A clampdown that indiscriminately imposes hard borders (e.g. building walls) disproportionally affects survivalist smugglers, hurts the poor

living in borderlands, and causes socioeconomic collateral damage. However, such measures are seldom sufficient to deter professional smugglers who simply adapt to new markets, change routes, and amend their interactions with state actors to continue their practices.

Figure 3: A local petrol station selling a mix of legal and illegally refined products

Source: images by Stakeholder Democracy, taken on 18 November 2012, reproduced from Flickr.com under CC BY-NC-ND 2.0.

Oil theft, smuggling, and the illicit trade in petroleum products is often seen as a lesser form of organized crime than human trafficking, the drugs trade, smuggling of weapons, kidnapping, and other forms of violence and terrorism. However, oil theft opportunity crimes give rise to other forms of organized crime. Oil theft riches fund other criminal activities, such as illegal arms trafficking, violence, extremism, terrorism, kidnapping, drug trafficking, and human trafficking (Katsouris and Sayne 2013). Skill sets for oil theft and other crimes (e.g. smuggling of narcotics or people) overlap. Crime-on-crime activities and turning local populations into sympathetic audiences for their cause are what make the activities of oil theft syndicates, criminal cartels, freedom fighters, and terrorist groups remarkably similar (Cook 2008). This is also one of the key reasons why oil theft activities are so difficult to root out. The Transnational Alliance to Combat Illicit Trade (TRACIT) has evaluated and compared 12 global illicit trades, including the illicit trade in petroleum products, in terms of their wider impact on society and the SDGs (Bonnier and Bonnier 2019). The impact of oil theft is the most diverse among these trades. In addition to smothering economic growth (SDG 8) by undermining tax revenues, causing a loss of natural resources, and subverting economic stability, oil theft affects eight other SDGs (Romsom 2022).

2 Maritime oil theft

Various oil theft practices are described in Romsom (2022), mostly focused on land-based operations. However, other than by pipelines, the large-volume transportation of crude oil and fuels occurs by tankers. Significant oil theft also takes place in this part of the supply chain

Misappropriation, i.e. delivering less than the contracted volume to maximize profits, is, in comparison to piracy (see Section 2.4), a relatively subtle but effective method of conducting oil theft. The defrauding often involves customers, employees (and employers), and suppliers. Most thefts aim to be repeated by avoiding detection, or to be too immaterial to warrant action by the defrauded party. Yet the prevalence of misappropriation makes this kind of oil theft big business.

2.1 Misappropriation during crude oil loading

About 60 per cent of global crude oil production is transported by tanker. Once a tanker is loaded, its cargo's chemical fingerprint is typically a mix of many different crudes from a variety of oil fields. It is hence not possible to determine the origin of a crude cargo by its chemical composition. Unless a designer crude marker is added to the crude (see Section 6.1), it is practically impossible to determine if a crude cargo is mixed with stolen crude. It is generally at the point when crude oil is loaded on board a tanker that ownership of the crude transfers from seller to buyer and that taxes are due. Therefore, custody transfer metering (or fiscal metering) needs to be of high quality and accuracy (Engineering Institute of Technology n.d.). When crude oil is loaded, samples are taken to determine if it is within a certain range of API gravity,[2] sulphur content, and contamination. A common type of contamination is 'basic sediment and water' (BS&W). Crude specifications generally allow BS&W up to 0.5 or 1.0 per cent (S&P Global Platts 2022). BS&W is often carried in suspension or as an emulsion and is only detectable with sample analysis. 'Off-spec' cargoes happen frequently, particularly when BS&W separates as free water during the tanker voyage. When a cargo is found to be off spec, the origin of contamination could be the shore tank at the load port, the shore pipeline during loading, or the ship itself. If a cargo is found to be off spec on arrival at the discharge port, the ship is held liable and may be faced with a claim (Samaritis 2016). Due to the large volume carried in a Suezmax carrier (1 m bbl) or a very large crude carrier (VLCC, 2 m bbl), 'optimising' BS&W can be lucrative. A 1 per cent BS&W in a Suezmax is 'worth' US$0.65 m; in a VLCC it is US$1.3 m. A 1 per cent misappropriation of global crude with BS&W equates to more than US$13.5 bn per year.[3] Illegal ship-to-ship (STS) transfers, to avoid taxes or to export stolen crude, involve much less-accurate metering and assessment of contamination. Such transfers can affect the overall quality of the cargo and cause it to go off spec. There are many refineries that take off-spec cargoes at lower prices and that have a more relaxed attitude to conducting due diligence on the origins of cargoes purchased (see Section 6.3).

2.2 Misappropriation of fuels at refineries

Refineries are particularly vulnerable to oil theft, as the complexity of operations and infrastructure allows such theft to occur deeply hidden yet in plain sight. The fuel theft at Shell's Pulau Bukom refinery in Singapore is particularly telling in terms of the theft syndicates involved, the duration and scale of the theft operations, and the brazen criminal conduct of some of Shell's own

[2] API (American Petroleum Institute) gravity = (141.5/SG) − 131.5, with specific gravity (SG) the density of crude oil divided by the density of water. Crude oil with degree API (°API) of higher than 10 floats on water; lower than 10 and it sinks below water.

[3] About 60 per cent of all crude produced (95 m bpd) is transported by tanker and assumes an oil price of US$65/bbl.

employees. Pulau Bukom is Shell's largest wholly owned refinery, with a crude distillation capacity of half a million barrels per day (Figure 4). It is a sophisticated integrated refinery and petrochemicals complex, hosting an ethylene cracker complex, butadiene extraction unit, base oils plant, and bitumen production unit (Shell n.d.).

Figure 4: Shell Bukom refinery in Singapore

Source: image by budak, taken on 12 March 2016, reproduced from Flickr.com under CC BY-NC-ND 2.0.

The sequence of thefts happened from 2007 onwards, including 11 confirmed individual incidents of misappropriation during 2017 and 2018 alone. The refinery fuel theft (2014–18) is estimated at more than 340,000 tonnes of gasoil, worth US$150 m (Khasawneh and Ungku 2018). The theft involved two syndicates of perpetrators, with at least 30 people detained or charged to date, including:

- Eleven employees of Shell Eastern Petroleum Pte Ltd (Shell). Individual refinery operators at the bottom of the syndicate hierarchy earned US$150,000 from their illegal activities. A Shell fuel safety surveyor received US$500,000 for his part in the conspiracy in 2014–16 (Tang 2021). One of the masterminds of the conspiracy, who has pleaded guilty to 36 charges of criminal breach of trust, corruption, and money laundering, admitted to having received US$4.2 m in criminal proceeds (Lum 2022).
- Brokers who arranged the transactions, including at least three staff of Sentek Marine & Trading Pte. Charges were made against the company founder and managing director, a marketing and operations manager, and a cargo officer. The theft involved a Singapore bunkering vessel (*Sentek 26*) owned and operated by Sentek, Singapore's second-largest marine fuel supplier by volume in 2019 (Lam 2020).
- Three foreign captains and chief ship officers of foreign vessels that had loaded the stolen cargoes. These transnational aspects of the crime further complicated discovery, enforcement, and jurisdiction issues. The vessels, such as *Prime South*, *Prime Splendour*, and

MT *Gaea*, that bought the misappropriated gasoil belonged mainly to the company Prime Shipping. The forfeiture of Prime South (valued at US$4.5 m) was imposed by the Singapore court. One ship's captain was sentenced to five and a half years in jail for his part in misappropriating more than 8,000 tonnes of gas oil over ten occasions during 2016–17. He claimed to have received US$70,000–90,000 in total for his role. The other captain was sentenced to 70 months in jail, while the chief officer received a 30-month sentence. The captains acted on instructions from the major shareholder and the then chair of the board of Prime Shipping Corporation; a warrant was issued for his arrest, but he has thus far remained out of jurisdiction (See 2021).

- Thirteen employees from various surveying companies (including Intertek; Lam 2020) were bribed for a total of US$116,900. These surveying companies were tasked with validating the amount and quality of fuel transferred between parties under contract (CPIB 2021).

The case is ongoing in court and further charges are expected to be made. Detailed knowledge of refinery operations allowed the syndicate to deploy technical methods to hide the theft, such as:

- simultaneous fuel pumping operations combining theft-related activities with normal operations;
- routing the stolen fuel so as to avoid meters;
- simultaneous loading of legitimate fuel sold together with the transfer of the stolen fuel into the same vessels.

Physical misappropriations were difficult to detect, even though accounting processes highlighted the loss. Even after further improving metering accuracy, accounting processes, and other operational measures, losses continued to occur. After eliminating other potential causes of losses, misappropriation was suspected as the cause. After evidence was obtained about the theft, Shell implemented a range of measures at a cost of US$6 m, specifically targeted at preventing future theft (Lam 2021):

- additional high-accuracy meters;
- closed-circuit tv camera system;
- theft monitoring software.

This example shows that fuel theft is often committed by an illegal cross-industry syndicate rather than by individual actors, aligning the actions of refinery staff, bunker companies, traders, ship crew, fuel surveyors, transfer vessels, black-market fuel customers, etc. The information provided through Singapore's court cases reveals that despite the large number of people involved in the theft syndicates (for the Shell Bukom case at least 30, although double that number is more likely), the bulk of the profits went to those not so far caught.[4]

[4] Assuming a high US$500,000 average reward for each of 60 potential accomplices, this accounts for only one-fifth of the value of the fuel stolen.

2.3 Misappropriation during fuel bunkering

Misappropriation of maritime fuel is very common and many schemes exist to defraud refineries and ship-management companies. Such schemes are commonly based on siphoning off fuel and selling the difference between contracted volumes and the actual delivered volumes (i.e. fraud) (Mahmud 2021).

2.3.1 Adulteration of fuel quality

Adulteration of fuels generally serves two overlapping purposes:

- to make up additional volume, so more can be sold;
- to covertly replace or dilute high-value components with inferior chemicals so that low-quality products can be sold at high prices.

The next two sections discuss two common fuel adulteration schemes. A variant of the 'milo' scheme was discussed in section 3.1.1 of the first report on oil theft, involving the illegal use of LCO as a low-quality substitute for diesel in a grand-scale fuel adulteration scheme in China, worth US$3.9 bn annualized in avoided fuel taxes (Romsom 2022).

The cappuccino effect

Similarly to the manipulation of BS&W for crude oil cargoes, (marine) fuels offer opportunities to manipulate delivered volumes, for example by adding air to the fuel. This is such a well-known fraud scheme that it has its own name: the 'cappuccino effect' (Chinoy 2014). The cappuccino effect remains one of the most common and widely used malpractices in the fuel bunkering industry. It is common to find a sudden 'drop' in a ship's fuel levels days after bunkering that can equate to a fuel loss of 30–40 tonnes, i.e. a loss of US$20,000 for marine gasoil or US$14,000 for intermediate fuel oil. The frothing in bunker fuel is caused by blowing in compressed air through the fuel delivery hose. Because the air is initially held in suspension in the fuel, it would appear that the right volume of fuel is delivered as ordered. However, when the fuel settles, the trapped air is liberated and the liquid fuel level in the tank drops. The problem can be avoided by using the right type of meter—one that is able to measure the mass as well as the volume of the fuel delivered. As the cappuccino effect influences the density of the fuel, this is then easily detected. Mass-flow meters (MFM), such as Coriolis meters, have been in existence for many years and have many benefits beyond being accurate. Singapore has developed a standard for bunker procedures that specifies MFM and prohibits the use of compressed air during the bunker process (see Section 2.3.3).

Making milo

As an alternative to adding air to fuel, other fluid contaminants can be added, such as mud, spent cooking oil, used motor oil, styrene, solvents, dry cleaning fluids, fertilizers, cosmetics, and other chemical waste. Generally, these 'additives' cause the fuel mixture to become opaque grey-brown, hence its name: 'milo'. Rogue fuels are known to cause 'phantom' ship engine failures with untraceable origins (Sahu and Tan 2020).[5] In 2018, a global wave of bad bunkers affected some 200 vessels, with at least 80 cases originating in Houston, 35 in Panama, and 15 in Singapore (*Ship & Bunker* 2018). Panama's overall marine fuel sales declined in 2018, with shipping companies

[5] A key issue with bad bunkers is that these adulterated fuels pass conventional fuel testing and meet ISO 8127 chemical requirements for bunkers. New 2020 IMO regulations for very low sulphur shipping fuels appear not to have not solved these fuel adulteration and quality issues, with many reports of sediment related fuel-quality issues.

deciding to bunker elsewhere. Some ships affected by fuel quality-related engine failures were adrift in open sea; others ran aground. Apart from safety and environmental risks from ship breakdowns at sea, there are concerns about criminals adulterating ship fuels not only for profit but also as a deliberate act of sabotage to facilitate piracy.

2.3.2 Manipulation of metering and fuel data

The fuel bunkering business is highly competitive, with oversaturated supply in key bunkering hubs. Bunker companies deliver a non-diversified commodity-priced product and rely on operational cost efficiency as a key competitive differentiator. This business is vulnerable to institutionalized theft, with companies seeking 'additional value' as well as individuals seeking get-rich-quick schemes. There are a variety of methods that aim to defraud by manipulating fuel delivery data. Here are a few of the most common data manipulation methods, often applied in combination:

- comingling unmetered and unaccounted for volumes during a commercial supply;
- mis-stating the original fuel in the tank;
- manipulating fuel delivery metering devices;
- applying the wrong conversion factors;
- intentional 'errors' and falsification of delivered fuel records;
- siphoning off delivered volumes.

The following is an example of a common fuel theft scheme that involves a syndicate of criminal actors all benefiting from the fraud:

The amount of fuel consumption of a ship is influenced by a large number of factors, such as current, waves, wind, distance travelled, the ship's speed, etc. Hence, the amount of fuel remaining on board has a substantial degree of uncertainty. Fuel surveyors would understate the remaining fuel on board, so that bunker suppliers could overstate the amount of fuel delivered, while the difference is sold on the black market. For this scheme to work, the ship's captain and crew must be part of the ploy. Misappropriated fuel is often sold by the ship's crew in small parcels to converted tug-boats or fishing trawlers in neighbouring countries, making it even more difficult to trace the theft. Such schemes of 'syndicated shoplifting' involve buy-back arrangements: the fuel thief makes a cash payment to the complicit crew to sell off some of the ship's fuel as their share of the loot. Once the fuel has been transferred, e.g. into a converted tugboat, the fuel (marine gasoil) will then be sold on the open market as diesel to local villages and distributed, for example in water bottles sold from the roadside to scooters (Figure 5). This supply-chain network of fuel theft creates a large market for stolen fuel, and this consumer demand supports fuel theft at a mass scale.

Figure 5: Examples of roadside illegal fuel sales in Siem Reap, Cambodia (left), and Phuket, Thailand (right)

Source: left-hand image by HeyItsWilliam, taken on 21 April 2012, reproduced from Flickr.com under CC BY-ND 2.0; right-hand image by Edwin.11, taken on 15 May 2011, reproduced from Flickr.com under CC BY 2.0.

Shipping is a margin business, and fuel costs account for 50–60 per cent of the running cost of most merchant vessels. Reducing fuel consumption by just 1 per cent can mean an annual saving of US$50,000 for a mid-sized bulk carrier and US$300,000 for a large container ship. Optimizing fuel (including theft prevention) is crucial in order for ship owners and operators to be competitive in their market. More stringent environmental regulations, in particular the expansion of emission control areas (ECAs) and stricter emission standards in ECAs drive shipping companies to convert their engines to higher-quality fuels. The change in shipping fuels towards gasoil and other low- or zero-sulphur options increases the marketability as well as the margins achieved from fuel theft.

Shipping companies struggle to arrest fuel theft. They are dependent on bunkering standards and enforcement from local authorities. Metering 'errors' can represent up to 27 per cent (Gloystein and Geddie 2018) and are difficult to prove, unless the ship has its own (untampered-with) MFM. With fuel a major operating cost, ship companies are installing improved metering and fuel tracking systems, to enhance the monitoring of fuel balance and usage. Also, more reliable surveyors (those less likely to be bribed) help to avoid fuel theft. Digital receipt systems for fuel supplies limit opportunities for falsification of records and human error in fuel bunkering. Electronic systems can automatically generate official records between MFM output and delivery notes without human intervention.

There are a variety of reasons why despite these above efforts, maritime fuel theft is difficult to root out. Many fuel thefts involve shipping crews. Ship companies are highly dependent on the reliability and integrity of their captains to avoid illicit practices on board. Unless crew members talk, it is difficult to obtain evidence of fuel malpractices. The variety of parties involved in theft obscures the evidence trail. Each fuel theft incident may be too small for a shipping company to act upon. Small-scale fuel theft incidents are so pervasive that they do not affect companies' competitiveness (because every shipping company suffers in the same way). Considered petty theft, these acts are often condoned as an 'accepted loss'. Culprits are smart in limiting their individual thefts to below the threshold of materiality. Misappropriation is so common that fuel trading companies plan for losses of 0.2–0.4 per cent of ordered cargo volumes. However, Defence IQ estimates the total illegal maritime fuel trade in South-East Asia (SEA) to be worth US$10 bn per year, i.e. 3 per cent of SEA fuel consumption (Gloystein and Geddie 2018). Defence IQ's estimate has been substantiated by the impact of MFM standards being applied in Singapore fuel bunkering.

2.3.3 Regulations and technologies preventing fuel theft

Singapore is SEA's main refinery hub, the world's largest marine refuelling port, and one of the world's most important fuel trading hubs. Singapore marine bunkering accounts for 20 per cent of global bunkering sales. Compared with other countries, Singapore's marine business is exceptionally well regulated, with mandatory standards for operations and a maritime and port authority (MPA) that actively controls compliance and punishes malpractice. Singapore's courts are effective in holding criminal organizations and white-collar crimes to account. Still, even in Singapore, frequent acts of malpractice occur in fuel trading and bunkering businesses. Some cases demonstrate the blurring of lines between legal and illegal activities, with the undesired consequence that legal businesses, including banks, are getting caught in the shady practices of the bunker business.

The Singapore local market currently has in excess of 40 suppliers/traders of bunker fuels; many are small companies. This is a major reduction from the 63 bunkering companies that existed a few years ago. Many of the companies that have disappeared had their licences removed due to fraud and other malpractice (see Box A). The city state has made many strides to root out fuel theft, but its efforts also highlight how deeply oil theft and fraud are embedded in the industry. Bankruptcies of fuel trading and bunkering companies often follow delisting by MPA for fraud, dragging other fuel trading companies and banks into a sea of unpaid debt. In the last few years, Singapore fuel fraud-related bankruptcies left an unpaid debt of more than US$6 bn. The maritime fuel industry consequently faces serious physical and financial compliance issues and major credit risks.

The Singapore port is the most advanced globally in the implementation and enforcement of standards to prevent fuel theft. In September 2014, Singapore arrested 53 people involved in the illegal ship fuel trade, most of whom were crew members selling their own ships' fuel (Mahmud 2021). Detailed regulations for fuel bunkering operations have since been implemented. Code of practice SS 648 specifies fuel transfer meter standards (MFMs are mandatory on Singapore bunker vessels), MFM calibration requirements, and terms for claims regarding fuel quality and quantity disputes. Code of practice SS 600, detailing documentation and verification procedures, prohibits the use of compressed air (often used for making cappuccino bunkers) during the bunkering process. Singapore has backed up the application of these standards with efforts to enforce compliance through patrols and with the MPA exerting its authority. Furthermore, Singapore courts have taken judicial action against fraud and theft.

The use of MFM is estimated to have saved Singapore US$1.7 bn to date in what otherwise would have been subject to malpractice such as fuel adulteration and short-selling by on average 2.5 per cent (Ship & Bunker 2020).[6] Despite these measures, there are still efforts to cheat and steal, for example through the use of strong magnets to manipulate the MFM readings (by up to 27 per cent). For this offence, Inter-Pacific Petroleum and others recently had their bunkering licences revoked.

[6] Singapore made MFM obligatory for marine gasoil (MGO) bunkering since 1 January 2017 and for intermediate fuel oil (IFO) since 1 July 2019. In the period following implementation of this rule until October 2020, MFM technology saved marine fuel buyers in Singapore US$1.7 bn. Singapore is one of the few ports worldwide that publishes detailed bunker sales volumes. Comparing this volume data with wholesale-to-retail price spreads, before and after MFM implementation, pre-MFM bunkering volumes appeared to be shorted by 2.5 per cent on average.

Box A: Singapore bunkering industry faces serious compliance issues and major credit risks

In 2020, Singapore had 45 operational and licensed bunkering companies. This followed a period of significant weeding out of malpractice among bunker companies that tallied 63 in number in 2012. The Marine and Port Authority of Singapore (MPA) announced in October 2019 that it had revoked Inter-Pacific Petroleum's bunker craft operator licence after it found 'magnetic interferences' affecting numerous mass-flow meter readings across its bunker tankers. With effect from 9 December 2019, Inter-Pacific ceased to operate as a bunker supplier in the Port of Singapore. The company leaves behind debts totalling US$168.5 m. Between 2012 and 2019, the MPA revoked the bunkering licences (in-year) of 19 companies because of fraud and malpractice.

Singapore bunker companies involved with fraud, fuel theft, and malpractice

1) **Inter-Pacific (2019)** for magnet interferences affecting measurements of bunkers supplied in numerous MFM readings across Inter-Pacific's fleet of bunker tankers.
2) **Southernpec (2019)** for magnet interference of MFM in bunkering operations, inaccurate recording of information in bunkering documents.
3) **Transocean Oil (2017)** for falsification of records and discrepancies in the stock movement logbooks on board the bunker tankers.
4) **Panoil Petroleum Pte Ltd (2017)** for unauthorized alterations on the pipelines of their bunker tankers and non-compliances to the bunkering procedures.
5) **Universal Energy Pte Ltd (2017)** for delivery of bunkers that were severely aerated as well as stoppages during bunkering operations. Creditors subsequently filed US$105 m in claims.
6) **AC Oil (2016)** for discrepancies and wrongful declarations in the records kept; incidences of bunker transfers between bunker tankers without MPA's approval; and carrying a more flammable Class B petroleum product, despite being licensed to carry only marine gasoil, a Class C petroleum product.
7) **Seaquest Tanker (2016)** for discrepancies and wrongful declarations in the records kept on board their bunker vessels; incidences of bunker transfers between bunker tankers without MPA's approval.
8) **Vermont UM Bunkering (2016)** for discrepancies and wrongful declarations in records kept on board their bunker vessels; for incidences of bunker transfers between bunker tankers without MPA's approval. In 2017, members of its senior management were charged with conspiracy to cheat customers.
9) **Tankoil Marine Services (2015)** for discrepancies and wrongful declarations in the records kept; for incidences of bunker transfers between bunker tankers without MPA's approval.
10) **Hong Fatt Oil Trading (2015)** for discrepancies and wrongful declarations in the records kept; for incidences of bunker transfers between bunker tankers without MPA's approval.
11) **Coteam Petroleum Trading (2014)** for allowing other companies to use their bunker delivery notes (BDNs) to supply bunkers; for delivering bunkers on behalf of unlicensed company to customers of that company.
12) **Northwest Resources (2014)** following the conviction of one of the company's directors for bunkering-related corruption offences, having been charged with 50 counts of bunkering-related offences under the Prevention of Corruption Act.
13) **Excel Petroleum Enterprise (2014)** for allowing other companies to use their BDNs to supply bunkers.
14) **Lian Hoe Leong & Brothers (2014)** for allowing other companies to use their BDNs to supply bunkers.
15) **Coast Channels Marine Service (2013)** for allowing other companies to use their BDNs to supply bunkers.
16) **Golden Lights HS Bunkering (2013)** for allowing another company to use its BDNs to supply bunkers to the customers of that company.
17) **Shing Li Shipping (2013**) for delivering bunkers on behalf of an unlicensed company to customers of that company.
18) **Palmstone Petroleum (2013)** for allowing another company to use its BDNs to supply bunkers to customers of that other company.
19) **Windbuild Petrofin (2012)** for allowing another company to use its BDNs to supply bunkers to the customers of that company; for also delivering bunkers on behalf of an unlicensed company to customers of that company.

Source: MPA Singapore (various dates).

Progressive Power Co Pte Ltd (2014) and **JL Petroleum** Pte Ltd (2015) were convicted for supplying bunkers without a licence and using BDNs belonging to another company; committing an offence punishable under Singapore Regulation 78(b).

The malpractice of **Tankoil Marine Services** (revoked in 2015) also resulted in the bankruptcy of global bunker company **OW Bunker** in 2014, with a loss of US$125 million and US$1.5 bn in global outstanding debts, of which US$730 m was for outstanding fuel bills (Bunker Index 2014). In the transactions between OW Bunker's subsidiary in Singapore, **Dynamic Oil Trading**, and Tankoil Marine Services, 'unfathomable amounts' of bunker fuel volume were reported to have disappeared without trace (*Ship & Bunker* 2015).

In March 2018, 22 individuals, including two employees from **Brightoil**, pleaded guilty at a Singapore court over an illegal transaction of 45 metric tonnes of marine gasoil (MGO) from Singapore registered bunkering vessel Brightoil 326 (*Manifold Times* 2018). In November 2018, Brightoil's entire Singapore bunker tanker fleet was placed under arrest, following a winding up order against Brightoil on behalf of Vietnam-based trader Petrolimex after Brightoil failed to repay more than US$30 million in debt. In 2019, Brightoil's entire bunker fleet of six bunker vessels was subsequently sold off. Various banks issued additional claims on Brightoil, exceeding US$47 million.

In 2019, **Coastal Oil Singapore** Pte Ltd filed for liquidation with US$354 m in bank debt against a modest US$61 m in tangible assets. Debt fraud allegations were raised against Coastal Oil by Cosco Shipping International Co. Ltd (Hogg 2019; Mui and Tay 2020).

In 2020, **Ocean Bunkering** filed for bankruptcy (Reuters 2020) among the fallout of parent company **Hin Leong**'s admitted malpractice of incurring US$800 million in futures losses over the years that were not reflected in the financial statements (Hume and Palma 2020). Hing Leong oil trading business collapsed under a debt of US$3.9 bn (Hume et al. 2020) and its owner O.K. Lim has been charged in the Singapore court with 25 counts of abetment of forgery for the purpose of cheating (Reuters and Chen 2021).

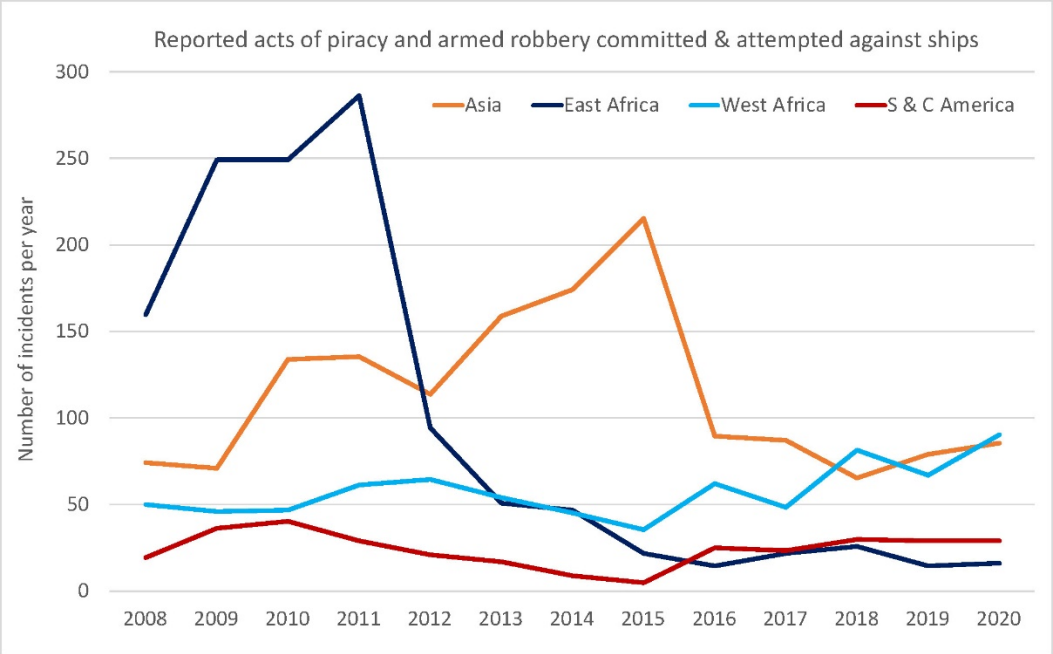
2.4 Oil tanker piracy

According to international law, piracy is defined as a violent action for private ends and without authorization of a public authority, committed outside the normal jurisdiction of any state. The historic objective of piracy was to make financial profit out of the capture of commercial ships and their cargoes (Jenkins n.d.).

Piracy is regarded as an offence against the law of nations and therefore public vessels of any state are permitted to seize a pirate ship and try the crew in court, regardless of nationality and domicile. If found guilty, pirates can be punished and their ship confiscated. In the late twentieth century, the hijacking of ships and aeroplanes became a new form of piracy, often linked to terrorism and terrorist organizations. In recent years, piracy has again been more focused on commercial vessels for financial profit through theft, but also through ransom from kidnapping. A modern form of piracy is the digital hijacking of assets for financial profit using ransomware. Although the assets hijacked are often within a state's jurisdiction, the digital pirates are more typically located outside of the range of the judicial authorities of the victim (see Section 3).

Following the decline in large-scale piracy off the coast of Somalia (East Africa) after 2010–11, piracy and armed robbery of sea vessels spiked in Asia, from 2012 to 2016. This was followed by a marked increase in similar piracy events in West Africa in 2016 and subsequent years (see Figure 6).

Figure 6: Shifting geographical patterns of maritime piracy and armed robbery at sea, 2008–20



Note: the graph above shows piracy and armed robbery incidents against all types of vessels, including tankers.

Source: author's elaboration based on various IMO pricay reports.[7]

Among the different ships that are targeted, the piracy of oil tankers is the most brazen and lucrative. The objective is commonly to board and hijack the tanker in mid-seas, switch off its communication systems and AIS (automatic identification system) transponder, and sail it to a predetermined location where it meets the pirates' mother ship (e.g. another stolen tanker) for an STS transfer of the hijacked vessel's cargo to the mother ship. Transfer points are either in international waters where there is no jurisdiction or in 'no man's land', i.e. where territorial waters overlap between countries and there is no control from either authority. The transfer of crude or fuel to another vessel can take up to a day, and it is in this period that the piracy operation is most vulnerable to intervention. For such a piracy act to be successful, detailed information is needed about the target's route, schedule, and cargo volume and content (different oil cargo types require different tankers). In some incidents, there are indications of conspiracy between tankers and pirates, as well the involvement of established syndicates that organize the thefts and manage the onward sale and distribution of the stolen oil. However, an informal network of contacts and ad hoc soliciting for black-market marine fuel supplies are also part of the overall scheme.[8] Data analytics have also revealed patterns of piracy events disproportionally 'affecting' some shipping companies, with multiple vessels being pirated in succession. It is unlikely to be just bad luck that some of these same shipping companies also had ships that were pirated more than once. Another common target for pirates is an oil-smuggling vessel from another crime syndicate.

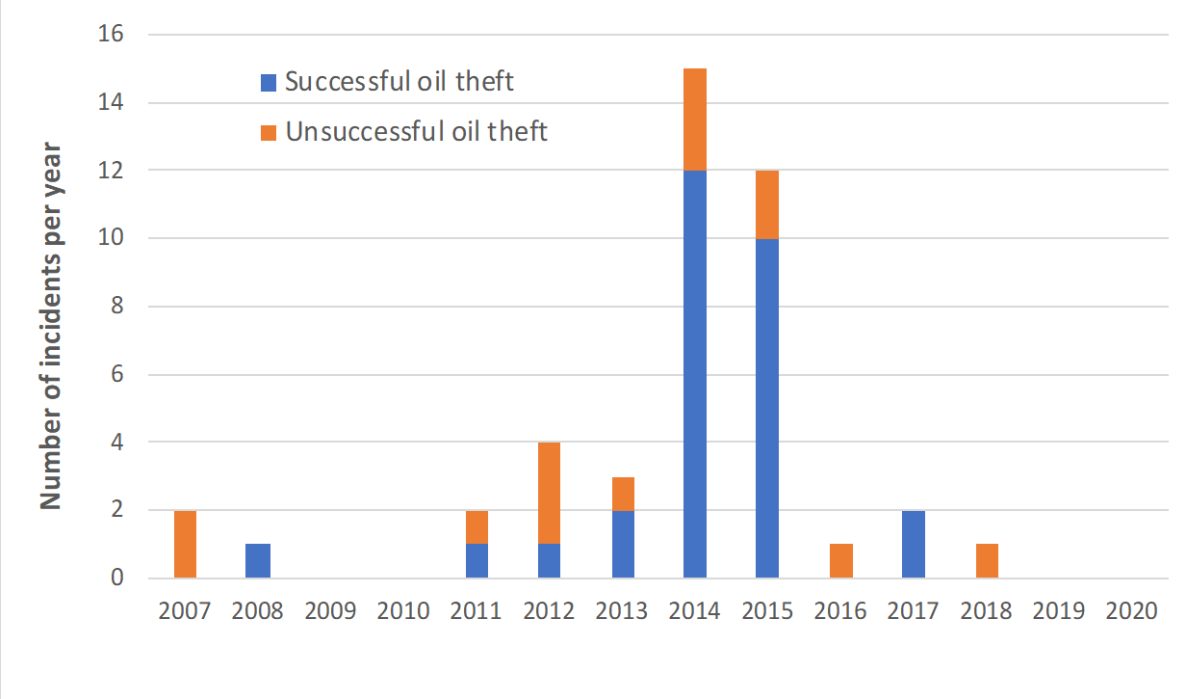
[7] Piracy reports available at: https://www.imo.org/en/OurWork/Security/Pages/Piracy-Reports-Default.aspx (accessed 24 March 2022).

[8] In September 2014, following intervention by the Singapore Police Coast Guard, the Singapore authorities arrested 53 people involved in the illegal fuel trade, including the ship crew (Mahmud 2021).

2.4.1 Oil piracy in Asia

In 2014, 12 successful incidents of oil tanker piracy occurred in the South China Sea (mostly off the east coast of Malaysia), eight of which involved vessels that had left Singapore. This was a marked increase from 2011, when only one such incident had been reported (see Figure 7). Perpetrators appeared to target vessels loaded with a higher grade of fuel or with better-quality oil from Singapore refineries. Most of the incidents targeted marine gasoil (MGO), which is abundant and relatively highly priced, has high demand, and can be sold as diesel fuel on the black market. Other product types targeted were marine diesel oil (MDO), automotive diesel fuel (ADF), diesel, marine fuel oil (MFO), and lube oil. The desire to avoid fuel taxes and exploitation of fuel price differences across countries have a large influence on the prevalence of such oil-theft-related piracy.

Figure 7: Piracy incidents targeting tankers for oil theft in South East Asia have been declining since 2016



Source: authors' illustration based on ReCAAP (n.d.-b).

The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) is the first regional government-to-government agreement to promote and enhance co-operation against piracy and armed robbery against ships in Asia. It currently has 20 contracting parties—14 countries in Asia plus Australia, Norway, the Netherlands, Denmark, the United Kingdom, and the United States. ReCAAP uses data analytics to identify correlations and trends related to piracy and armed robbery against ships at sea (ReCAAP 2020). It has reported on 1,700 such incidents in Asia from 2007 to 2020, with information that includes the number of perpetrators, types of weapons used, treatment of crew, items stolen, types of ships boarded, and time of incident. It provides relevant information to its Information Sharing Centre (ISC) and Information Network System (IFN) to prevent further incidents.

According to ReCAAP, during 2007–20, 36 per cent of illegally boarded ships were tankers, 27 per cent were bulk carriers, 14 per cent were tug-boats or supply vessels, and 13 per cent were container ships. Tankers (crude, petroleum products, LPG, LNG, and chemical tankers) accounted for 577 reported incidents at sea, including 43 ship hijacks (29 successful and 14 attempted), mostly during 2011–15 and the most recent in 2018 (see Table 1; ReCAAP n.d.-b). In the majority of

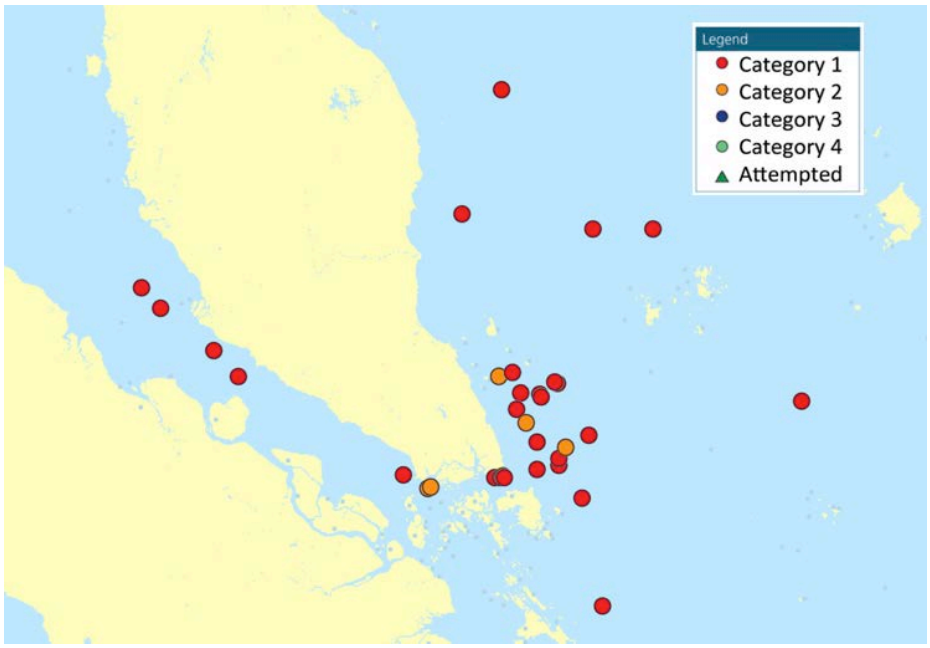
reported piracy incidents, the pirates boarded the tanker while underway, tied the crew and locked them in the cabin, took over control of the tanker, and transferred the oil to another tanker or barge that came alongside (ReCAAP 2014/2015). Fourteen of the 24 oil-siphoning incidents during 2011–14 happened in the South China Sea, with a further two cases in Indonesia and one in the straits of Malacca and Singapore (see Figure 8). Preferred locations are far from shore and outside the jurisdictions of regional authorities, to allow sufficient time to transfer the oil. It should be noted that robberies from tankers may mask initial attempts to steal the tankers' oil that were abandoned when the fuel carried was not of the type desired by the pirates or the attempts were abandoned for other reasons (Walje 2014).

Table 1: Success in countering tanker piracy incidents with intent to steal oil in South East Asia

	2011	2012	2013	2014	2015	2016	2017	2018
Successful	1	1	2	12	10	0	2	0
Unsuccessful	1	3	1	3	2	1	0	1
Total	2	4	3	15	12	1	2	1
Oil stolen (metric tonnes)	0.8	830	1,690	11,378	N/A	N/A	2,070	N/A

Source: authors' construction based on ReCAAP (n.d.-b).

Figure 8: Location of hijacking of tanker incidents, 2007–18



Source: reproduced from ReCAAP (n.d.-b), with permission.

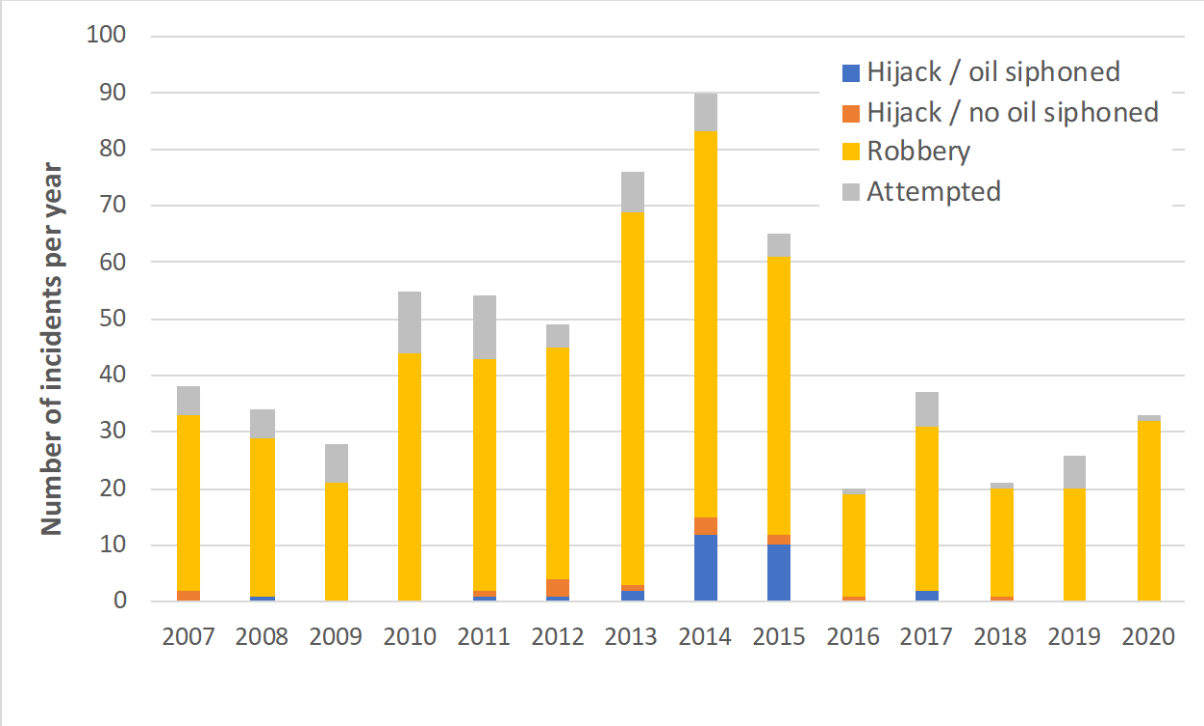
While oil-theft-related tanker piracy has been successfully contained, the overall number of incidents involving piracy and sea robbery in Asia has been increasing in recent years (see Figure 9), particularly in Singapore Straits, while new maritime threats such as cybersecurity are emerging. With 20 incidents since 2016, kidnapping for ransom is a more recent trend. From March 2016 to the end of 2019, 78 crew members were abducted in the Asia region, of whom ten either died or were killed while all but one of the rest were released or rescued. The fate of the remaining individual is unclear (Mohindru 2020).

A key factor in preventing a successful hijack is the vigilance of the crew in activating the ship security alert system (SSAS) (Anish 2020), a silent alarm beacon that signals the ship's details and location to the ship's owner and to SSAS monitoring services, who will in return notify the nearest

national authorities to dispatch law enforcement forces. Another factor in preventing piracy is the effective communication and co-ordination of organizations such as ReCAAP with regional authorities and the maritime community. ReCAAP, in collaboration with the IFC (Information Fusion Centre) and RSiS, have issued a guide for tankers operating in Asia to help them avoid piracy and robbery (ReCAAP et al. n.d.).

ReCAAP has also defined an incident severity categorization (categories 1 to 4) based the level of violence and the economic loss incurred: see Appendix A. Tanker hijacking incidents are the most severe, Category 1 or Category 2.

Figure 9: Robberies, hijacks, and attempted hijacks involving tankers in South East Asia, 2007–20



Note: it is likely that not all attempts to target tankers have been reported to ReCAAP.

Source: authors' illustration based on ReCAAP (n.d.-b).

A key factor in preventing a successful hijack is the vigilance of the crew in activating the ship security alert system (SSAS) (Anish 2020), a silent alarm beacon that signals the ship's details and location to the ship's owner and to SSAS monitoring services, who will in return notify the nearest national authorities to dispatch law enforcement forces. Another factor in preventing piracy is the effective communication and co-ordination of organizations such as ReCAAP with regional authorities and the maritime community. ReCAAP, in collaboration with the IFC (Information Fusion Centre) and RSiS, have issued a guide for tankers operating in Asia to help them avoid piracy and robbery (ReCAAP et al. n.d.).

ReCAAP has also defined an incident severity categorization (categories 1 to 4) based the level of violence and the economic loss incurred: see Appendix A. Tanker hijacking incidents are the most severe, Category 1 or Category 2.

2.4.2 Oil piracy in West Africa

Maritime security is essential to maintaining the flow of revenues from oil and gas, which have the potential to contribute significantly to development in West Africa. Maritime insecurity prevents the Gulf of Guinea countries from fully realizing the profits of their oil wealth. Moreover, maritime insecurity caused by acts of oil piracy also impacts the economies of neighbouring non-oil-producing countries. Benin's government revenues fell by at least 28 per cent in 2012, following 22 pirate attacks off the country's coast (mainly targeting tankers carrying oil products) the previous year. The revenue reduction was caused principally by a 70 per cent decline in economic activity in the Port of Cotonou (Romsom 2022: section 3.2.1). This example highlights the impact of oil-theft-inspired piracy and its potential to cripple the public finances and governments of developing nations, even if, like Benin, they are not oil producers (UNODC 2013).

In 2014, piracy in the Gulf of Guinea increased at an alarming rate. In 2016, the UN Security Council spoke out against piracy and armed robbery in the Gulf, as it badly affected the economic development of the region and threatened commercial maritime activities (UNSC 2016). It called for a comprehensive regional framework to eradicate these illegal practices, stressing the importance of addressing underlying causes and strengthening justice systems and judicial co-operation in the region. Key connections threatening the stability of countries in the region were highlighted:

1. The links between maritime piracy and poor governance, extreme poverty, and socio-political violence.
2. The links between maritime piracy and transnational organized crime.
3. The links between maritime piracy and the financing of activities of terrorist groups operating in the region.

Despite this international attention in 2019, the Gulf of Guinea was still the region most affected by piracy and maritime robbery worldwide. Although fewer incidents were reported compared with 2018 (98 versus 112, including 40 tanker incidents, 30 cases of kidnapping of crew, six of which involved tankers, and four cases of vessel hijacking), there was a 60 per cent increase, to 164, in the number of crew members reported kidnapped and held for an average period of 34 days (ranging from two to more than 84 days), in addition to 95 seafarers held hostage for a shorter period of up to four days (Joubert 2020).

In 2019, three of the four vessels hijacked in the Gulf of Guinea were tankers; the fourth was a tug boat used to attack another ship. All hijacked vessels were flagged in Gulf of Guinea countries (three in Nigeria and one in Togo) and were managed by local companies, allowing criminals to know these local vessels' routines and operations. However, none of the three tanker hijackings in 2019 resulted in oil theft or ransom. A fast response by international navy vessels located in the Gulf of Guinea resulted in pirates abandoning ship upon their approach, or their interception and arrest. The third hijacked tanker was abandoned after it ran out of fuel.

Following fast-response measures to counter oil piracy, particularly in the Gulf of Guinea, tankers have become the target of alternative acts of piracy, whereby the objective is now not cargo but rather to kidnap crews for ransom. This has a lower risk for criminals, as the act of kidnapping is faster and escape more certain than the activities required to transport, transfer, and escape with a large volume of stolen oil. There is further evidence that success in tackling oil piracy has made criminals focus on other targets, including other criminal groups. This criminal-on-criminal crime, conducted to stay outside the scope of state-centred law enforcement efforts, has unfortunately escalated the level of violence.

Nigerian authorities claim that a number of kidnapping cases are related to illegal oil transactions. For example, they claim that the kidnapping of crew from the tanker *Apecus* on 19 April 2019 was staged. The plan was to use this tanker and another tanker, the MT *Invictus*, to move stolen crude oil from Nigeria to Ghana. The managing director of the oil trading and shipping company Petrogress Inc. was arrested for oil smuggling, together with 17 accomplices. Tankers used by Petrogress Inc. have a track record of use as transfer vessels in prior oil tanker hijacks (MT *Invictus*) and illegal bunkering operations (Joubert 2020).

Instances of oil theft may go unreported when they involve insider complicity, or when reports are withheld to avoid an increase in insurance premiums. With the effective collaboration of international naval forces, criminals have relocated their activities to territorial waters and land-based operations where international forces have no jurisdiction.

2.4.3 Policy responses and regional approaches against oil piracy

At the 2016 UN Security Council resolution against piracy and armed robbery in the Gulf of Guinea, the then UN assistant secretary-general for political affairs, Tayé-Brook Zerihoun, remarked:

> Ultimately, countering the current threats requires a combination of capacities, including qualitative improvements in the collection of intelligence; the sharing and improved analyses of intelligence; enhancement of the capacities—both infrastructure and training—of local enforcement agencies of the Gulf of Guinea countries; and the establishment of an effective customs and border control system throughout the sub-region. (UNSC 2016)

Regional co-operation in capacity-building efforts was deemed necessary to avoid duplication of effort. The Security Council said it recognized that regional peace and stability, the strengthening of state institutions, economic and social development, respect for human rights, and the rule of law are all necessary to create the conditions for the eradication of piracy and armed robbery at sea in the Gulf of Guinea (DefenceWeb 2016).

Oil piracy and its entanglements with maritime security and oil smuggling is a regional issue involving transnational crime syndicates. Arms proliferation, crude oil theft, terrorism, and migration are interrelated, cross-state issues affecting maritime security (Chatham House 2013). The increased sophistication of transnational crime networks demands similar sophistication in transnational co-operative law enforcement (One Earth Future 2020; Ralby 2017a). Various regional organizations have an interest in maritime security and have overlapping mandates: the Maritime Organization of West and Central Africa (MOWCA), the Economic Community of Central African States (ECCAS), the Economic Community of West African States (ECOWAS), and the Gulf of Guinea Commission (GGC). Among these, the GGC, established in 2001, has the strongest mandate for regional co-operation on maritime issues.

Recognizing the multidimensional nature of (oil-theft-based) piracy and robbery at sea, some organizations have developed integrated approaches to address the underlying causes and issues. One such organization is Stable Seas, initially a collaboration of One Earth Future Research, Secure Fisheries, and Oceans Beyond Piracy (One Earth Future 2021). Stable Seas, now an independent foundation with a global scope, has focused on developing a more comprehensive and holistic understanding of the interconnected nature of maritime security challenges. It developed a Maritime Security Index to measure and combine disparate issues, previously treated as siloed areas. The index has been adopted by navies, coast guards, and government agencies to monitor and address maritime security. Stable Seas' outreach programme aims to share its research and

targeted information with national governments. Its holistic approach also provides detailed analysis on newly emerging maritime security issues. One of the challenges is that criminal actors quickly respond to security-enhancing initiatives, seeking to keep one step ahead of law enforcement organizations. Violent non-state actors thereby exploit the maritime domain and the connection between insecurity at sea and onshore. The United Nations Office on Drugs and Crime (UNODC) provides funding to Stable Seas to continue its valuable work. There are many similarities (and relationships) between maritime security and oil theft, not least because piracy is one of the mechanisms for committing oil theft crimes. There is also much similarity in underlying issues, methods, and drivers behind these syndicated criminal activities. Stable Seas' methodologies could well be applicable to targeted approaches to preventing and countering oil theft across its supply chain.

3 Cyberattacks on oil infrastructure

Not all cases of oil theft/piracy involve physical actions. Increasingly, thefts using cyber methods are posing a major global threat. Some 2,000 cyber-ware attacks are estimated to have occurred in the USA alone in 2020—many related to oil and gas systems.

A most significant example of this was on Friday 7 May 2021, when a cyberattack on the Colonial pipeline in the US resulted in the temporary shutdown of this nationally critical infrastructure. The Colonial pipeline system (Figure 10) transports in excess of 100 m gallons per day of gasoline, diesel, and jet fuel from Houston to New York Harbour over a distance of 5,500 miles. This equates to no less than 45 per cent of all fuel consumed on the US East Coast. The hack caused one of the largest energy supply disruptions in US history. The incident involved ransomware, a scheme in which the infrastructure is digitally hijacked, with malicious software blocking use of the system until money is paid to the attackers. Payments are usually made in cryptocurrency. Such attacks can be highly disruptive and costly, particularly when there is no alternative way to operate the infrastructure following a hijacking that could mitigate the impact of the encryption (Stracqualursi et al. 2021). Two days after the attack occurred, the US passed emergency legislation to relax requirements for fuel transported by road and by ship.

Figure 10: Colonial Pipeline terminal, East Brooklyn, Baltimore, Maryland

Source: image by Orbital Joe, taken on 30 May 2005, reproduced from Flickr.com under CC BY-NC-ND 2.0.

The DarkSide criminal group is suspected to have been responsible for the attack. DarkSide follows a double-extortion trend, using 'cryptoware' that not only encrypts the victim's data and makes it unusable but also exfiltrates[9] a copy of the data and threatens to make it public if the group does not get paid. This professional organization treats its ransomware operation as a 'ransomware-as-a-service' (RaaS) business model, providing training and a software toolkit to affiliate franchises in return for a share of their earnings. It even has a 'code of ethics' on its website on the dark web, detailing who it will not attack and how it establishes the pricing for its 'services' (Russon 2021). Similarly to physical oil theft syndicates, cybercriminal organizations such as DarkSide work with other organizations, including 'access brokers', who provide them with harvested login details of user accounts of organizations to be targeted with ransomware. After six days of shutdown, the Colonial pipeline company had paid the DarkSide group US$4.4 m and pipeline operations restarted on 12 May (Eaton and Volz 2021). An alleged US$5 m ransom had been demanded. Contributing to the decision to end the hijack was panic buying by consumers who were concerned about product shortages; and the critical shortages across fuel stations triggered by their fuel hoarding.. In the six days of the pipeline hijack, 68 per cent of gas stations in North Carolina ran out of fuel; in Georgia, 49 per cent; in South Carolina, 52 per cent; in Virginia, 54 per cent (Volz et al. 2021). Lack of redundancy in the supply chain further adds to the effectiveness of cyberattacks on energy infrastructure.

In addition to oil pipelines, gas pipelines are very vulnerable to cyberattacks. In 2020, the natural gas pipeline grid supplied about 40 per cent of US electricity generation. Gas storage in case of upsets is limited to the inventory of compressed gas in the pipeline (known as 'line pack'). Profit-

[9] Data exfiltration is a form of a digital security breach that occurs when an individual's or company's data is copied, transferred, or retrieved from a computer or server without authorization (Lord 2018).

focused criminals select the most sensitive, high-value, and continuity-of-supply-critical systems for their ransomware attacks (Greenberg 2021). Energy systems are particularly attractive targets as the (socioeconomic) cost of a crippling power disruption significantly outweighs the cost of paying the ransom. Most ransomware cases are never publicized and the ransom is paid. For high-value targets, specific designer malware code is created that evades early detection and prevents recovery (e.g. by logging victims out of the system and changing user and administrative passwords, thereby disabling network servers and isolating affected computers) (Goud 2019). Another factor in attacking and disabling critical energy infrastructure involves fuel price trading schemes based on prior knowledge of the disruption.

On only a few occasions has digital malware specifically targeted industrial control systems. When this has happened, state actors have been the main suspects. In 2011, for example, 'Stuxnet' was deployed as a digital weapon to destroy uranium-enriching centrifuges at Natanz in Iran (Zetter 2014). In 2016 'Crash Override' caused a short power blackout in Ukraine, but further analysis revealed that the intent of the cyberattack was to establish the circumstances to create an unsafe, potentially destructive scenario within Ukraine's power transmission equipment (Slowik 2019).

Cybercriminals, noting the potential to hijack digital-physical infrastructure for financial gain, have sometimes modified and further developed malware developed by state actors. 'Hermes', a ransomware program originally developed by the North Korean state-sponsored Lazarus Group, was further developed by cybercriminals into a new improved version, 'Ryuk' (Constantin 2021). Ransomware such as Ryuk is deployed in a very targeted manner against selected assets to gain control of critical infrastructure. The entry point for these hacks generally involves emails, personal computers, and administrative IT systems. However, once access is gained the criminals explore the victim's operational technology (OT) network to gain access to operation control systems and physical assets in order to be able to inflict material damage. It is therefore not coincidental that these criminal groups use malware developed by state actors that was designed specifically for this purpose. DarkSide shows affiliation with countries of the former Soviet Union, as it checks the language on the targeted system and aborts encryption if it matches those of any of these countries (Cybereason 2021).

In 2019, Ryuk was used against US Coast Guard critical process control monitoring systems (Cimpanu 2019), before it was redirected to attack a gas compression facility of a US gas pipeline operator in 2020 (Cimpanu 2020). A ransom payment was demanded. When the pipeline operator no longer had system and data access for safe operations, it decided to shut down operations for two days as a precaution and to avoid incidents. Although the attack occurred in a single gas compression station, the whole pipeline had to be shut down due to system dependencies. Similarly, the maritime industry (including petroleum tankers) is very exposed to cyberattacks, and modern forms of oil piracy can exploit these weaknesses for the benefit of oil-cybercrime syndicates (Wagstaff 2014). Already by 2011, the vulnerability to cyberattack of global oil supply had been revealed (Fineren 2011). In 2014, the British government estimated that the cost to UK oil and gas companies from cyberattacks was US$672 m per year. Most cybersecurity incidents are kept quiet, and therefore the true exposure currently is likely to be much higher. A further risk will occur when in the future cybercriminals extend their access to programmable logic controllers (PLCs), devices, and sensors that are even more deeply embedded in the victim's operations network. Corrupting decentralized PLCs, of which there are many, would allow criminals to interact directly with factory equipment (CISA 2020).

Cyberattacks against industrial assets have been steeply on the rise since 2019. In March that year, Norsk Hydro was hit with ransomware, affecting its 35,000 employees across 40 countries and with an ultimate financial impact of US$71 m. Norsk Hydro is one of the world's largest aluminium companies. Malware first entered a company personal computer via a Trojan-software-loaded

attachment to an email from a trusted customer. From there, the hackers were able to quickly invade the IT infrastructure and plant the ransomware. By the time the Trojan software was discovered by antivirus systems, it was already too late and most of Norsk Hydro's IT infrastructure was under the control of the hackers. 'LockerGoga'[10] ransomware then spread through most of Norsk Hydro's company network. Its aluminium smelters and production facilities were brought offline and production was halted. However, Norsk Hydro made three key decisions to counter the attack (Briggs 2019):

- no ransom would be paid;
- they would provide complete transparency about the attack;
- they would engage cybersecurity experts (in this case Microsoft's Detection and Response team, DART) to help restore operations.

Norsk Hydro's response sets an industry standard for how to respond to a successful cyberattack. By going public, it prevented similar attacks on other companies. Furthermore, after its system was infected, Norsk Hydro needed to fully clean and rebuild the software and data systems anyway. The infected system (which had a secure backup) had therefore become of limited value. Finally, there was no guarantee that the hackers would or could fully restore the IT system without any remaining errors. Several key lessons resulted from the Norsk Hydro attack and similar incidents:

- have emergency response procedures in place to deal with cyberattacks at all levels in the company (individual, plant operational, IT, corporate, etc.);
- maintain a safe capability to take manual control of the system and to maintain business continuity if the IT system is no longer reliable or available: this is particularly important if an unexpected loss of power can instantaneously compromise the safety of production processes or cause uncontrolled emissions;
- alert all employees to the treatment of cyberattacks and provide training to recognize phishing events and malicious attachments;
- implement multi-factor authentication processes for digital access to the network;
- maintain a segmented, multi-domain digital system architecture with firewalls to mitigate against a potential spread of a digital attack;
- maintain digital separation between an organization's IT network and its digital OT network;
- disable the ability to connect any unapproved devices to the company network;
- regularly back up data on separate secure systems;
- stay informed on changing threats and digital attack practices.

The Ransomware Task Force (RTF) calls ransomware 'no longer just a financial crime; it is an urgent national security risk that threatens schools, hospitals, businesses, and governments across the globe' (IST 2021). The organized actions of cybercriminals follow similar patterns to those used by oil theft crime syndicates:

- Criminals focus on vulnerable infrastructure, exploiting technical/operational gaps in administration (IT) and operations (OT) systems.
- They are able to gain access to or work as insiders, to learn the victim's methods and weaknesses before striking.

[10] The same ransomware attacked a number of other industrial firms, including Altran Technologies, Hexion, and Momentive. It is also thought to have been used in the Colonial pipeline system attack.

- Work practices focus on the ability to repeat the same crime multiple times rather than striking just once. The negative impact on victims of each event is designed to be 'bearable', such that the same system weaknesses can be exploited repeatedly.
- Criminals work transnationally, exploiting limitations in countries' jurisdiction to cover their tracks and avoid prosecution.
- They are organized as a business, with formalized commercial structures as well as loose affiliations.
- The organizations often hide in plain sight, being protected by powerful actors or as extensions to legitimate businesses.
- Criminal work practices evolve continuously and respond proactively to stay ahead of law enforcement measures, which have to play catch-up with the criminals.

Ransomware criminals make themselves known once they have positioned themselves firmly in the victims' systems, while oil theft can go unknown (unless infrastructure is hijacked). However, similarly to oil theft, the secrecy and stigma associated with ransomware attacks make it extremely difficult to get a true picture of the number of attacks, the costs, and the patterns in assets targeted. The FBI estimates that 2,400 ransomware attacks happened in the US in 2020, a steep increase from the year before. The global cost of ransomware in 2020 is estimated to have ranged from US$42 bn to US$170 bn, with two-thirds of victims admitting to having paid part or all of the ransom (Tidy 2021). RTF's comprehensive report recommends 48 actions to combat ransomware threats and includes the following priority recommendations:

- designate ransomware attacks as a national security threat;
- make it mandatory for victims to report if they do pay criminals;
- create a 'response and recovery fund' to support ransomware victims and help them recover;
- increase regulation of cryptocurrency services;
- exert pressure on nations which are complicit, or which refuse to act against domestic ransomware groups.

Energy infrastructure, such as ships, ports, oil, gas and fuel pipeline systems, and refineries, are soft targets for ransomware and are deemed to be less well protected than electrical power plants and distribution networks. However, an interruption of fuel or gas supply also has the ability to knock out power facilities or impair other socioeconomic activity.

4 Gaps in addressing oil theft

Oil theft has proven to be persistent and resilient against law enforcement measures. It exploits weaknesses in petroleum infrastructure, processes, and organizations, as well as weaknesses and gaps in regulations, law enforcement capacity, and jurisdiction. This section discusses a number of examples that illustrate key gaps in tackling oil theft:

- oil theft information gaps;
- gaps in national and international collaboration to counter oil theft;
- oil theft law enforcement, jurisdiction and other judicial gaps;
- gaps in community support to stop oil theft.

4.1 Basic information on oil theft is lacking

Informed solutions to confronting pervasive oil theft problems require basic data that are mostly lacking. Systematic, comprehensive, and holistic data gathering and analysis are needed to expose, understand, and address the interconnected nature of oil theft challenges. These include:

- **How much oil is produced and how much is stolen?** This requires information on illegal oil pipeline taps, the location, number, and volumes siphoned, and the number and capacity of artisanal refineries. Information is also needed on legal and illegal bunker operations, the number and capacity of legal and illegal (converted) tankers, fuelling patterns, and volumes at legal and illegal bunker locations. Hence, there is the additional complexity that legal and illegal operations and assets overlap: legal tankers bunker illegal oil; legal volumes and transactions are adulterated or blended with illegal oil; and legal oil volumes are misappropriated through defrauded metering.
- **How is stolen oil transported and traded?** A fraction of the stolen oil is processed and used in the domestic market (Figure 11), another part is smuggled to neighbouring markets, and the remainder is exported and sold legally on global markets. Again, criminals exploit the blurring between legal and illegal activities to launder stolen oil into the commercial market. Options for storage, inter-tanker transfers, crude blending, trading of ownership, etc. provide many pathways to obscure the trail of stolen oil. Information on transport should include global geographies. For example, export markets that have reportedly received stolen crude volumes originating from Nigeria[11] include the United States, Singapore, Thailand, Indonesia, Brazil, China, and the Balkan states (Katsouris and Sayne 2013).
- **How are illegal oil financial transactions conducted?** Oil thieves have options to launder the profits of their illegitimate activities through cash transactions, offshore banks in tax havens, use of shell companies, intermediaries, bribing bank officials, cryptocurrencies, overseas purchases, etc. In Nigeria, proceeds from overseas sales of stolen oil are often imported as cash. Disparities in oil pricing policies and subsidies provide incentives for oil smuggling. More research is needed into the economics of oil smuggling.

Figure 11: Illegally produced diesel is transported to market in recycled drums on Cotonou boats

Source: images by Stakeholder Democracy, taken on 15 and 18 November 2012, reproduced from Flickr.com under CC BY-NC-ND 2.0.

[11] Structural differences between reported Nigerian export figures and import figures from the above countries suggest that stolen Nigerian crude is purchased and transferred to overseas commercial markets.

4.2 International efforts to counter Nigeria's oil theft are lacking

Internationally, the flagrant oil thefts in Nigeria and other countries have been largely ignored. Although there are important international aspects of this illegal trade, such as bribery, money laundering, environmental damage, and the involvement of militant/extremist organizations, there have been few specific programmes to counter global oil theft, including in some of the ways mentioned in the previous sub-section. The concerted international stance against the wave of piracy in Gulf of Guinea since 2016 (see Section 2.4.2) has been the most decisive action from the international community to date. While pirates initially targeted mainly tankers for their cargo, they now persist in pursuing a kidnapping business model. However, actions against oil tanker piracy address only a small segment of West Africa's oil theft. There are at least four key reasons for the low priority that the international community seems to give to actions against oil theft:[12]

1. It is seen as a domestic problem (mistakenly, as oil theft compromises the integrity of foreign markets and international financial systems).
2. The secretive and violent characteristics of this illegal trade render very difficult any intelligence-based action.[13]
3. The transnational organized crime networks involved are too flexible, mobile, creative, and diffuse to easily cut the illegal oil trade.
4. Government officials are unenthusiastic about doing anything substantial to disrupt the illegal trade.

In view of these complexities, a Chatham House study into Nigeria's oil theft resulted in the following key recommendations (Katsouris and Sayne 2013):

- Nigeria and its prospective partners should prioritize the gathering, analysis, and sharing of intelligence.
- Nigeria should consider taking other steps to build the confidence of partners.
- Other states should begin cleaning up parts of the trade they know are being conducted within their borders.
- Nigeria should articulate its own multi-point, multi-partner strategy for addressing oil theft.

Oil theft is a multifaceted and multidimensional global phenomenon. Siloed and geographically singular approaches to countering it are unlikely to be effective, as theft syndicates demonstrate flexibility, change location and practices, and target different parts of the oil supply chain.

4.3 Closing law enforcement and judicial gaps in the fight against Mexico's oil theft

Mexico is a textbook case of enforcement swamping:

> If enforcement resources are constrained, the expected value of the penalty facing potential violators falls as the frequency of violation rises. Thus, trends in rule-breaking will tend to be self-reinforcing … The search for 'root causes' of high

[12] For example, oil theft costs Nigeria US$12 bn per year in lost product and much more in environmental and socioeconomic damage (Romsom 2022).

[13] Local legitimate businesses that may be 'in the know' generally do not want to share information for fear of repercussions. In this shady business, there are not only the violent criminal gangs to worry about. Anonymous government officials, critical to business continuity, may run or benefit from illicit schemes on the side.

> violation rates may therefore be in vain. Enforcement policies, especially against illicit markets, should be designed with this phenomenon in mind. (Kleiman 1993)

The ability of oil theft syndicates to flexibly adapt theft operations and the availability of a large number of individual theft points (see Romsom 2022: section 4) make law enforcement activities to counter oil theft very labour-intensive and often ineffective. Moreover, the theft of oil, which is a widely available and relatively low-cost commodity, may attract only low penalties under the code of law. Compared with high-value and illicit items, such as drugs and weapons, oil theft generally ranks lower on the law enforcement priority list. However, it is the scale of oil theft as a business that sets it apart. For a theft syndicate, the aggregated annual value can run into the hundreds of millions of US dollars. In 2016, the top three oil theft cartels in Mexico committed oil theft with an annual value of US$372 m, US$212 m, and US$187 m respectively. In 2018, Mexico's annual oil theft was estimated at 81,000 bpd from more than 12,500 illegal pipeline taps, and valued at US$3 bn (Semple 2019). Furthermore, oil theft should be a much higher priority for law enforcement because its proceeds are used to finance other organized crime activities and it triggers violence against the community and in crime-on-crime actions (see Romsom 2022: box C and section 4.3).

As an alternative to focusing on individual oil theft activities, Mexican law enforcement has targeted the organizational structures of the crime syndicates. However, efforts to curb the influence and power of the cartels by taking out their main leaders and to precipitate infighting among cartel organizations backfired when they resulted in the destruction of the cartel hierarchy. The most aggressive and violent factions within the cartel organizations reacted by causing even more violence and committing more widespread criminal activities without the restrictions of a chain of command. Particularly for co-operative, relatively non-hierarchical crime organizations, taking out 'kingpins' causes these businesses to flexibly adapt, reorganizing their 'cell structures' and creating new opportunistic allegiances between cells and sometimes across crime groups.

Crime syndicates, and the crimes themselves, are often transnational, exploiting gaps in jurisdiction to avoid getting caught. However, some convictions in US criminal cases, involving oil stolen from Pemex and imported to the US, indicate that successful verdicts could be achieved by proving other related crimes, e.g. tax evasion, bribery, extortion, money laundering, conspiracy, obstruction of justice, perjury, or participation in an organized criminal group. Several other factors have contributed to successful cases, such as witness protection programmes and, first and foremost, good cross-border co-operation among law enforcement agencies. Nevertheless, preventing oil theft is even more effective if legal efforts are complemented by other measures, such as physical oil asset protection, targeted sanctions, supply-chain due diligence, etc.

Soon after taking office in December 2018, Mexico's new president Andrés Manuel López Obrador, elected on a wave of populist anger, declared action against fuel theft as his first priority to deliver on his promise to tackle crime and corruption and to reduce poverty and inequality. Mexico, in the thrall of extreme violence committed by criminal cartels, was ready for change. A particularly damaging pipeline attack had spilled 36,000 barrels of gasoline and triggered a wave of government reactions. Federal security forces were mobilized to protect Pemex fuel assets (including pipelines) and also to provide a sense of security to local populations. An all-out campaign saw the arrest of thieves and complicit Pemex employees. Accounts were frozen and property seized. To break the huachicoleo,[14] pipelines that had the most illegal taps were shut down despite the local fuel shortages this caused. Following an illegal tap into a gasoline pipeline

[14] Mexico's oil theft is so pervasive that it has its own name (see *Yucatan Times* 2019).

that was blamed on the shortages (Barrera 2019), an explosion occurred on 18 January 2019 and ultimately killed at least 137 people among a crowd that had gathered with containers to collect free fuel (Harrup and Whelan 2019). By May 2019, within four months of the start of President López Obrador's anti-fuel theft campaign, the amount of oil theft had reduced by 95 per cent, from 81,000 to 4,000 bpd.

However, the battle against the huachicoleo is a long-term effort, with criminal organizations able to wait it out for security forces to stand down or to once again change their business model. Since 2019, fuel crime has literally gone underground. Exploiting their skills in digging tunnels for drug smuggling, cartels now drill tunnels also for oil theft and to evade the regular patrols of security forces. In April 2021, the authorities found a tunnel system in a suburb north of Mexico City. It was one of several recently discovered to tap fuel pipelines and store stolen fuel in plastic containers in underground warehouses. The tunnel system was discovered when one section collapsed and a tap was left open. Four other tunnels were later discovered in the same area. More tunnel systems were discovered elsewhere in the country. These tunnels are designed as permanent infrastructure, with ventilation and electricity. The siphoning systems are exceedingly advanced, such as utilizing a double tap system also deployed in Nigeria (Romsom 2022: section 4.1.1). These oil theft schemes have become highly professional and industrial, being technologically and resource intensive and requiring investment to build the necessary infrastructure. According to Pemex, in December 2020 oil theft was still relatively low, at 5,600 bpd (Zuza 2021). There also appears to have been a shift in the crime business model, with the focus moving from large-volume oil theft to kidnapping, extortion, and equipment theft (Argus 2020b). Also, armed attacks on Mexico's offshore oil and gas infrastructure and vessels have risen to high-risk levels. In the first four months in 2020, 14 cases of armed offshore attacks were documented, although only three of these were reported to international maritime agencies (Argus 2020a).

4.4 The battle to win hearts and minds

The next phase of the fight against oil theft in countries such as Mexico and Nigeria must include a sustained campaign by their governments for the hearts and minds of the local population, to break their support for the fuel thieves. By offering employment and cheap or free fuel, giving gifts, and providing community services such as paying for healthcare, the Mexican cartels have embedded themselves firmly in local communities. The government is in fierce competition for the loyalty of its citizens and has to convince many parts of society that have felt neglected under successive regimes which were unable or unwilling to provide basic services or opportunities for local development. Increased alignment and co-operation between federal and local government entities are necessary to create a foundation for sustained local development.

The situation in Mexico is similar to that in the Niger Delta, where local communities support and protect criminal groups that provide them with discounted fuel, because official fuel distribution in rural areas is inadequate. The fuel theft business also provides locals with jobs and income. Oil theft criminals leave pipeline taps flowing to allow farmers to collect fuel. Mexican farmers are compensated for spills on their land that caused property damage. There is an underlying 'hearts and minds' approach to maintaining the loyalty of local communities to the criminal groups. Collusion between criminal groups and law enforcement compounds this and adds yet more obstacles in countering oil theft. Criminal proceedings against law enforcement and security personnel are rare. One counter-measure taken by Pemex is to stop pipeline transport of engine-ready fuel and instead execute the final fuel mixing at storage sites that can be better protected. However, in response, the cartels now focus increasingly on hijacking fuel tankers that distribute fuels to filling stations.

In Nigeria, fuel subsidies have been a longstanding means of providing rural communities and the poor with discounted fuel. However, corruption and the abuse of fuel subsidies has been a major problem. In 2011, Nigeria's Petroleum Support Fund was defrauded out of US$6 bn (Romsom 2022). Although community financial support is instrumental for the government to win back its role, fuel subsidies are too untargeted an instrument to be cost-effective. As part of the measures taken by the Nigerian government to strengthen the fiscal sector in light of the fallout of the COVID-19 pandemic, fuel subsidies were removed in the revised 2020 budget. Apart from attracting corrupt practices, the subsidies had largely benefited households with higher incomes. The IMF advised the Nigerian government on other more targeted social spending measures to support the poor at a fraction of the cost (IMF 2020). The removal of fuel subsidies is also expected to have a significant impact in countering fuel smuggling and round-tripping (exporting and reimporting the same fuel).

The long-awaited Nigerian Petroleum Industry Bill was approved by parliament in July 2021 (Gupte 2021). It proposes to separate the regulatory from the commercial functions of the Nigeria National Petroleum Company (NNPC). The setting up of two new independent regulators is proposed. Going forward, it will be essential to strike the right balance between independence and accountability, while ensuring data and information sharing between regulators and relevant ministries and agencies. For transparency and accountability purposes, adhering to the principle that all petroleum sector revenues, including royalty, taxes, government profit oil share, and dividends, should flow through the Federation Account will be important and helps to reduce vulnerability to corruption (IMF 2020). This will provide additional fiscal resources for the Nigerian government to help communities.

The 'moral economy' logic, whereby oil theft is seen as an entitlement of local communities (Figure 12) and other stakeholder groups to their share of the resource, carries perhaps the greatest cost of all. In an extensive study by Chatham House published in 2013, criminal groups often described their own activities as economically rational, politically necessary, morally defensible, and socially productive (Katsouris and Sayne 2013). A foundational solution to the problem of crude theft and artisanal refineries is the provision of local electricity and fuel to communities, which could trigger increased economic activity and reduce the demand for illicit and poor-quality fuel. However, measures against oil theft need to both address the risk of occurrence (prevention) and seek to mitigate the consequences of oil theft for peoples' lives and the environment (such as local violence and pollution) (Romsom and McPhail 2021a, b).

Figure 12: Makeshift fuel filling station in Nigeria

Source: image by Akintunde Akinleye for Canal C, taken on 27 November 2012, reproduced from Flickr.com under CC BY-NC 2.0.

5 A multidimensional approach is needed to break the economy of oil theft

As this paper has shown, oil theft is engrained in the energy supply chain, to a degree that it is being priced in routinely as a cost by traders and considered accepted petty theft by shipping companies. Oil theft is conducted as a business (oil-theft-as-a-service), often with intent to escape discovery, so that similar thefts can be repeated many times over. Crime syndicates are highly organized and often represented as legitimate businesses that use their infrastructure, processes, and knowledge to commit theft. Stolen crude oil and fuel can disappear without trace, either traded on the international commercial market or absorbed into the local black market (Figure 13). Crime syndicates and the crimes themselves are often transnational, exploiting gaps in jurisdiction. Crime syndicates quickly adapt their business practices when law enforcement becomes more effective. They evolve from ship piracy to stealing tanker cargoes to kidnapping tanker crews; from physical ransom of assets to digital ransom via ransomware.

Figure 13: Hong Kong-flagged oil/chemical tanker *Lighthouse Winmore*, seized in Yeosu, South Korea

Note: the *Lighthouse Winmore* was seized by the South Korean government in December 2017 on suspicion of violations of UN sanctions; it is alleged that the tanker was involved in illegal STS transfers, including 600 tonnes of oil to the North Korean vessel *Sam Jong 2*; around the same time, the tanker *Koti* was also impounded by South Korea on suspicion of illegal STS transfers (Lee 2019).

Source: image by EZEK, taken on 4 June 2018, reproduced from Flickr.com under CC BY-ND 2.0.

Acts of oil theft are also so pervasive and differentiated that no single measure is adequate to break the cycle. Oil thefts of all types should be targeted as illegal businesses, rather than illegal acts. Successful efforts deployed against other types of international crime organizations should be reviewed to assess their applicability and effectiveness against oil theft. The exposure of an oil theft crime is unlikely to bring down the oil syndicate responsible. The thieves that are caught in the act are often expendable from the syndicate's point of view, and the money flows and profits remain hidden. The fight against oil theft has much in common with the global 'war on drugs', but oil theft is more complicated, as it involves a product that is a legally traded commodity.

5.1 Commonalities in oil theft

The research presented in this and the previous working paper has revealed the following commonalities in oil theft:

1. Oil theft organizations work as transnational crime syndicates, with hybrid structures that are in part hierarchically organized and also built around loose allegiances and associations. **Organizational cell structures** (similar in design to those of terrorist organizations) are robust against being compromised. Taking out established oil theft kingpins often leads to the creation of new opportunistic allegiances between cells and across crime groups, and causes even more violence as factions in the syndicate reposition themselves. Oil theft crime syndicates are diversified, with collaborators across fuel traders, shipping companies, third-party fuel inspectors, oil company personnel, and government officials.

2. Oil theft criminals **exploit transnational aspects of their crimes**, such as gaps in jurisdiction, to hide their activities and increase their profit margins (e.g. price arbitrage due to cross-border differences in taxation and fuel subsidy regimes).
3. Oil theft is prevalent because its **business model is to replicate a similar oil theft** repeatedly. It does so by (mostly) avoiding detection, or even through the deployment of a franchise model for digital ransomware organizations. Law enforcement generally focuses on the theft act, but catching oil theft criminals in the act generally does not compromise the replicability of the crime. When a theft is detected, the organization quickly covers its tracks, adapts its geography or execution strategy, and continues its business.
4. Oil theft syndicates can **adapt crime execution strategies and even switch their business models** very quickly. Capital invested in existing oil theft schemes is easily redeployed. When limited law enforcement capacity focuses on a certain theft practice, crime organizations adapt, e.g. from hijacking oil tanker cargoes to kidnapping tanker crews, from crude oil theft to fuel theft, from local black-market fuel distribution to fuel smuggled in bulk across states, from smuggling on land to smuggling by ship tanker, from 'cappuccino bunkers' to tampering with MFM meters. Cyberattacks, growing in scale, number, and sophistication, substitute or complement physical crimes. Oil and maritime infrastructures are critically exposed to cybercrimes and ransomware.
5. Oil theft organizations are **linked to other crime businesses**, such as arms trafficking, extremism, and state actors that offer protection and opportunity. Mexican criminal cartels switch focus flexibly between drugs trafficking and oil theft, depending on the deployment of limited law enforcement capacity. This allows oil theft organizations to 'wait it out' until the deployment of security and law enforcement is reallocated over time. Some skills, such as the ability to build complex tunnel systems, are being repurposed, e.g. from drugs smuggling to conducting underground illegal pipeline taps.
6. Oil theft crime syndicates extend their reach and influence by **buying allegiances, support, and information** through bribes, profit sharing, and extortion. Complicity is through active support (e.g. government security forces protecting oil theft sites) as well as passive (e.g. not inspecting ship cargoes that pass checkpoints). The extended oil theft syndicates are highly covert and it is often not clear who is and who is not involved, even at very high levels in government and legal businesses. Oil theft reaches the boards of petroleum-related companies, the service industry, and the financial sector.
7. Oil theft **contaminates legal oil markets and financial markets**. Crime syndicates work under cover of and with the support of legal businesses. Insider jobs obscure how much of the organization is involved. Complicit fuel tanker and bunkering crews are known to have been instructed by their senior management to commit their illicit acts, as in the case of the large fuel thefts at the Shell Bukom refinery in Singapore. Stolen oil is sold by traders on legal markets. Banks unwittingly finance fraudulent companies and transactions.
8. Oil theft activities often **mix legal commercial operations with illegal activities**, such as simultaneous operation of commercial fuel delivery with illegal theft; use of commercial tankers to transport stolen fuel; the blending of stolen crude oil with legal cargoes in STSs, and the blending of smuggled or untaxed restricted fuels with legal fuels. Even the businesses 'ethics', 'customer service desks', and donations to worthy causes of certain ransomware crime organizations contribute to the perception of legality.
9. Exposure to oil theft causes **unforeseen collateral damage to the legal economy**. Discovery of related corruption, fraud, and other malpractices of bunker fuel companies and rogue traders subjected Singapore to a string of bankruptcies and over US$6 bn in unpaid debts to suppliers, traders, and banks not involved with these crimes.

10. Oil theft and related insecurity have substantial negative effects on the economic activities of developing countries. Whether countries produce oil or not, **government tax income is directly impacted** (see earlier example of Benin in Section 2.4.2).
11. Overall, the hidden costs of oil theft substantially exceed the value of the oil that is stolen. A key loss to developing economies is **lack of business confidence and underinvestment**. In Nigeria, the oil capacity shut-in and oil being deferred is more than twice the amount of oil estimated to be stolen. The annual loss in petroleum profit tax alone exceeds US$20 bn, 63 per cent of the total government tax revenue of US$32 bn in 2019 (IMF 2020).
12. In addition to the violence, the loss of resources, and the destruction of the environment that oil theft causes, arguably the biggest potential loss to developing countries is the **loss of loyalty of the people to their government**. Loss of taxable income impairs a government's ability to take care of its people and stimulate local development. As governments compete for the 'hearts and minds' of their citizens, oil theft criminals describe their illicit acts as economically rational, politically necessary, morally defensible, and socially productive (Katsouris and Sayne 2013). In this 'moral economy', the loyalty of communities is being bought by oil theft syndicates, as locals are roped in to their destructive schemes. This runs the risk of contaminating people's mindset and criminalizing other sectors of the economy.

5.2 International solutions to counter oil theft

International solutions to address oil theft can be categorized into the following three areas: stolen oil volumes, stolen oil transport, stolen oil money:[15]

5.2.1 Stolen oil volumes

- The existing technology for crude oil fingerprinting limits its applicability to stopping theft and prosecuting those accountable. However, **designer tracers or markers for crude oil and fuels** do show promise and are increasingly being successfully deployed in a number of locations.
- **Protection of pipeline systems** exposed to potential illegal taps can be improved through technologies such as pipe-in-pipe lines, fibre-optic sensors, drone surveillance, and pressure-drop-controlled flow stations. These provide a combination of early warning and early intervention to minimize thefts and spills.
- In combination with **improved metering technology**, such as the use of MFM, measures to avoid meter tampering and improved onboard fuel and cargo management systems, the ability to conduct malpractice can be significantly restricted. Similarly, digital technologies can assist in making fuel inspections by third-party surveyors tamperproof. Singapore's mandatory SS 648 standard prescribes the use of MFM for bunkering operations and is the first of its kind in the world (MPA Singapore 2019).
- Singapore's implementation and enforcement of obligatory standards to prevent fuel theft during bunker operations, is recommended for adoption by other bunker ports. Over the last 20 years, Singapore has developed and implemented a number of **standards across the entire value chain for bunkering**—from standards on bunkering procedures to

[15] These three basic areas extend into the digital domain, such as the digital hijacking of oil transport infrastructure and digital payments through cryptocurrency.

increasing transparency and reducing disputes, to the use of new technologies on mass-flow metering, which helps to increase efficiency.[16]

- Singapore's **enforcement practices in trading and fuel bunkering operations** provide a framework for an aspiring global standard. Public revocation of bunker licences by the port authority and prosecution in courts of illegal practices provide a deterrent to others.
- **Practice-sharing of oil trading and bunkering regulations** and enforcement thereof among nations' regulators can promote best practices that are tailored to local situations.
- Data analytics, drone inspections, satellite imaging, remote radar detection, and other information gathering and processing technologies can assist in **discovering oil theft patterns** with the aim of preventing theft.
- **Transparency on oil theft crimes** (such as by SPDC, the Shell Petroleum Development Company of Nigeria, on oil spills, ReCAAP on oil tanker attacks, and Colonial pipeline on the recent cyberattack) allows other potential victims to stay informed on changing threats and criminal practices. The rise in insurance premiums related to oil theft is an obstacle to transparency.

5.2.2 Stolen oil transport and trade

- Appropriate mechanisms for **domestic fuel pricing policies** and abolishing fuel subsidies inhibits incentives for fuel smuggling, as price differentials are removed. They also have the advantage of being in line with evolving carbon-reduction agendas. Cross-border fuel price equalization reduces transnational demand for smuggled fuels. However, this may not stop the concealment of stolen fuel through illegal exports.
- If the number of roads or water ways is limited, **targeted checks can be instigated at strategic oil theft choke points** to catch illegal tanker truck or barge transports of stolen oil. However, thieves may move their point and mode of transport if such alternatives exist.
- **International maritime co-operation** between domestic navies and international naval forces has significantly improved presence and response times in piracy-prone seas. Consequently, the global hijacking of oil tankers for their cargoes has been significantly reduced since 2016. An STS transfer of crude or fuel cargo from a hijacked vessel to a pirate's mothership may take 24 hours. Rapid response forces are now able to respond within a fraction of that time period. Instead, pirates have become more interested in the kidnapping of international tanker crews as a business model, allowing them to spend much less time on board. Besides the difficulty of catching pirates 'in the act', there are legal hurdles to halting ships and impounding vessels and more work can be done to make existing frameworks and processes more effective.
- Commercial-class oil tankers that wait offshore but do not dock at any oil export terminal can be a tell-tale sign of illegal oil loading. STS transfers are commonly used to obscure the evidence of oil theft. These activities can be spotted when vessels are in proximity for a period of time. Such vessels can be intercepted during STS activity or later inspected for cargo contents.
- To avoid detection, ships involved in illegal oil loading will switch off or tamper with their AIS transponders, so ship registration of AIS must be enforced. However, jurisdiction to act can be a limited under maritime law. A sudden loss of transponder signal is easily

[16] Singapore's current bunkering-related standards and technical references are as follows: SS 600: 2014 Code of Practice for bunkering; SS 648: Code of Practice for Bunker Mass Flow Metering (MFM); SS 524: 2014 Specification for quality management for bunker supply chain; TR 56: 2017 Technical Reference for LNG bunkering.

detected and a clear sign of abnormal conduct. The manipulation of ship transponder signals should attract steep penalties, including barring of such ships from ports.

- **Data analytics on ship transponder signals** provide detailed information on ships' movements, and software automation can assist in identifying those vessels most likely to be involved in illegal oil trades. AIS monitoring can be complemented by other satellite detection, such as radar signals and other emissions from ships. Extending this information trail to include ports visited, bills of lading, bunker activities, vessel management and ownership, crew, etc. can provide detailed forensics on the illegal oil trade. However, Somali pirates have been known to hack into AIS signals to select vessels to target for hijacking;
- **Digital technology that limits the manipulation of data**, such as that deployed by Singapore for bunkering operations, removes potential sources of errors and falsification of records for fuel deliveries. Digital receipt systems for fuel supplies automatically generate official records between transfer meters and delivery notes without human intervention.
- Third-party independent surveyors are repeatedly caught in facilitating oil theft by falsifying records. **Third-party surveyor and certification** companies need to develop tamperproof business processes that avoid these reputation-damaging acts.

5.2.3 Stolen oil money

- **Stringent regulation of cryptocurrency services** is needed to break the criminal links with off-the-book payments associated with oil theft, cybercrime extortion, and tax avoidance schemes.
- **Anti-money-laundering activities** are very difficult to pursue for financial regulators in developing economies. However, many international banks have been 'educated' through recent public cases and 'encouraged' by steep fines. Hence, commercial banks should now be in a position to act as whistle-blowers if they observe signs of illegal fund transfers or money-laundering activities. The exclusion of criminal organizations from the international banking system would be a big step forward in avoiding the contamination of legitimate businesses with criminal oil theft profits.
- **Oil theft sanctions should be applied with precision**, and blanket sanctions (e.g. a general ban on a specified country's oil) should be avoided. In a manner similar to the US sanctions targeted at corporate entities and individuals involved with (state-sponsored) terrorist and criminal activities, the international community could act to ban banking, visas, and asset ownership, freeze assets, etc. for those involved in the illegal oil trade. Thieves should be placed on 'do-not-trade' lists and companies should be barred from offering theft networks goods and services (e.g. vessel insurance). However, for such targeted sanctions to be effective, many countries involved in the international oil trade would need to participate. Such sanctions could limit thieves' rights to travel, to obtain loans to fund their illegal business, and to access their (overseas) funds and financial assets and would also raise red flags at banks and trading partners. However, loopholes for culprits exist and shadow banking (cash transactions/cash smuggling, cryptocurrency) may limit the effectiveness of targeted sanctions.
- The financial sector funds oil trading and bunkering companies' liquidity requirements. Therefore, **financial due diligence** provides another key mechanism to protect the public's interest. However, this requires regulatory and legal systems to be effective in their duties, including bankruptcy and insolvency provisions.
- Digital technologies (such as the digital receipt system) can also assist with supply-chain due diligence to track the origins, transportation, and changes of ownership of oil cargoes.

Block chain technologies and non-fungible tokens (NFTs) can provide proof of authenticity of the origin and subsequent transactions of oil cargoes.

- **International courts and courts in countries other than where oil has been stolen** could play a more active role in holding criminal organizations and syndicates to account for the consequences of their illegal activities in the oil trade. At present, international oil companies appear to be targeted by foreign courts mainly for wrongdoing in developing countries. However, this sets a precedent for doing the same with regard to international criminal organizations that corrupt international oil markets and destabilize developing economies.
- **Prosecution for acts of bribery** also offers an opportunity for action. The transport of or payment for illegal oil could constitute a bribe under the US Foreign Corrupt Practice Act (FCPA) if government officials are involved in the transaction or shipment. Bribe charges could be raised for paid 'services' that facilitate oil thefts (through action or non-action).

In this list of possible actions, no single solution would prevent current pervasive acts of global oil theft. However, in combination these actions could certainly create significant hurdles to constrain crime syndicates from exploiting the enabling environments for theft; the facilitation, aiding, and abetting of corruption and fraud; and the exploitation of regulatory weaknesses and loopholes. Each country may emphasize different aspects in this repertoire of measures, depending on the local situation and progress already made to curb oil theft (see Box B). So once again, international co-ordination would be an important part of any holistic solution.

Among the above initiatives, financial due diligence has been much in the public eye and this relates to perceptions of transparency in commodity trading in general. The mobilization of international organizations and agencies to take a stronger stance against oil theft is greatly needed. The international maritime sector, through organizations such as IMO (IMO n.d.), ReCAAP, and Stable Seas, promotes a holistic approach to addressing piracy and armed robbery against ships. Its guidance and methodologies are likely to benefit efforts to counter other types of oil theft. As oil theft threats and practices change, particularly into areas of cybercrime and ransomware, specialist advice and support are increasingly important to protect energy installations and fuel supplies against disruption and extortion.

Box B: China's 'whole-of-government' approach to addressing illicit fuel, tax fraud, and air quality degradation

On 22 April 2021, the vice-governor of Guangdong (China), an oil company veteran, convened a meeting with government agencies and national oil firms to address the clampdown on illicit LCO trading and sales that were leading to substandard fuels and air pollution. The meeting came on the heels of the arrest by Guangdong police of several people, including two BP staff, for illicit trade and sales of LCO. What made the meeting remarkable was the 'whole-of-government' approach to addressing the problem of illicit fuels. Government agencies represented included environment, safety, quality inspection, customs, energy regulation, and tax administration. Also represented were shipping companies and fuel marketing specialists from national oil companies and state refiners CNPC, Sinopec, and CNOOC. Guandong is China's largest oil-consuming province and accounts for 40 per cent of China's LCO imports. LCO is a petrochemical feedstock that has similarities to diesel but is of inferior quality. As traders exploited a tax loophole, China's LCO demand grew by 360 per cent to 511,500 bpd in April 2021, compared with 142,000 bpd two years earlier. Because LCO was exempted from consumption tax (charged at US$29 per bbl) and can be used as a diesel substitute, fraudulent oil traders could make illicit profits through tax evasion and fuel price differentials. The unnaturally high LCO demand increase from China led to US$3.9 bn in avoided fuel taxes on an annualized basis. The whole-of-government clampdown aimed to address a combination of issues: illicit (non-quality-controlled) fuels, government tax evasion, and air pollution concerns. Starting from 12 June 2021, China imposed a consumption tax of US$37.50 on LCO, 27.6 per cent higher than the tax on gasoil and diesel. Using this fiscal instrument, the Chinese government was able to destroy the artificial demand for LCO and meet each of its objectives. However, a consequence of China's action is likely to be the systemic lower repricing of LCO in Asian markets. This, in combination with higher domestic fuel taxes, makes it more profitable for oil theft syndicates to smuggle low-cost LCO into the country and illegally blend it with legitimate fuels (Aizhu and Samanta 2021a, b; Zhou 2021; see also Romsom 2022: section 3.1.1).

The application of technology, such as satellite monitoring, drones, digital surveillance, molecular tracers, and data analytics, is another key component in countering oil theft. Information sharing and capacity building by technology partners are essential to close information gaps on stolen oil volumes, transport, and money flow. Box C provides an overview of some of the organizations that could be instrumental in mobilizing international concerted action against oil theft.

Box C: Organizations instrumental in mobilizing international concerted action against oil theft

The following organizations have valuable knowledge and expertise that could support capacity building and mobilizing international action against oil theft:

Global organizations

- UNODC—United Nations Office on Drugs and Crime
- UNCTAD—United Nations Conference on Trade and Development
- UN Global Compact
- IMF—International Monetary Fund
- TRACIT—Transnational Alliance to Combat Illicit Trade (NGO for corporations and select trade associations committed to mitigating the economic and social impacts of illicit trade)
- Basel Institute on Governance (its International Centre for Asset Recovery is dedicated to strengthening and supporting the capacity of developing and transition countries to recover stolen public assets)
- One Earth Future Foundation (NGO, an incubator of innovative peacebuilding programmes)[17]
- Atlantic Council (think tank)
- Carnegie Endowment for International Peace (think tank)

[17] 'One Earth Future was endowed with the belief that solving complex problems facing humanity calls for a fundamentally different way of working together. Rather than institutions working to achieve individual mandates, OEF works with the belief that sustainable peace requires a system of networked organizations working in harmony to solve problems' (One Earth Future n.d.).

- EITI—Extractive Industries Transparency Initiative (multi-stakeholder group that supports its global standard for the good governance of oil, gas, and mineral resources)
- IMO—International Maritime Organization (UN agency to improve the safety and security of international shipping and prevent pollution from ships)
- Stable Seas (transnational non-profit initiative for actionable maritime security and governance research)
- UN Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (Office for Disarmament Affairs)
- BIS Cyber Resilience Coordination Centre—Bank for International Settlements) (aims to promote global monetary and financial stability through co-ordination of global central banks and monetary policy)
- Global Cyber Alliance (non-profit dedicated to making the internet a safer place by reducing cyber risk)

Regional organizations

- GCC—Gulf of Guinea Commission
- MOWCA—Maritime Organization of West and Central Africa
- ECCAS—Economic Community of Central African States
- ECOWAS—Economic Community of West African States
- ReCAAP (Information Sharing Centre, Information Fusion Centre, Information Network System)
- ASEAN (Association of Southeast Asian Nations)

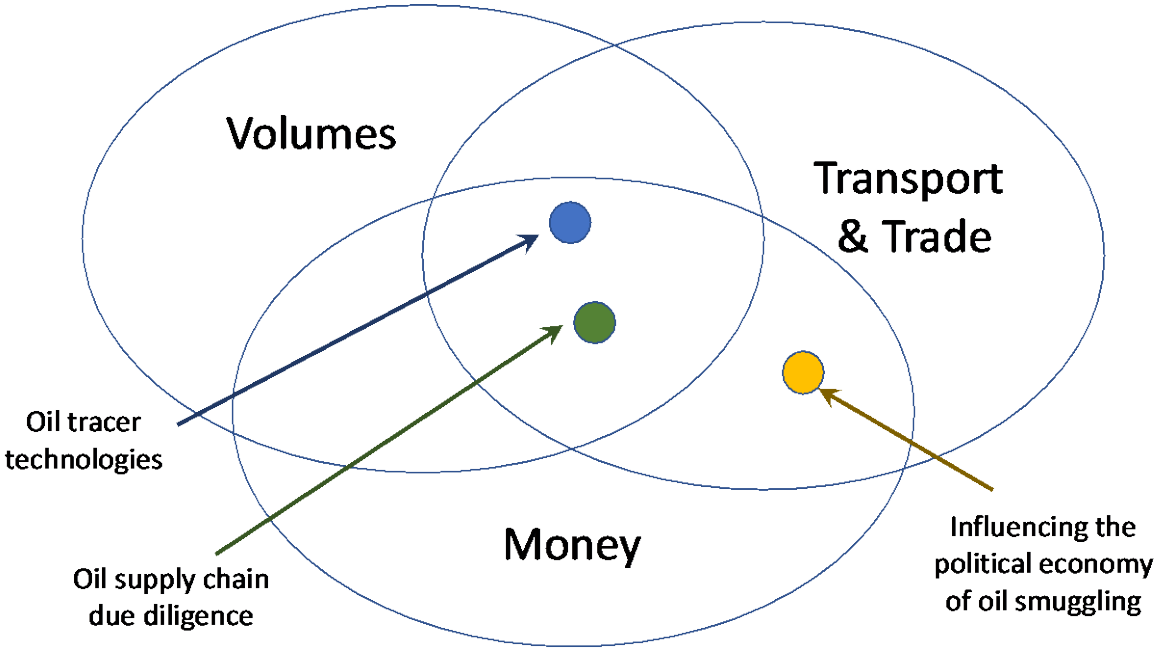
Country organizations

- International Action Against Corruption—I-ACT (in UK Foreign, Commonwealth and Development Office, a multi-component programme fighting corruption as a top international priority)
- RTF (US Ransomware Task Force)
- NIST cybersecurity programme ((US National Institute for Standards and Technology)
- Singapore government, including MPA (Marine and Port Authority) and CSA (Cyber Security Agency)
- RSiS (S. Rajaratnam School of International Studies, Singapore)

6 Example solutions

The previous section discussed an inventory of potential solutions to break the chain of global oil theft, across the three problem areas: stolen oil volumes, stolen oil transport, and stolen oil money. In this section, three high-impact opportunities are discussed in more detail. These examples have been selected because they overlap the three theft areas and therefore impact the problems on multiple fronts. The arrows in Figure 14 indicate the types of methodologies available and how they impact the three dimensions, indicated in the circles.

Figure 14: Three high-impact example solutions against oil theft



Source: authors' illustration.

6.1 Oil tracers

Section 2.1 mentioned that although each crude has its own chemical fingerprint that allows it to be traced back to its origin, once multiple crude types are blended together in pipeline or storage or upon loading, this forensic information is lost in the mix. However, it is possible to add a designer marker or tracer to a produced crude, crude blend, or fuel. For example, if oil is earmarked for export, a marker A can be added at the producing location, identifying the origin of the oil. A second marker B can be added at the point of tanker loading. If oil marked A turns up anywhere without marker B also being present, it can be inferred that it was stolen between points A and B.

Although crude markers can be designed to be robust against chemical filtering and therefore difficult to remove, once crude is refined (e.g. in an artisanal refinery) any trace of the marker is likely to have disappeared. For designer tracers to be effective, they need to satisfy a number of criteria, such as being low cost and easy to deploy; fast, accurate, and low cost to detect; stable and with a low detection limit; covert, irreproducible, and unforgeable; unremovable; and harmless to people and the environment. Marked oil can be made secure against counterfeiting by making tracers practically invisible, i.e. applying them at very low concentrations (measured in parts per million). Only when the exact tracer is known can it be identified in a legitimate cargo. Some tracers are designed not only for qualitative use (whether the tracer is present or not) but also in a quantitative manner. This is valuable in situations when adulteration of crude oil or fuel with other liquids is suspected. The degree of dilution of the tracer is indicative of the degree of adulteration.

It is expected that the valuable role of designer tracers will expand over time, not only in tracing oil theft but also in securing zero-carbon oil shipments, for which production, transport, and sometimes use have been offset by carbon credits. Customers that purchase such premium cargoes need to be assured that the supply chain is auditable and unadulterated. It is expected that once such enhanced due diligence on oil cargoes becomes more common, this will trigger demand for

a great variety of individually unique designer tracers. Such 'encoding' can be achieved by blending a limited number of designer tracers into a great variety of different proportions.

Fuel marking is not new. A fuel dye has long been applied to mark fuels with the aim of avoiding tax evasion in situations where there is differential tax on the same or similar fuels, based on:

- type of use: lower tax for extra-light heating oil compared with diesel fuel for automotive use;
- consumer: lower-tax diesel for agricultural users compared with car/transport users;
- quality: higher-sulphur marine diesel versus low-sulphur diesel used in car transport.

Fuel marking is an effective measure to combat fuel theft and fuel adulteration. In addition to applying fuel markers, the oil supply chain can also be secured with electronic cargo tracking and security systems (ECTS). These devices monitor movements of cargo transports, such as tanker trucks, and certain tampering with the cargo.

6.1.1 African examples

In Ghana, after a pilot in 2013, a full-scale petroleum product marking scheme (PPMS) was implemented for officially imported fuels in 2014. Fuel stations selling unmarked fuels are now penalized. Furthermore, all subsidized fuels are marked to identify adulteration of high-grade with lower-grade fuels. As a result, fuel adulteration in Ghana dropped by 78 per cent (Ralby 2017b).

In 2009, 29 per cent of all fuels in the highly competitive downstream market in Uganda were estimated to be adulterated, in addition to a quarter of the oil smuggled into the country. Imported fuel is siphoned upon country entry and then topped up with water or low-cost kerosene. Fuel marking regulations were introduced in 2009; fuel adulteration had dropped from 29 to 10 per cent by 2012 and further to 5 per cent by 2015. Fuel samples are taken from trucks and tested at mobile sites. The testing, overseen by live video feed, takes five minutes to identify if fuel markers are present, absent, or diluted. The latter is an indication of (the degree of) fuel adulteration. Although official estimates of the reduction in fuel smuggling and fuel adulteration (to 0.6 per cent in 2016) may be suspect, overall fuel quality in Uganda has improved significantly. However, fuel theft modalities also adapted to the clampdown. While fuel testing only requires 0.5 litres, corrupt testing officials on average siphoned off 22 litres from each truck. At one border checkpoint alone, this amounted to 1.2 m litres per year of stolen fuel (Daily Monitor 2011). Also, the problem of fuel adulteration proves to be persistent. In 2016, 140 filling stations near the capital Kampala were closed because of fuel adulteration. In remote areas, in the absence of filling stations, fuel is distributed by intermediaries who are prone to adulterating fuel mainly with kerosene. Hence, the kerosene tax that was eliminated a year earlier to relieve the poor, was reinstated. Continued high volumes of imported kerosene are indicative of the ongoing problem of fuel adulteration. Officials and government organizations are suspected to be systemically colluding with fuel adulterers in large-scale fraud, rendering the fuel-marking efforts less effective. (Ralby 2017b).

6.1.2 The European experience

In the EU, fuel marking was introduced in 1995. An EU-common yellow dye was implemented in 2002 to mark low-tax diesel and kerosene destined for heating instead of automotive transport.

However, many EU countries continue to have their own colour dyes for low-tax fuels, e.g. a green dye for low-tax agricultural diesel in the Republic of Ireland and a red dye for the same in the Netherlands. Fuel laundering (i.e. the removal of the marker dye from fuel) became a major criminal business and a key source of finance for terrorist activities. During the period of the 'Troubles' in Northern Ireland, a large share of funding for local paramilitary and terrorist organizations came from smuggling and washing of agricultural diesel from the Irish Republic. After the Belfast ('Good Friday') Agreement for peace had been agreed, professional smuggling networks continued their lucrative fuel fraud, but for financial profit instead of political motives. This is similar to what has been seen in other countries, where the profit motive supersedes political drivers for committing oil theft and fraud (Romsom 2022: section 4.3). In March 2013, a cross-border joint task force raided the farm of an alleged former chief of staff of the IRA army council and discovered a fuel-laundering plant with a capacity of 70,000 litres per day (equating to an annual revenue loss of US$27 m for the British government). In addition to 39,000 litres of fuel on site, 18,000 litres of toxic waste were discovered. Criminals conduct their laundering operations by adding acids to dissolve the fuel dyes, leaving harmful residues that can cause significant damage to the environment if not properly disposed of (Interpol 2014).

Despite the long history of fuel marking and clear examples of its successes (such as in Serbia; ADB 2015), continued fuel smuggling and fraud costs Europe more than US$4 bn in estimated lost taxes annually (Rozhov and Strzelecki 2013). One lesson is that fuel marking needs to be complemented by other transnational government measures to further arrest fuel fraud. EU Regulation 1805/2018, which enables the freezing of criminal assets at European level, came into force in December 2020. Not long thereafter, on 8 April 2021, a collaboration of public prosecution offices (PPOs) across Bulgaria, Germany, Hungary, Malta, and Romania, under the co-ordination of Italian PPOs, seized assets worth US$720 m in six countries and arrested 23 Italian suspects, in response to a fuel tax fraud worth US$1.1 bn. The scheme deployed by these crime syndicates appears to be a typical case of VAT fraud, known as missing trader intra-community (MTIC) fraud or carousel fraud (Pouwels 2021). Investigations into this tax fraud, which had been run by two mafia-style Italian crime groups from Naples and Reggio Calabria, had started in 2017 (Eurojust 2021).

6.1.3 An example from Asia

In September 2019, the government of the Philippines started its PPMS to counter a loss of US$7.1 bn in taxes from fuel smuggling during 2010–19. In 2016, excise and value added tax collection from petroleum products amounted US$1.1 bn, while estimates of fiscal revenue loss from smuggled and adulterated fuels ranged from US$566 m to US$922 m (i.e. 34 to 45 per cent of petroleum products in the Philippines escaped taxation). The fuel-marking project cost was estimated at US$0.016 per litre and its terms of reference (GOVPH 2018) prescribed that markers were to be:

- impossible to imitate, replicate, remove, or alter;
- light and heat resistant and chemically stable in composition and concentration for at least three years;
- embedded at the molecular level, invisible, odourless, and able to mix homogeneously with a wide range of fuel products;

- able to detect dilution of marked fuels at a low detection threshold and provide sufficient certainty for legal prosecution purposes at 5 per cent dilution or more;
- compliant with motor-engine emissions environmental and health regulations and meeting safety standards;
- non-reactive to fuel, additives, and other markers added by the oil companies, to not affect their performance.

The terms of reference also prescribed requirements and performance measures for field testing units and mobile fuel analysers. After 21 months, having marked more than 24 bn litres of fuel (60.7 per cent diesel, 38.7 per cent gasoline, and the remainder kerosene), the programme had helped to secure US$4.7 bn in tax collection. Twenty-four companies participate in the fuel marking programme, including Petron, Shell, Unioil, Seaoil, and Insular Oil, representing 68 per cent of the total fuel volume marked.

6.2 Influencing the political economy of the smuggling trade

Sustainable solutions to oil theft and smuggling require a much better understanding not only of why these activities occur, but also of how the operations are shaped and executed. Smugglers and state structures are commonly seen as antagonists. Smugglers are supposed to evade law enforcement by operating in remote areas and across poorly controlled border areas. Perceptions of the involvement of state actors in smuggling operations are often limited to frontline officials conducting petty crimes by occasionally taking bribes to allow certain goods to be smuggled across the border. If smuggling continues to occur, it is commonly assumed that the state lacks the capacity to enforce its rules. Smuggling is also seen to be subversive and, particularly in developing countries, an indication of a state's weakness and fragility. Therefore, government policies often focus on strengthening border security particularly in remote areas, by building walls and fences, and by implementing more-effective surveillance technologies. Enforcement of regulations is bolstered by training frontline border officials in anti-bribery and smuggling detection skills.

However, research into actual smuggling operations shows that smuggling very often occurs at controlled border posts rather than in remote areas. Beyond geography and border security infrastructure, the nature of the interaction between smugglers and state structures is the most powerful predictor of the routes through which different smuggling networks prefer to operate Gallien and Weigand 2021). Professional smuggling networks interact with state structures/actors very differently from the petty corruption model of individual border agents. Professional smugglers need predictability in their operations and cannot be dependent on the wiles of individual agents whose actions and duty rosters are unreliable and subject to instant change. Professional smugglers benefit from using the state's infrastructure and (protection) services, to carry out their operations with greater efficiency and at lower cost. They continuously weigh cost and risk to optimize their business model and often prefer to pay a high but fixed and predictable cost at a border to facing the risk of their smuggled goods being impounded, their business rolled up, and themselves being arrested. For this dependability and efficiency of operations, professional smugglers are willing to pay a substantial business fee. In fact, some smuggling operators prefer to pay a significant fee over open borders, if this protects their market share and the prices of smuggled goods. A flat-fee arrangement between a smuggling network and a state structure can be a significant barrier to entry for would-be smugglers. Such a flat-rate interaction structure helps to sustain market concentration by reducing competition and facilitating large-scale smuggling operations, thereby supporting the syndicate's market share and predictably sizeable profits. In many societies, a flat-fee arrangement also increases the social respectability and acceptance of smugglers and their business.

At least six different archetypes of interactions between state structures or actors and smugglers can be distinguished (see Table 2). One extreme type is '**Genuine enforcement**', which basically describes the enforcement of the law, without exceptions. Smugglers only succeed when they are able to avoid detection. The opposite extreme is '**toleration**', whereby state authorities allow smugglers to conduct their affairs without enforcing the rules that would prohibit them from doing so. Although the toleration is informal, it is regulated and institutionalized. Consequently, the risk of detection is not an issue. This type of state–smuggler interaction occurs when the state has no capacity to deal with the smuggling or when the smuggling fulfils a socioeconomic need (smuggling as a survivalist activity). In some smuggling operations, the state authorities are directly involved in the operations; this model is prevalent for high-value, high-risk goods that require particular security measures ('**state as smuggler**' interaction model). The state security forces not only protect the smugglers with whom they partner but also go after rival smuggling syndicates that do not work with the authorities. Oil theft and smuggling operations in Nigeria, Russia, and Brazil show characteristics of the state as smuggler model (see Romsom 2022: sections 4.1.2, 4.3, 5.1).

The '**cat and mouse**' interaction model describes a situation in which state actors pursue smugglers and if smugglers are caught in the act, they have to pay a very steep bribe (but not a fine), often a pre-agreed amount, to the enforcement officers. Otherwise, if the smugglers are not caught in the act, they go free. In this interaction model, law enforcement accepts that smuggling occurs and smugglers are not pursued beyond the boundaries of the 'game'. **Petty corruption** describes a different type of interaction whereby a bribe is sought from an individual state agent, but it is not clear upfront if the bribe is likely to be accepted or at what level. This type of interaction generally occurs for small-scale acts of smuggling, and success is dependent on the personal relationship between smuggler and state agent. Professional smugglers generally avoid this type of corruption, as the outcome is too unpredictable and the scheme is not resilient to changes in individuals. The final **flat-fee** interaction mode has already been described above.

Actual state–smuggler interaction schemes may be modified forms or combinations of these six archetypes. The interaction models may differ on the two sides of a border, and may vary depending on the type and scale of goods smuggled. Interaction models are also subject to changes over time, as external factors change or as smuggling syndicates further expand their operations.

Table 2: Six archetypes of state–smuggling interactions

Type	State–smuggler interaction	Predictability	Bribes	Evasion	Market concentration	Financial benefit for state actor
Genuine enforcement	Detection and successful evasion are both possible	Severe uncertainty around detection/evasion for all parties; clarity on consequences	Not possible	Yes	Low to High	None
State as smuggler	Toleration for state smugglers only	State (self-)protection from consequences	Not necessary	No	Very high	Very high
Cat and mouse	Detection and successful evasion are both possible	Severe uncertainty around detection/evasion for all parties; clarity on consequences	If detected, bribes are necessary and standardized	Yes	Moderate	Potentially high, but with high risk
Petty corruption	Ad hoc interaction based on personal relations	Consequences unclear for smugglers	Necessary and not standardized	No	Low	Low to moderate
Flat rate	Defined and agreed interaction	Clarity on consequences	Necessary and standardized	No	High	High
Toleration	Defined and agreed interaction	Clarity on consequences	Not necessary	No	Very low	None

Note: a comprehensive description of the types of state–smuggling interactions is provided by Gallien and Weigand in their excellent paper 'Channeling Contraband: How States Shape International Smuggling Routes' (2021).

Source: authors' construction adapted from Gallien and Weigand (2021)

The effectiveness of increasing state enforcement capacity depends on the interaction model between state and smugglers. Whether a smuggling syndicate opts for smuggling routes that target official border crossings or those that avoid them depends on the form of state–smuggler interaction. This interaction is shaped jointly by the smuggler and the state structure/actors rather than by the smuggler alone. The smuggler's business model (risk, cost, scale, type of goods) drives which type of interaction can be condoned. While the motivations of the smuggler can be understood in terms of its business tolerance for unpredictability, cost of evasion, cost of interaction, benefits from using state infrastructure, profitability from market concentration, etc., it is equally important to understand the motivations of the state structure for condoning and sometimes seeking an interaction *other than* the genuine enforcement that we often assume. Financial gain is a likely factor, but this does not necessarily imply a petty corruption model (see Table 2). Other factors, such as distributional politics (in case of the toleration model) and assuring domestic supplies of goods can drive political acquiescence. The smuggler–state interaction model therefore determines not only the operational model of the smuggling syndicate but also the smuggling economy's market structure (Gallien 2019).

The relationship-driven model helps to explain how smuggling syndicates diversify their businesses. Once a smuggling route has been set up and agreed with the states' structures, the same route and model can be utilized to traffic other goods, sometimes going the opposite way. What is 'accepted' under a flat-fee arrangement, in terms of types of goods, scale of operations, etc., is subject to habituation. Over time, this enables smuggling syndicates to extend their business model and expand their spheres of operation. Such underlying dynamics allow, for example, some opportunistic smugglers of fuel in containers to develop over time into an international network

of organized crime, which may include professional smuggling of oil, arms, and drugs and trafficking of people. Money earned from smuggling also finds its way into political activities, particularly if the interacting state structure is politically affiliated. This secures the relationship, benefiting both the smuggling syndicate and the actors in the state structure. The interaction model further shapes the dynamics between smuggling syndicates and local communities. Syndicates that are excluded from the state–smuggler interaction may raid the operations of their competitors and cause insurgencies. Yet professional smugglers do not favour conflict zones. The benefits of a vacuum in enforcement are generally more than offset by unpredictability in smuggling operations. Violence is particularly likely to occur with changes in the interaction and changes that affect market concentration (see Romsom 2022: sections 3.2.2, 3.2.3).

Oil smuggling is generally conducted through discrete acts of lower value and higher frequency than, for example, arms or drug smuggling, and therefore has a higher tolerance for unpredictability. A professional fuel smuggling syndicate can price in a loss percentage due to the risk of detection. It can also decide to invest more in detection evasion to reduce the probability of detection, or distribute the smuggled fuel across smaller parcels to reduce the impact of individual cases of detection. It can also engage with a state structure to barter a flat rate and allowing it to operate unchecked.

At the Malaysia–Thailand border in Narathiwat province, the '**flat-rate**' model is the dominant model for smuggling operations that include fuel crossing the border into Thailand. Flat fees are paid by professional smugglers to officials on both sides of the border and are shared among authorities, including customs officials, border police, and immigration. By contrast, fuel smuggled across the border between Libya and Tunisia (Gallien 2018) is a typical case of '**cat and mouse**' interaction. At night, jeeps cross the border from Tunisia into Libya to load goods, including fuel. Upon their return to Tunisia, they choose their routes carefully in the difficult terrain along the border that extends for hundreds of kilometres. Custom officials try to detect and catch the smugglers in their own jeeps. If they are successful the smuggler pays a steep bribe but, crucially, is not arrested. The next night, the game starts anew (Gallien and Weigand 2021). The land border across Algeria and Morocco has been officially closed since 1994. However, makeshift border crossings were constructed by creating doors in the border fence staffed by Moroccan soldiers. Smugglers operated under '**petty corruption**' by paying bribes to the soldiers. From 2011 onwards, the soldiers stopped taking bribes from small fuel smugglers and allowed them to pass unhindered ('**toleration**'). However, they continued to ask for bribes from larger smugglers. The petty corruption model does not suit the professional smugglers that operate at a much larger scale. Instead, they opt to avoid detection by smuggling fuel at night in cars in remote border areas (Makhifi 2013). If caught, they would be arrested and their cars and contraband confiscated ('**genuine enforcement**') (Boukhars 2013). Another example of genuine enforcement is Singapore, where authorities have clearly defined standards that aim to curb fuel theft, and the capacity and will to enforce when laws are broken or standards are not adhered to (see sections 2.2 and 2.3).

More knowledge is needed to create a more nuanced understanding of the considerations and motivations that drive both smugglers and state actors in different country cases. Beyond the cost–risk assessments of smuggling networks, this should also include contextual input, such as normative perceptions, border histories, and local state–society relationships. As the interaction models shape the smuggling economy, individual smuggling syndicates evolve over time. Shifting tolerances, market consolidation, and expanded versus reduced opportunities for smuggling syndicates may transform the interaction model. These developing interactions eventually contribute to the shaping of states. When state officials or influential entities within states become interdependent with officials or entities in other states to maintain an illicit supply chain, other elements in the relations between those states can be jeopardized (Ralby 2017c). The political

economy of smuggling needs further development and testing with actual data to direct government efforts effectively and ultimately towards genuine enforcement.

6.3 Supply-chain due diligence initiatives

Due diligence is an important tool for the oil supply chain to regulate itself. End users increasingly value the origination of the products they purchase. The extractives industries and their supply chains similarly recognize the need for standards in transparency about the origination of commodities, as well as performance standards for suppliers, transporters, and traders. Governments, industry, and civil society are supporting various mandatory and voluntary due diligence schemes (Katsouris and Sayne 2013). Learning from due diligence efforts across extractives industries could be exchanged and adapted to develop workable schemes and solutions.[18] The associated efforts and costs for supply-chain due diligence ought to be borne by all the participants in the supply chain and not just by the upstream producers (Östensson 2020). It is worth noting that oil traders and buyers are increasingly incentivized to validate oil supply chains, as their carbon footprint is increasingly regulated and priced for imported products (Romsom and McPhail 2020). Therefore, synergy value exists in oil supply-chain due diligence, as this prevents both value leakage due to oil theft and fuel adulteration, as well as supporting higher prices for deliveries of oil cargoes with a proven low carbon footprint.

In 2003, the EITI was established as a demonstrable response to broad public demand for more transparency. At present, 55 countries have signed up to EITI's disclosure standard and are subject to regular review against the standard (EITI n.d.). Transparency initiatives are good in principle, as they allow a more fact-based assessment on issues such as corruption and illicit money flows. They also provide a common framework for a comparative analysis with peer countries, to establish trends over time and assist in identifying best practice. Proponents of transparency measures to target oil theft could look to campaigns against illegal trades in other natural resources for examples.

In the maritime sector, ReCAAP (see Section 2.4.1) is a good example of a regional government-to-government agreement to promote and enhance co-operation against piracy and armed robbery against ships in Asia. It shares factual data on individual incidents, trends, and best practice. Stable Seas (see Section 2.4.2) focuses on developing a more comprehensive and holistic understanding of the interconnected nature of maritime security challenges, expressed in a Maritime Security Index. It has also developed an outreach programme to share its research with national governments and provide them with targeted information. Both examples assist in transparency and knowledge sharing in maritime security that is directly relevant for preventing maritime oil theft and piracy. Key issues to overcome in further promoting transparency on incidents include insurance cost exposure when reporting oil theft and reputation issues, particularly if company staff and ship crews are involved in wrongdoing. Insurance companies will benefit from increased reporting, as this will help to prevent further incidents. Methodologies deployed by ReCAAP and Stable Seas are likely to be applicable to developing targeted approaches to counter and prevent oil theft across its supply chain (including non-maritime). There is similarity in the underlying issues, methods, and drivers behind the syndicated criminal activities involved (in some cases, the crime syndicates are the same).

[18] The oil tracer solutions described in Section 6.1 can be viewed as analogous to marking diamonds with laser engravings to prove their legitimate origins and to differentiate them from 'conflict diamonds'. However, the purpose of due diligence (and the use of tracers) for oil supplies is not to stigmatize their origin but to protect the integrity of the oil supply chain.

Increased transparency over onshore oil theft is also much needed. For many years, Shell Nigeria has reported oil spills and joint investigation visits (JIVs) are being conducted by key stakeholders. For Shell this provides transparency, as more than 90 per cent of volume spilled is due to sabotage and theft (see Romsom 2022). Reliable and comprehensive statistics on illegal oil taps, spills, artisanal refineries, etc. are instrumental in closing the knowledge gap on how much oil gets stolen (and where). Furthermore, the JIV process is also beneficial in ensuring diligent clean-up after each case has been properly recorded (and the cause of the spill determined). Increased transparency on the amounts of oil spilled, the causes of spills, and the effectiveness of the clean-up is necessary to keep stakeholders informed and aligned and avoid repeat occurrences.

In addition to increased overall transparency, each participant in the oil market should conduct detailed commercial due diligence on suppliers, buyers, traders, and individual oil trades and cargoes. Vertically integrated oil companies and large refining companies deploy their in-house due diligence methods on any crude oil purchases for their refineries. New sellers have to go through an initial vetting process to get pre-approved. Usually the assessment has two elements: verification of paperwork and checking of references. Once a crude seller has been accepted, a second verification process takes place for each individual transaction. Companies conduct these checks for two key reasons: (1) to avoid being scammed by sellers that have (illegitimate) paperwork, but no cargoes to sell—advance-fee fraudsters are particularly common; (2) to protect a company's reputation when dealing with disreputable sellers or cargoes. However, deals typically get done months in advance of actual transport and delivery. Hence, there is little incentive for crude buyers to check later if specific cargoes contain stolen crude. Smaller legitimate but less careful traders can also provide routes for illegitimate crude to enter global commercial markets. The use of molecular markers, described in Section 6.1, provides an effective complement to the due diligence framework in securing the right and unadulterated cargoes.

Crude oil and fuel cargo purchases are often financed by banks, particularly if these transactions involve traders as intermediaries, who tend to have less capital availability. Banks' finances are directly exposed if oil trades fail, or if there is fallout from other related malpractice. For example, Singapore's failed oil trader Hin Leong owes 23 banks, including HSBC Holdings, DBS Group Holdings, and OCBC Bank, at least US$3 bn in debt after committing fraud by failing to report US$800 m in losses accumulated over years. Such high-profile bankruptcies tend to spill over to other trading and fuel bunkering firms, creating a wave of other bankruptcies and bank exposures (see Box A, Section 2.3.3). Banks are therefore obligated to perform regular due diligence on their loans and letters of credit, as such exposures are likely to surface in the cyclical oil market.

In addition to individual companies' and banks' in-house due diligence processes, there is scope to introduce a global scheme for oil due diligence by recognized and respected third parties. Such parties could assess and verify individual sellers (e.g. as an accreditation scheme) and provide supply-chain evaluations for individual cargoes. Financiers and insurers could link their services to such independent verification. Blacklists of proven offenders could send a strong signal to commercial parties and make it much harder for oil criminals to do legitimate business.

Such due diligence activities are exceedingly important, yet they do not stop deliberate rogue buyers, sellers, and traders from conducting their illegitimate activities. There will always be actors who pursue financial profits as their primary objective. However, due diligence processes as described can corner illegitimate elements in the supply chain and avoid cross-contamination of global markets. Law enforcement activities can then be more focused on those uncertified parties and their transactions. Due diligence processes may also not be foolproof, and repeated evaluations are necessary in case 'behaviours' change or new information becomes available. Therefore, the ultimate accountability remains with the transacting parties and not with the due diligence service providers. End-use customers' purchasing choices should also become more

discerning about the details of the fuels they buy. Independent supply-chain analysis, accreditation, and certification schemes can support raising such awareness with end-use customers. There are also lessons to be learned from other commodity sectors that are affected by illegal activities, such as logging.

There is an urgent need for a global reporting mechanism for the warning signals that oil due diligence processes may raise. Transnational law enforcement agencies may detect patterns in global data analytics that may expose oil theft syndicates. Such information can also be used to make fiscal regimes more secure against fraud. This can involve aligning cross-border fuel prices but also changes in value added tax schemes (such as in the EU) that were at the root of the massive fuel fraud conducted by the Italian mafia (Section 6.1). Transnational judicial measures, such as Regulation 1805/2018, which enables the freezing of criminal assets at European level, make law enforcement increasingly effective on the international stage (see also Section 4.3).

With the emergence of cross-border CO_2 taxes (VanderWolk 2021), independent supply-chain due diligence is also of value in verifying the carbon intensity of oil shipments, now that carbon-neutral and low-carbon cargoes are starting to be sold in the global market with price premiums paid for by discerning customers. The use of technologies such as MFM; automated digital records and delivery notes without human intervention; satellite monitoring; NFTs and blockchain technology for securing documentation; and potential tracer information linked to oil cargoes, invoice numbers, etc. could further contribute to a more secure and trusted supply chain. In addition, increased transparency by governments on individual oil transactions (price, volume, grade, buyer, tanker, loading date, etc.) could assist the verification of oil shipments, their origin, and their supply chain.

7 Conclusion

Oil theft is a large-scale global problem, not limited to developing countries. It is pervasive and versatile. It has many facets and modalities, ranging from violent acts of piracy aimed at capturing and transferring cargoes of oil tankers, to misappropriation by physical theft and adulteration of fuels, to cross-border smuggling operations, to massive 'white-collar' crimes in elaborate tax evasion schemes. The schemes to conduct oil theft crimes are continuously adjusting to maintain an advantage over any progress made by law enforcement. Compared with high-value and illicit items, such as drugs and weapons, oil theft generally ranks lower on local law enforcement's priority lists, yet the financial, economic, environmental, and social costs are immense, as this paper has sought to demonstrate.

Internationally, oil theft has thus been largely ignored. Although there are important international aspects of this illegal trade, such as bribery, money laundering, environmental damage, and the involvement of militant/extremist organizations, there have been few specific international programmes to counter it. Oil theft is often mistakenly seen as a domestic problem, but in reality, as this paper has shown, it also compromises the integrity of foreign markets and international financial systems. Furthermore, the secretive and violent characteristics of this illegal trade often prevent any intelligence-based action, while the transnational organized crime networks involved are too flexible, mobile, creative, and diffuse to pursue. National government officials are sometimes unenthusiastic about doing anything substantial to disrupt the illegal trade—which can sometimes be linked to their own engagement in the trade itself.

However, it is the scale of oil theft as a business that sets it apart. At US$133 bn per year, **oil is the world's largest stolen natural resource, while fuel is the global number one most**

smuggled natural resource. Oil theft should be a high priority for law enforcement also because its proceeds are often used to finance other organized crime activities and because it triggers violence against the community and in crime-on-crime activities. The impact of oil theft has been broadly documented in the first working paper.

This second working paper on oil theft has focused on recent oil theft trends, particularly on schemes involving fuel theft and fraud, as well as the concerning trend of cryptoware attacks on oil and gas installations. Cyberattacks and ransomware digital crimes are growing in scale, number, and sophistication. Criminals are expected to significantly increase the use of digital crime to substitute or complement physical oil theft. Oil and maritime infrastructures are critically exposed to cybercrime. In those developing countries that do not deploy the very latest cybersecurity, this is likely to be a growing problem in the years ahead.

Examples of successes against oil theft are often the result of a combination of the following:

1. smart applications of theft detection technology and standards;
2. processes and systems that promote transparency and sharing best practice; and
3. transnational collaboration in law enforcement and judicial processes, and alignment in (cross-border) fiscal regimes.

Some recent successes against oil theft are:

- Singapore regulations and mandatory standards for maritime fuel bunkering, combined with mandatory MFM, have reduced local misappropriation of marine fuels by US$1.7 bn from 2017 to 2020.
- Strong enforcement was exercised by Singapore's MPA in revoking the bunkering licences of 19 companies because of fraud and malpractice between 2012 and 2019. This reduced the number of Singapore-licensed bunker companies from 63 to 45 (with one new entrant into the fuel bunkering business in the period).
- In a whole-of-government approach, Chinese authorities closed the tax gap for LCO in China, stopping an illegal fuel adulteration scheme worth US$3.9 bn per year in avoided fuel taxes that caused harmful emissions to health and the environment.
- A combination of the application of a silent SSAS and information sharing, communication, and co-ordination by ReCAAP on maritime robbery and hijacking incidents has reduced the number of reported tanker piracy incidents in Asia from 15 in 2014 to zero since 2019.
- The concerted international stance against the wave of piracy in Gulf of Guinea since 2016 has been the most decisive action from the international community to date. Following UN Security Council discussion in 2016 and subsequent international co-operation to ensure the fast response of navy vessels in Gulf of Guinea, the number of tanker hijacks to steal their cargoes has declined significantly. In 2019 there were four vessel hijackings (including three oil tankers), but none of these resulted in oil theft or ransom of the vessels. Nevertheless, the number of tanker incidents in Gulf of Guinea remains high, with 40 incidents reported in 2019, including six cases of kidnapping of tanker crews.
- The cyberattack on the Colonial pipeline in the US on 7 March 2021 caused one of the largest energy supply disruptions in US history. The facility was brought quickly back online by 12 May after the company had paid the DarkSide hackers responsible US$4.4 m in Bitcoin. Many valuable lessons were learned. This event contrasted with Norsk Hydro's earlier experience and response. The organized actions of cybercriminals follow similar patterns to those of oil theft crime syndicates in at least seven distinct aspects. Learning

from the Norsk Hydro attack and the recommendations from the US RTF provide valuable practical advice to prevent and respond to cryptoware attacks.

Despite the above successes and learning, oil theft has proven to be persistent and resilient against law enforcement measures. Theft syndicates exploit weaknesses in petroleum infrastructure, processes, and organizations, as well as weaknesses and gaps in regulations, law enforcement capacity, and jurisdiction. Key gaps remain in tackling oil theft, including:

- oil theft information gaps;
- gaps in national and international collaboration to counter oil theft;
- oil theft law enforcement, jurisdiction, and other judicial gaps;
- gaps in community support to stop oil theft.

Informed solutions to confronting pervasive oil theft problems require basic data that are mostly lacking. Systematic, comprehensive, and holistic data gathering and analysis are needed to expose, understand, and address the interconnected nature of oil theft challenges. These include:

- How much oil is produced and how much is stolen?
- How is stolen oil transported and traded?
- How are illegal oil transactions conducted?

Contrasting the four key enforcement gaps are 12 oil theft commonalities:

1. Oil theft syndicates are organized in loose cell structures, not too dissimilar from terrorist organizations.
2. They exploit transnational gaps in law enforcement and judicial systems.
3. They replicate similar (often identical) oil thefts repeatedly.
4. They flexibly adapt theft execution strategies and even switch their business models.
5. Oil theft organizations are frequently linked to other crime businesses.
6. They extend their reach and influence by buying allegiances, support, and information through bribes, profit sharing, and extortion.
7. Oil theft contaminates legal oil markets and financial markets.
8. Oil thieves often mix legal commercial operations with illegal activities.
9. Exposure of oil theft can cause unforeseen collateral damage to the legal economy, such as strings of bankruptcies and unpaid debts to suppliers, traders, and banks, even if these were not at all involved with any crimes.
10. Oil theft and related insecurity greatly affect economic activity and government tax income of developing countries.
11. Oil theft causes a lack of business confidence and underinvestment in developing economies.
12. Beyond the violence, the loss of resources, and the destruction of the environment that oil theft causes, the biggest potential loss to developing countries is the loss of loyalty of the people for their governments.

Acts of oil theft are so pervasive and differentiated that no single measure is adequate to break the cycle of theft. Oil theft should be regarded as illegal business, rather than as a set of separate illegal acts. Actions against oil theft should target the transnational crime syndicates that continue to find ways to replicate their thefts by adapting their theft strategies and business models.

Reliable intelligence gathering is needed to obtain detailed oil theft information and assess trends. Technologies, such as designer tracers used as oil markers, fibre-optic sensors in pipelines, remote

sensing by satellite, and drone surveillance, AIS, and SSAS devices on ships, combined with data analytics, can make a key contribution in protecting assets against oil theft, as well as determining patterns that can be used as indicators and warning signals that oil theft is ongoing.

The international community should take a stronger stance against oil theft. Transnational oil theft crime syndicates are often linked to other crime businesses, such as arms, drug and people trafficking and extremist organizations. The actions needed to stop oil theft are similar to those taken against other international organized crime. However, the international community should work with and be led by the countries where oil theft occurs. International solutions to address oil theft can be categorized into the aforementioned three key areas: stolen oil volumes, stolen oil transport, and stolen oil money.

Finally, this paper has proposed several actions for each category. Solutions that overlap these three areas show most promise as these impact oil thieves on multiple fronts. Three specific examples were discussed: oil tracer technologies, influencing the political economy of fuel smuggling, and supply-chain due diligence initiatives. Each country may emphasize different aspects in this repertoire of measures, depending the local situation and progress already made to curb oil theft.

Figure 15: Leaving the petrol station (Cameroon)

Source: image by Carsten ten Brink, taken on 27 December 2010, reproduced from Flickr.com under CC BY-NC-ND 2.0.

References

ADB (Asian Development Bank) (2015). 'Fuel-Marking Programs: Helping Governments Raise Revenue, Combat Smuggling, and Improve the Environment'. *The Governance Brief*, 24. at: https://www.adb.org/sites/default/files/publication/174773/governance-brief-24-fuel-marking-programs.pdf (accessed 10 February 2022).

Aizhu, C., and K. Samanta (2021a). 'China's Fuel Clampdown Curbs Its LCO Imports, Korean Refiners to Suffer'. Reuters, 28 April. Available at: https://www.reuters.com/article/china-oil-lco-idUSL4N2MH03L (accessed 10 February 2022).

Aizhu, C., and K. Samanta (2021b). 'China's Guangdong Province Holds Meeting to Tackle Illicit Fuel Trade: Sources'. Reuters, 24 April. Available at: https://www.reuters.com/article/china-oil-lco-idUSL4N2ME182 (accessed 10 February 2022).

Anish (2021). 'What is Ship Security Alert System (SSAS)?' Marine Insight, 28 May. Available at: https://www.marineinsight.com/marine-piracy-marine/what-is-ship-security-alert-system-ssas (accessed 7 February 2022).

Argus (2020a). 'Call Grows to Flag Mexico's Gulf as High-Risk'. Argus, 30 July. Available at: https://www.argusmedia.com/en/news/2128157-call-grows-to-flag-mexicos-gulf-as-highrisk (accessed 9 February 2022).

Argus (2020b). 'Mexican Oil Caught between a Hug and a Hammer'. Argus, 19 August. Available at: https://www.argusmedia.com/en/blog/2020/august/19/mexican-oil-caught-between-a-hug-and-a-hammer (accessed 9 February 2022).

Balima, H., D. Daly, and B. Loko (2020). 'External Private Financing and Domestic Revenue Mobilization: A Dilemma?' Working Paper WP/20/230. Washington, DC: IMF. https://doi.org/10.5089/9781513560397.001. Available at: https://www.imf.org/en/Publications/WP/Issues/2020/11/08/External-Private-Financing-and-Domestic-Revenue-Mobilization-A-Dilemma-49741 (accessed 7 February 2022).

Barrera, A. (2019). 'Death Toll from Mexico Pipeline Blast Reaches 91, Pemex Defends Response'. Reuters, 21 January. Available at: https://www.reuters.com/article/us-mexico-fuel-theft-casualties-idUSKCN1PF1EC (accessed 9 February 2022).

Bonnier, U., and L. Bonnier (2019). 'Mapping the Impact of Illicit Trade on the Sustainable Development Goals'. New York: TRACIT. Available at: https://unctad.org/system/files/non-official-document/DITC2019_TRACIT_IllicitTradeandSDGs_fullreport_en.pdf (accessed 7 February 2022).

Boukhars, A. (2019). 'Barriers versus Smugglers: Algeria and Morocco's Battle for Border Security'. Carnegie Endowment for International Peace, 19 March. Available at: https://carnegieendowment.org/2019/03/19/barriers-versus-smugglers-algeria-and-morocco-s-battle-for-border-security-pub-78618 (accessed 10 February 2022).

Briggs, B. (2019). 'Hackers Hit Norsk Hydro with Ransomware: The Company Responded with Transparency'. Microsoft, 16 December. Available at: https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency (accessed 9 February 2022).

Bunker Index (2014). 'OW Bunker's Global Debt and the Claims So Far'. Bunker Index Insights & News, 19 November. Available at: https://bunkerindex.com/news/article.php?article_id=14102 (accessed 9 February 2022).

Chatham House (2013). *Maritime Security in the Gulf of Guinea*. London: The Royal Institute of International Affairs. Available at: https://www.chathamhouse.org/sites/default/files/public/Research/Africa/0312confreport_maritimesecurity.pdf (accessed 9 February 2022).

Chinoy, K.H. (2014). 'Tricks of the Bunker Trade: Cappuccino Bunkers, an Illustrated Guide to Loss Prevention'. Ship & Bunker, 12 August. Available at: https://shipandbunker.com/news/features/bunker-quality-quantity/849698-tricks-of-the-bunker-trade-cappuccino-bunkers-an-illustrated-guide-to-loss-prevention (accessed 9 February 2022).

Cimpanu, C. (2019). 'US Coast Guard Discloses Ryuk Ransomware Infection at Maritime Facility'. ZDNet, 30 December. Available at: https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/ (accessed 9 February 2022).

Cimpanu, C. (2020). 'DHS Says Ransomware Hit US Gas Pipeline Operator'. ZDNet, 19 February. Available at: https://www.zdnet.com/article/dhs-says-ransomware-hit-us-gas-pipeline-operator/ (accessed 9 February 2022).

CISA (2020). 'Alert (AA20–049A): Ransomware Impacting Pipeline Operations'. Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security, 18 February and 24 October. Available at: https://us-cert.cisa.gov/ncas/alerts/aa20-049a (accessed 9 February 2022).

Constantin, L. (2021). 'Ryuk Ransomware Explained: A Targeted, Devastatingly Effective Attack'. CSO Spotlight, 19 March. Available at: https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly-effective-attack.html (accessed 9 February 2022).

Cook, D. (2008). 'Oil and Terrorism'. Working Paper on 'The Global Energy Market: Comprehensive Strategies to Meet Geopolitical and Financial Risks'. Houston, Texas: The James A. Baker III Institute for Public Policy, Rice University. Available at: https://www.bakerinstitute.org/media/files/Research/b5edc3ae/IEEJoilterrorism-Cook.pdf. (accessed 7 February 2022).

CPIB (2021). 'Former Shell Employees Charged for Corruption'. Corrupt Practices Investigation Bureau, 23 February. Available at: https://www.cpib.gov.sg/press-room/press-releases/former-shell-employees-charged-corruption (accessed 9 February 2022).

Cybereason (2021). 'Cybereason vs. DarkSide Ransomware'. Cybereason, 1 April. Available at: https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware (accessed 9 February 2022).

Daily Monitor (2011). 'UNBS Officials Siphon Fuel into Black Market'. Daily Monitor (Uganda edition), 6 August, updated 24 January 2021. Available at: https://www.monitor.co.ug/uganda/news/national/unbs-officials-siphon-fuel-into-black-market-1497820 (accessed 10 February 2022).

DefenceWeb (2016). 'UN Wants Gulf of Guinea Piracy Halted'. DefenceWeb, 26 April. Available at: https://www.defenceweb.co.za/security/maritime-security/un-wants-gulf-of-guinea-piracy-halted/?catid=108 per cent3Amaritime-security&Itemid=233 (accessed 9 February 2022).

Desjardins, J. (2017). 'Crude Awakening: The Global Black Market for Oil'. Visual Capitalist, 4 May. Available at: https://www.visualcapitalist.com/global-black-market-fuel-theft/ (accessed 7 February 2022).

Eaton, C., and D. Volz (2021). 'Colonial Pipeline CEO Tells Why He Paid Hackers $4.4 Million Ransom'. *The Wall Street Journal*, 19 May. Available at: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 (accessed 9 February 2022).

EITI (Extractive Industries Transparency Initiative) (n.d.). 'Countries: Implementation Status'. Available at: https://eiti.org/countries (accessed 10 February 2022).

Engineering Institute of Technology (n.d.). 'Introduction to Fiscal Metering'. Available at: https://www.eit.edu.au/resources/introduction-to-fiscal-metering/ (accessed 7 February 2022).

Eurojust (2021). 'Action to Counter Italian Fuel Tax Fraud Worth Almost EUR 1 Billion'. European Union Agency for Criminal Justice Cooperation Press Release, 8 April. Available at: https://www.eurojust.europa.eu/action-counter-italian-fuel-tax-fraud-worth-almost-eur-1-billion (accessed 10 February 2022).

Fineren, D. (2011). 'Cyber Attacks Could Wreck World Oil Supply'. Reuters, 8 December. Available at: https://www.reuters.com/article/oukin-uk-cyber-attacks-oil/cyber-attacks-could-wreck-world-oil-supply-idUKTRE7B71EZ20111208 (accessed 9 February 2022).

Gallien, M. (2018). 'An Economic Malaise Lies at the Heart of Libya–Tunisia Border Standoff'. Middle East Eye, 31 July. Available at: https://www.middleeasteye.net/opinion/economic-malaise-lies-heart-libya-tunisia-border-standoff (accessed 10 February 2022).

Gallien, M. (2019). 'In North Africa's Borderlands, Smuggling Has Helped Keep a Fragile Peace. Now It's Under Threat'. *The Washington Post*, 19 June. Available at: https://www.washingtonpost.com/politics/2019/06/19/north-africas-borderlands-smuggling-has-helped-keep-fragile-peace-now-its-under-threat/ (accessed 10 February 2022).

Gallien, M., and F. Weigand (2021). 'Channeling Contraband: How States Shape International Smuggling Routes'. *Security Studies*, 30(1): 79–106. https://doi.org/10.1080/09636412.2021.1885728

Gloystein, H., and J. Geddie (2018). 'Shady Triangle: Southeast Asia's Illegal Fuel Market'. Reuters, 18 January. Available at: https://www.reuters.com/article/us-singapore-oil-theft-southeast-asia-an-idUSKBN1F70TT (accessed 9 February 2022).

Goud, N. (2019). 'Fact Sheet of LockerGoga Ransomware Which Hit Norsk Hydro'. Cybersecurity Insiders. Available at: https://www.cybersecurity-insiders.com/fact-sheet-of-lockergoga-ransomware-which-hit-norsk-hydro (accessed 9 February 2022).

GOVPH (2018), *Terms of Reference: Establishment and Operation of a Fuel Marking and Field Testing System*. Manila: Department of Finance, Bureau of Customs, and Department of Budget and Management, Philippine government. Available at: https://customs.gov.ph/wp-content/uploads/2018/06/06042018_TOR_BOC_Fuel_Marking_final.pdf (accessed 9 February 2022).

Greenberg, A. (2021). 'The Colonial Pipeline Hack Is a New Extreme for Ransomware'. WIREDy, 8 May. Available at: https://www.wired.com/story/colonial-pipeline-ransomware-attack/ (accessed 9 February 2022).

Gupte, E. (2021). 'Nigerian Parliament Passes Key Oil Reform Bill, Awaits President's Approval'. S&P Global Platts, 1 July. Available at: https://www.spglobal.com/platts/en/market-insights/latest-news/oil/070121-nigerian-parliament-passes-key-oil-reform-bill-awaits-presidents-approval (accessed 10 February 2022).

Harrup, A., and R. Whelan (2019). 'Death Toll Rises to 85 from Mexican Pipeline Explosion'. *The Wall Street Journal*, 20 January. Available at: https://www.wsj.com/articles/death-toll-rises-to-85-from-mexican-pipeline-explosion-11548035455 (accessed 9 February 2022).

Hogg, W. (2019). 'Bunkering and Banks: Once Bitten, Twice Shy?'. InfoSpectrum, 28 January. Available at: https://blog.infospectrum.net/bunkering-and-banks-once-bitten-twice-shy (accessed 9 February 2022).

Hume, N., and S. Palma (2020). 'Hin Leong Founder Says $800m of Losses Not Recorded'. *Financial Times*, 19 April. Available at: https://www.ft.com/content/3410d523-9a29-41c3-a79b-c24d15da7413 (accessed 9 February 2022).

Hume, N., S. Morris, and S. Palma (2020). 'Hin Leong Trading Files for Bankruptcy Protection', *Financial Times*, 18 April. Available at: https://www.ft.com/content/934c018a-4d81-456f-9c35-b3b068db481e (accessed 9 February 2022).

IMF (2020). 'Nigeria Staff Report for the 2020 Article IV Consultation'. IMF, 1 April. Available at: https://www.imf.org/en/Publications/CR/Issues/2019/04/01/Nigeria-2019-Article-IV-Consultation-Press-Release-Staff-Report-and-Statement-by-the-46726 (accessed 9 February 2022).

IMO (International Maritime Organization) (n.d.). 'Maritime Security'. Available at: https://www.imo.org/en/OurWork/Security/Pages/Default.aspx (accessed 9 February 2022).

INTERPOL (2014). 'INTERPOL Casebook Highlights Links between Illicit Trade and Organized Crime'. INTERPOL Trafficking and Counterfeiting Casebook 2014. Available at:

https://www.interpol.int/News-and-Events/News/2014/INTERPOL-casebook-highlights-links-between-illicit-trade-and-organized-crime (accessed 10 February 2022).

IST (Institute for Security and Technology) (2021). *Combatting Ransomware: A Comprehensive Framework for Action. Key Recommendations from the Ransomware Task Force*. Bay Area, CA: IST. Available at: https://securityandtechnology.org/ransomwaretaskforce/report/ (accessed 9 February 2022).

Jenkins, J.P. (n.d.). 'Piracy: International Law'. Britannica. Available at: https://www.britannica.com/topic/piracy-international-law (accessed 9 February 2022).

Joubert, L. (2020). 'The State of Maritime Piracy 2019'. Stable Seas, 10 July. Available at: https://www.stableseas.org/post/state-of-maritime-piracy-2019 (accessed 9 February 2022).

Katsouris, C., and A. Sayne (2013). *Nigeria's Criminal Crude: International Options to Combat the Export of Stolen Oil*. London: Chatham House. Available at: https://www.chathamhouse.org/sites/default/files/public/Research/Africa/0913pr_nigeriaoil.pdf (accessed 7 February 2022).

Khasawneh, R., and F. Ungku (2018). 'Scale of Theft at Shell's Singapore Refinery Much Greater, Court Docs Show'. Reuters, 14 December. Available at: https://www.reuters.com/article/shell-oil-theft-idINKBN1OD0I0 (accessed 7 February 2022).

Kleiman, M.A.R. (1993). 'Enforcement Swamping: A Positive-Feedback Mechanism in Rates of Illicit Activity'. Mathematical and Computer Modelling, 17(2): 65–75. https://doi.org/10.1016/0895-7177(93)90240-Y

Lam, F. (2020). 'Fuel Supplier Sentek's Founder Charged in Shell Singapore Oil Heist'. *Business Times*, 2 October. Available at: https://www.businesstimes.com.sg/energy-commodities/fuel-supplier-senteks-founder-charged-in-shell-singapore-oil-heist (accessed 7 February 2022).

Lam, L. (2021). 'Former Shell Employee Admits Conspiring to Embezzle S$49m Worth of Gas Oil from Pulau Bukom Site'. Channel News Asia, 3 February. Available at: https://www.channelnewsasia.com/news/singapore/shell-employee-pulau-bukom-refinery-gas-oil-misappropriation-13776018 (accessed 7 February 2022).

Lee, D.S. (2019). 'State of Limbo: The Uncertain Fate of the *Lighthouse Winmore*'. NK News, 22 May. Available at: https://www.nknews.org/2019/05/state-of-limbo-the-uncertain-fate-of-the-lighthouse-winmore (accessed 18 February 2022).

Lord, N. (2018). 'Data Protection 101: What is Data Exfiltration?' Data Insider blog, 11 September. Available at: https://digitalguardian.com/blog/what-data-exfiltration (accessed 13 February 2022).

Lum, S. (2022). 'Shell Bukom Heist: One Mastermind Admits to Siphoning $128m of Gas Oil'. *The Straits Times*, 8 February. Available at: https://www.straitstimes.com/singapore/courts-crime/shell-bukom-heist-one-mastermind-admits-to-siphoning-128m-of-gas-oil (accessed 9 February 2022).

Mahmud, A.H. (2021). 'Beyond the Shell Bukom Heist, a Deeper Look at How Marine Fuel Is Stolen in Singapore'. Channel News Asia, 17 January and 4 February. Available at: https://www.channelnewsasia.com/news/singapore/shell-bukom-heist-marine-fuel-bunker-theft-mpa-13829172 (accessed 7 February 2022).

Makhifi, J. Al (2013). 'Algeria Smuggling Crackdown Cuts Fuel Line to Morocco'. Arab News, 28 September. Available at: https://www.arabnews.com/news/466102 (accessed 10 February 2022).

Manifold Times (2018). 'Brightoil MGO Theft: 22 Plead Guilty at Singapore Court'. *Manifold Times*, 2 March. Available at: https://manifoldtimes.suzerin-development.com/news/brightoil-mgo-theft-22-plead-guilty-at-singapore-court/ (accessed 9 February 2022).

Mohindru, S. (2020). 'Piracy Incidents Spike around Singapore in 2019: ReCAAP'. S&P Global Platts. Available at: https://www.spglobal.com/platts/en/market-insights/latest-news/shipping/011620-piracy-incidents-spike-around-singapore-in-2019-recaap (accessed 9 February 2022).

MPA Singapore (2019). 'New Standard to Support Maritime Sector's Shift to More Sustainable Fuels'. Media Release 070/19. Singapore: MPA of Singapore. Available at:

https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/f692ed83-2ce3-420f-ae74-23a0dd201c9e (accessed 10 February 2022).

MPA Singapore (various dates). 'Port Marine Circulars'. Singapore: MPA of Singapore. Available at: https://www.mpa.gov.sg/web/portal/home/port-of-singapore/circulars-and-notices/port-marine-circulars (accessed 9 February 2022).

Mui, R., and P.G. Tay (2020). 'Coastal Oil Ex-Employees Charged with Cheating Singapore, HK Banks of over US$340m'. *Business Times*, 12 June. Available at: https://www.businesstimes.com.sg/banking-finance/coastal-oil-ex-employees-charged-with-cheating-singapore-hk-banks-of-over-us340m (accessed 9 February 2022).

One Earth Future (2020). 'Maritime Piracy Report Identifies Constantly Evolving Threat Requiring International and Inter-Agency Cooperation to Reduce Human Cost'. Available at: https://www.oneearthfuture.org/research-analysis/maritime-piracy-report-constantly-evolving-threat (accessed 9 February 2022).

One Earth Future (2021). 'Farewell to Stable Seas. A Tribute: Five Years of Sustained Impact To Date'. Available at: https://www.oneearthfuture.org/news/farewell-stable-seas-tribute-five-years-sustained-impact (accessed 9 February 2022).

One Earth Future (n.d.). 'Mission and Vision'. Available at: https://oneearthfuture.org/about/mission-and-vision (accessed 10 February 2022).

Östensson, O. (2020). 'Transparency in Extractive Industry Commodities Trading'. UNU-WIDER Working Paper 2020/172. Helsinki: UNU-WIDER. Available at: https://doi.org/10.35188/UNU-WIDER/2020/929-7 (accessed 10 February 2022).

Pouwels, A. (2021). 'Missing Trader Intra-Community Fraud'. Briefing by the Policy Department for Budgetary Affairs, requested by the CONT committee. Brussels: European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690462/IPOL_BRI(2021)690462_EN.pdf (accessed 10 February 2022).

Ralby, I.M. (2017a). 'Cooperative Security to Counter Cooperative Criminals'. Defence IQ, 21 March. Available at: https://www.defenceiq.com/naval-maritime-defence/articles/cooperative-security-to-counter-cooperative (accessed 9 February 2022).

Ralby I.M. (2017b). *Downstream Oil Theft: Global Modalities, Trends, and Remedies*. Washington, DC: Atlantic Council Global Energy Center. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2017/01/Downstream_Oil_Theft_web_0327.pdf (accessed 10 February 2022).

Ralby, I.M. (2017c). *Downstream Oil Theft: Implications and Next Steps*. Washington, DC: Atlantic Council Global Energy Center. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2017/03/Implications_and_Next_Steps_RW_0316.pdf (accessed 10 February 2022).

ReCAAP (2014/2015). 'Special Report on Incidents of Siphoning of Fuel/Oil at Sea in Asia'. ReCAAP ISC. Available at: https://www.recaap.org/resources/ck/files/reports/2014/Special%20Report%2001-2014%20(Siphoning%20Incidents).pdf (part I); https://www.recaap.org/resources/ck/files/reports/2015/Special%20Report%20on%20Siphoning%20Part%20II%20(9%20Jan%2015).pdf. (part II) (accessed 9 February 2022).

ReCAAP (2020). *Executive Director's Report 2020*. Singapore: ReCAAP. Available at: https://www.recaap.org/resources/ck/files/corporate-collaterals/ED_Report_2020_FINAL.pdf (accessed 7 February 2022).

ReCAAP (n.d.-a). 'Classification of Piracy and Armed Robbery against Ships Incidents'. Available at: https://www.recaap.org/classification_of_incidents (accessed 14 February 2022).

ReCAAP (n.d.-b). 'Interactive Incident Reports'. Available at: https://portal.recaap.org/OpenMap (accessed 9 February 2022).

ReCAAP, IFC, and RSiS (n.d.). 'Guide for tankers operating in Asia against piracy and armed robbery involving oil cargo theft'. Available at: https://www.ifc.org.sg/ifc2web/Publications/Other%20Products/Guides%20and%20Handbooks/Guide%20for%20Tankers.pdf (accessed 9 February 2022).

Reuters (2020). 'Ocean Bunkering to Suspend Marine Fuel Deliveries in Singapore: Sources'. Reuters, 16 April. Available at: https://www.reuters.com/article/us-singapore-oil-hinleong-bunker-idUSKCN21Y0ZB (accessed 9 February 2022).

Reuters and L. Chen (2021). 'Singapore Adds 23 Charges against Founder of Oil Trader Hin Leong'. Reuters, 30 April. Available at: https://www.reuters.com/business/energy/singapore-files-more-charges-against-oil-trader-hin-leong-founder-ok-lim-2021-04-30/ (accessed 9 February 2022).

Romsom, E. (2022). 'Global Oil Theft: Impact and Policy Responses'. UNU-WIDER Working Paper 2022/16. Helsinki: UNU-WIDER. https://doi.org/10.35188/UNU-WIDER/2022/147-1

Romsom, E., and K. McPhail (2020), 'The Energy Transition in Asia: Country Priorities, Fuel Types, and Energy Decisions'. WIDER Working Paper 2020/48. Helsinki: UNU-WIDER. https://doi.org/10.35188/UNU-WIDER/2020/805-4

Romsom, E., and K. McPhail (2021a). 'Capturing Economic and Social Value from Hydrocarbon Gas Flaring and Venting: Evaluation of the Issues'. WIDER Working Paper 2021/5 Helsinki: UNU-WIDER. https://doi.org/10.35188/UNU-WIDER/2021/939-6

Romsom, E., and K. McPhail (2021b). 'Capturing Economic and Social Value from Hydrocarbon Gas Flaring and Venting: Solutions and Actions'. WIDER Working Paper 2021/6 Helsinki: UNU-WIDER. https://doi.org/10.35188/UNU-WIDER/2021/940-2

Rozhov, K., and M. Strzelecki (2013). 'Fuel Fraud Costing Europe More Than $4 Billion in Lost Taxes'. Bloomberg, 28 August. Available at: https://www.bloomberg.com/news/articles/2013-08-26/fuel-smugglers-costing-europe-more-than-4-billion-in-lost-taxes (accessed 10 February 2022).

Russon, M.-A. (2021). 'US Fuel Pipeline Hackers "didn't mean to create problems"'. BBC News, 10 May. Available at: https://www.bbc.com/news/business-57050690 (accessed 9 February 2022).

Sahu, S., and A. Tan (2020). 'Bunker Fuel Quality Issues Surge as VLSFO Use Gathers Pace: Sources'. S&P Global Platts, 3 February. Available at: https://www.spglobal.com/platts/en/market-insights/latest-news/oil/020320-bunker-fuel-quality-issues-surge-as-vlsfo-use-gathers-pace-sources (accessed 9 February 2022).

Samaritis, K. (2016). 'Cargo Contamination on Tankers'. *The Standard*, May. Available at: https://www.standard-club.com/fileadmin/uploads/standardclub/Documents/Import/publications/standard-safety/2016/2150483-standard-safety-tankers-may-2016.pdf (accessed 7 February 2022).

See, K.O.J. (2021). 'Grounds of Decision: Prime Shipping Corp versus Public Prosecutor'. [2021] SGHC 71. High Court of the Republic of Singapore, 22 January, 4 February, and 29 March. Available at: https://www.elitigation.sg/gd/s/2021_SGHC_71 (accessed 7 February 2022).

Semple, K. (2019), 'Mexico Declares Victory over Fuel Thieves. But Is It Lasting?'. *The New York Times*, 5 May. Available at: https://www.nytimes.com/2019/05/05/world/americas/mexico-fuel-theft.html (accessed 9 February 2022).

Shell (n.d.). 'Shell Energy and Chemicals Park Singapore'. Singapore: Shell. Available at: https://www.shell.com.sg/about-us/projects-and-sites/pulau-bukom-manufacturing-site.html (accessed 7 February 2022).

Ship & Bunker (2015). 'Singapore Bunker Supplier Tankoil Declared Bankrupt, "Milestone" Hailed for OW Bunker Proceedings'. *Ship & Bunker*, 7 August. Available at: https://shipandbunker.com/news/world/208494-singapore-bunker-supplier-tankoil-declared-bankrupt-milestone-hailed-for-ow-bunker-proceedings (accessed 9 February 2022).

Ship & Bunker (2018). 'Bad Bunkers: As Many as 200 Vessels Now Affected'. *Ship & Bunker*, 27 August. Available at: https://shipandbunker.com/news/world/292849-bad-bunkers-as-many-as-200-vessels-now-affected (accessed 9 February 2022).

Ship & Bunker (2020). 'True Savings from Singapore MFM Rules, Closer to US$1.7b: Tolson'. *Ship & Bunker*, 20 October. Available at: https://shipandbunker.com/news/apac/483400-true-savings-from-singapore-mfm-rules-closer-to-us17b-tolson (accessed 9 February 2022).

Slowik, J. (2019). 'CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack'. Dragos Inc, 15 August. Available at: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf (accessed 9 February 2022).

Soud, D., I. Ralby, and R. Ralby (2020). *Downstream Oil Theft: Countermeasures and Good Practices*. Washington, DC: Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/downstream-oil-theft-countermeasures-and-good-practices/ (accessed 7 February 2022).

S&P Global Platts (2022). 'Specifications Guide: Asia Pacific and Middle East Crude Oil'. Available at: https://www.spglobal.com/platts/plattscontent/_assets/_files/en/our-methodology/methodology-specifications/apag-crude-methodology.pdf (accessed 7 February 2022).

Stracqualursi, V., G. Sands, and A. Saenz (2021). 'Cyberattack Forces Major US Fuel Pipeline to Shut Down'. CNN Politics, 8 May. Available at: https://edition.cnn.com/2021/05/08/politics/colonial-pipeline-cybersecurity-attack/index.html (accessed 9 February 2022).

Tang, L. (2021). '2 Ex-Shell Employees Jailed over S$200m Marine Fuel Heist at Pulau Bukom Refinery'. Today Online, 5 July. Available at: https://www.todayonline.com/singapore/2-ex-shell-employees-jailed-over-s200m-marine-fuel-heist-pulau-bukom-refinery (accessed 7 February 2022).

Tidy, J. (2021). 'The Ransomware Surge Ruining Lives'. BBC News, 30 April. Available at: https://www.bbc.com/news/technology-56933733 (accessed 9 February 2022).

UNODC (2013). 'Transnational Organized Crime in West Africa: A Threat Assessment'. Vienna: UNODC. Available at: https://www.unodc.org/documents/data-and-analysis/tocta/West_Africa_TOCTA_2013_EN.pdf (accessed 7 February 2022).

UNSC (2016). 'Piracy and Armed Robbery in the Gulf of Guinea'. New York: United Nations Security Council (UNCSC) 7675th meeting, 25 April. Available at: https://www.securitycouncilreport.org/atf/cf/ per cent7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9 per cent7D/s_pv_7675.pdf (accessed 9 February 2022).

VanderWolk, J. (2021). 'Global Consistency on Carbon Tax: A Role for the OECD's Inclusive Framework? (Correct)'. Bloomberg, 6 April. Available at: https://news.bloombergtax.com/daily-tax-report/global-consistency-on-carbon-tax-a-role-for-the-oecds-inclusive-framework (accessed 10 February 2022).

Volz, D., R. McMillan, and C. Eaton (2021). 'Colonial Pipeline Said to Pay Ransom to Hackers Who Caused Shutdown'. *The Wall Street Journal*, 13 May. Available at: https://www.wsj.com/articles/colonial-pipeline-expects-to-fully-restore-service-thursday-following-cyberattack-11620917499 (accessed 9 February 2022).

Wagstaff, J. (2014). 'All at Sea: Global Shipping Fleet Exposed to Hacking Threat'. Reuters, 24 April. Available at: https://www.reuters.com/article/tech-cybersecurity-shipping-idUSL3N0N402020140423 (accessed 9 February 2022).

Walje, M. (2014). 'OBP [Oceans Beyond Piracy] Notes a Worrying Spread of STS [Ship-to-Ship] Oil Theft in SE Asia'. One Earth Future, 1 October. Available at: https://www.oneearthfuture.org/research-analysis/obp-notes-worrying-spread-sts-oil-theft-se-asia (accessed 9 February 2022).

Wang, J.-Y. (1994). 'Macroeconomic Policies and Smuggling: an Analysis of Illegal Oil Trade in Nigeria'. Working Paper No 94/115. Washington, DC: IMF. https://doi.org/10.5089/9781451942880.001. Available at: https://www.imf.org/en/Publications/WP/Issues/2016/12/30/Macroeconomic-

Policies-and-Smuggling-An-Analysis-of-Illegal-Oil-Trade-in-Nigeria-1304 (accessed 7 February 2022).

Yucatan Times (2019). 'Where Does the Term "Huachicolero" Come From?'. 12 January. Available at: https://www.theyucatantimes.com/2019/01/where-does-the-term-huachicolero-come-from/ (accessed 9 February 2022).

Zetter, K. (2014). 'Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon'. Crown Publishing Group, press release. Available at: https://crownpublishing.com/archives/news/countdown-zero-day-kim-zetter (accessed 9 February 2022).

Zhou O. (2021). 'China's Apr Light Cycle Oil Imports Hit Record High 2 mil mt ahead of New Tax'. S&P Global Platts, 21 May. Available at: https://www.spglobal.com/platts/en/market-insights/latest-news/petrochemicals/052121-chinas-apr-light-cycle-oil-imports-hit-record-high-2-mil-mt-ahead-of-new-tax (accessed 10 February 2022).

Zuza, D. (2021). 'The Impressive Tunnelling Skills of Mexico's Gas Thieves'. InSight Crime, 16 April. Available at: https://insightcrime.org/news/underground-tunnels-discovered-mexico-reveal-sophistication-oil-theft-networks/ (accessed 9 February 2022).

Abbreviations and units

ADF	automotive diesel fuel
AIS	automatic identification system
API	American Petroleum Institute
bbl	barrel (1 bbl is 0.159 m^3)
BDN	bunker delivery notes
bn	billion
bpd	barrels per day
BS&W	basic sediment and water
DRM	domestic resource mobilization
ECA	emission control areas (under MARPOL regulations)
ECCAS	Economic Community of Central African States
ECOWAS	Economic Community of West African States
ECTS	electronic cargo tracking and security system
EITI	Extractive Industries Transparency Initiative
GGC	Gulf of Guinea Commission
IFC	Information Fusion Centre (on maritime incidents in SEA)
IFN	Information Network System (ReCAAP)
IFO	intermediate fuel oil
IMF	International Monetary Fund
IMO	International Maritime Organization
ISC	Information Sharing Centre by ReCAAP
LCO	light cycle oil
LNG	liquified natural gas
LPG	liquefied petroleum gas
m	million
MARPOL	International Convention for the Prevention of Pollution from Ships
MDO	marine diesel oil
MFM	mass-flow meter
MFO	marine fuel oil
MGO	marine gasoil
MOWCA	Maritime Organization of West and Central Africa,
MPA	Marine and Port Authority of Singapore
MTIC	Missing trader intra-community (fraud)
NFT	non-fungible token

NGO	non-governmental organization
OT	operational technology
Pemex	Petróleos Mexicanos (Mexico's national petroleum company)
PLC	programmable logic controller
PPMS	petroleum product marking scheme
RaaS	ransomware as a service
ReCAAP	Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia
RSiS	S. Rajaratnam School of International Studies, Singapore
RTF	Ransomware Task Force
SDG	sustainable development goal (as defined by the UN)
SEA	South-East Asia
SSAS	ship security alert system
STS	ship-to-ship (transfer of oil)
TRACIT	Transnational Alliance to Combat Illicit Trade
UNODC	United Nations Office on Drugs and Crime
VLCC	very large crude carrier

Appendix: ReCAAP incident severity category description, including level of violence and economic loss incurred

CAT 1—CAT 1 incidents involved large number of perpetrators; more than 9 men in 4 out every 10 incidents and 4–9 men in the other six incidents. The perpetrators were mostly armed with guns and knives, and the crew is likely to suffer some form of injury or physical violence such as being assaulted or tied up or threatened. In term of losses, the ship was either hijacked or the cargo on board was stolen, for example siphoning of cargo oil.

CAT 2—Majority of CAT 2 incidents involved 4–9 men who are likely to be armed with knives/machetes and in 1/4 of the incidents, armed with guns. The crew is likely to be threatened or held hostage temporarily to allow the perpetrators to steal the crew's cash and ship's property including engine spares. In a few cases, the crew suffered some form of injury or physical violence but less severe in nature compared with CAT 1 incidents.

CAT 3—The number of perpetrators involved in CAT 3 incidents usually involved groups of … 1–6 men. At times, the perpetrators were armed with knives/machetes/others or other items such as sticks, rods, bats etc. The crew was not harmed, although there were cases of crew subject to duress during the incident but not harmed physically. In almost half of the CAT 3 incidents, the perpetrators were unable to steal anything from the vessel, but in cases where losses were reported, stores and engine spares were the commonly targeted items.

CAT 4—The perpetrators were not armed and the crew not harmed. More than half of CAT 4 incidents involved … 1–3 men who escaped empty-handed upon [being] sighted by the crew.

This classification of incidents allows the ReCAAP ISC to provide some perspective on the piracy and armed robbery situation in Asia and to facilitate the maritime community to carry out risk assessment.

Source: ReCAAP (n.d.-a).