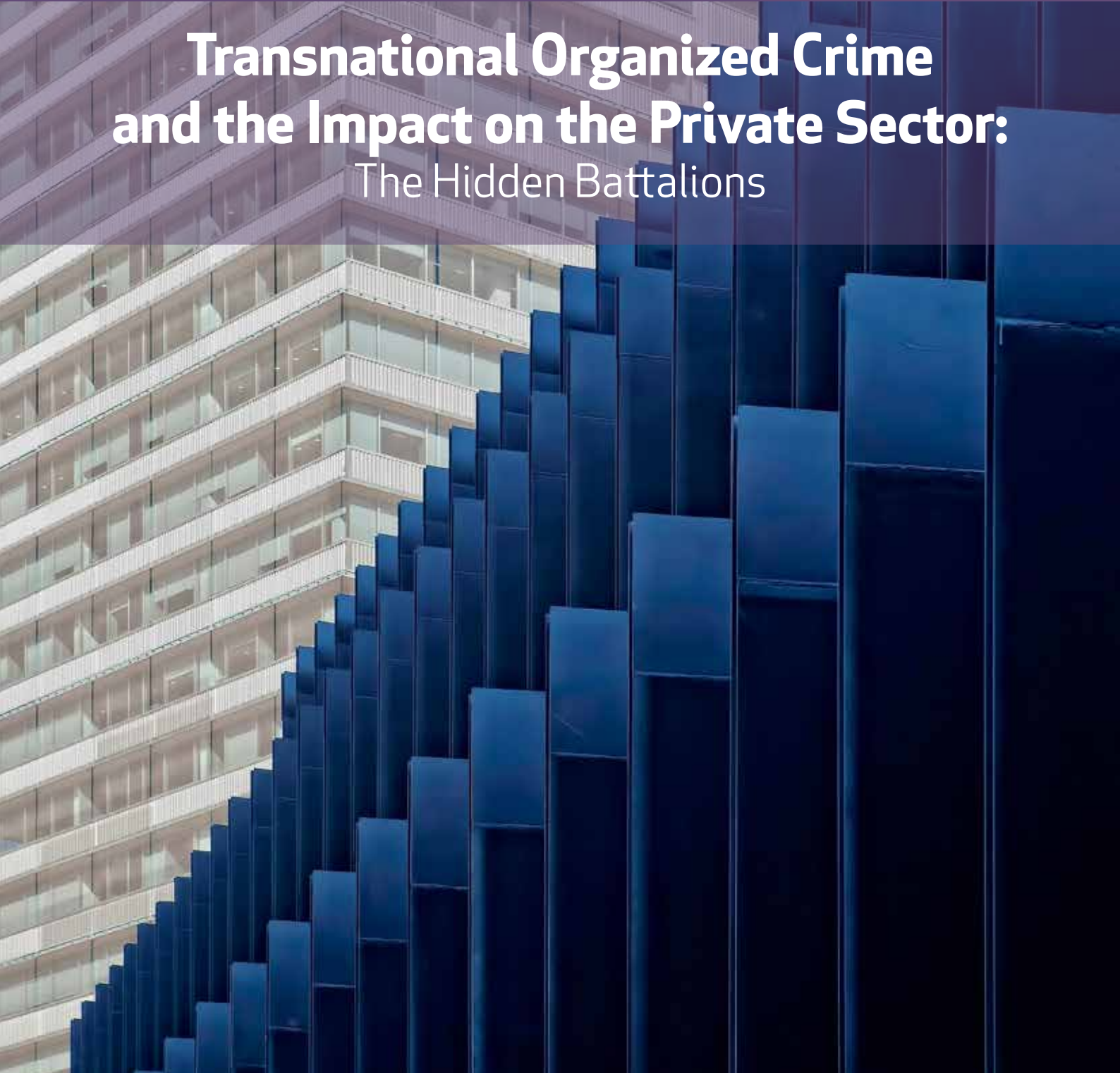


THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

Transnational Organized Crime and the Impact on the Private Sector: The Hidden Battalions



December 2017

Photo by Ricardo Gomez Angel CC0 1.0 Universal CC0 1.0 (<https://creativecommons.org/publicdomain/zero/1.0/>),
via Unsplash

© 2017 Global Initiative against Transnational Organized Crime. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global Initiative. Please direct
inquires to:

The Global Initiative against Transnational Organized Crime
WMO Building, 2nd Floor
7bis, Avenue de la Paix
CH-1211 Geneva 1
Switzerland

www.globalinitiative.net



Acknowledgements

This report was drafted by Robin Cartwright and Frances Cleland Bones for the Global Initiative. The authors drew heavily on the expertise of members of the Global Initiative's Private Sector Reference Group, in particular Nick Lewis OBE of Standard Chartered Bank and Jeff Frazier formerly of CISCO, now of smart City Media.

The authors would also like to thank the many private sector representatives who gave their time and comments to the sector studies.

Thanks also go to Claudio Landi for his tireless work on layout and presentation.



Executive Summary

This paper is based on a detailed review of the scale and nature of organised crime's infiltration of the private sector. These findings are a 'call to arms' for the international private and public sectors to transform their co-operation and teamwork.

We have adopted a practical definition of organized crime as that which is carried out by a group of people, suspected of serious criminal offences, over a prolonged period, motivated by profit or power.

In our analysis of six major private sector industries, six specific forms of organised crime stood out as either having material impact on the private sector, or using the private sector as facilitators.

Money laundering is the process of making dirty money look clean. One estimate puts it at 2% of global GDP – c.\$1.5 trillion. Money-laundering is an 'enabling crime', facilitating organized crime (as well as terrorism) with social and economic costs.

Asset misappropriation refers to stealing from businesses. For example, cargo thefts cost as much as \$30 billion in losses each year worldwide.

Counterfeiting and contraband, whilst thought of as being a consumer goods crime, is rife in a broad range of sectors, in particular technology products and pharmaceuticals, to devastating effect. It is estimated by OECD at \$461 billion, or 2.5% of world trade.

Fraud and extortion remain strongly present in the financial, construction and real estate industries. In construction extortion could account for of 20–30 per cent of lost project value.

Human trafficking. High volume, low skilled labour enterprises such as construction and building, have the highest penetration of trafficking incidence in the private sector.

Cyber Crime. Hacking attacks cost the average American firm \$15.4 million per year over. In 2015 68,000 URLs containing child sexual exploitation and abuse (CSEA) images were hosted online on 1,991 domains. The reputational impact means major tech companies apply significant collaborative resources to weeding out criminal, terrorist and CSEA activity.

Key Findings:

Finding#1: The Scale and Impact of Crime in the Private Sector is Truly Staggering. A conservative estimate of the value of organized crime was \$3.6-\$4.8 trillion, in 2015/2016, 7% of global GDP. The broader impact of organized crime is difficult to assess as it is multi-dimensional, and shared across the private, public sector, and society itself. The impact on the private sector only – in terms of revenue loss – is estimated at c\$130 billion.

The Institute of Economics and Peace (IEP) calculated the financial cost of terrorism at over \$52 billion in 2014. A conservative estimate of total transnational organized crime is \$870 billion a year. This is more than six times the amount of official development assistance and close to 7% of the world's exports of merchandise



Finding #2 Private sectors are either facilitators or targets. Crimes are either done 'to' private sector organisations, or 'through' them. Sectors are either the targets of fraud or asset theft themselves, particularly in construction, consumer goods (\$460 billion counterfeit goods), and financial card fraud, or they facilitate crime unwittingly, through use of technology networks by fraudsters to target victims, e.g. the real estate sector laundering dirty funds or the transport industry moving illicit goods.

Regulation varies between the 'victim' and 'enabling' industries. Laws are in place to criminalise the use of the private sector for technology or money laundering crime. The victim industries, however, often are reliant on existing laws around theft, or copyright infringement, which are not tailored to the activities of TOC groups and tend to have lower penalties for infringement.

Finding #3 Organized crime's impact on the private sector is growing not shrinking. Counterfeit goods have risen from \$250 billion to \$461 billion in the last 8 years. Asset theft in the transport and logistics theft rose by over 90% 2015 to 2016. There is a sense that regulation is not working: money laundering seizures equated to 0.2% of all laundered funds in one study; and after the dark web's Silk Road was taken down, many sites sprung up to take on and indeed grow the trade.

Finding #4 Direct impact of Crime Disproportionately felt in the global south. Sweatshops flourish in South Asia; trafficking of labour and sex workers originates predominantly in Africa, Asia and Eastern Europe; corruption in natural resources damages production in Africa and the Caucasus; technology fraud is driven from eastern and southern Europe, West Africa and the Middle East. Whereas in developed economies counterfeit drugs may comprise less than 0.2 percent of the market developing markets are often beset by 30% fakes, as a UNODC report showed for anti-malarial drugs in Africa.

Globalization is increasing the 'attack surface' for TOC groups. The abuse of the often weaker regulatory regimes in the Global South by TOC groups further increases the risk for the private sector operating in these areas.

Finding #5 Responses re confrontational rather than collaborative. There are very few examples of successful public and private sector co-operation against TOC groups. Private sector organisations complain that communication with the law enforcement sector is one-way and that the regulatory reporting burden, designed to combat crime, can act as a deterrent to co-operation. Tangible results have been seen when industries take the lead on disrupting the work of TOC groups, such as TAPA the Transported Asset Protection Association

We recommend a concerted effort to measure and communicate the incidence of organised crime that examines the full spectrum of private sector incidence and cost from organised crime.

Public/Private sector co-operation should be kick-started by a series of sector-specific joint events, attended by regulators, law enforcers and the private sector to identify the potential for further co-operation.

Following sector specific strategies, we recommend a cross-sector dialogue is pursued to enable learning from alternative approaches, along key themes

Industry bodies should do more to offer leadership and innovation in combatting organised crime in their supply chains

We recommend a cross industry dialogue to establish 'test cases' for systemic supply chain protection using technologies such as product level track and trace, authentication marking and labelling, and accreditation/verification of supply chain participation.



“When sorrows come, they come not single spies
but in battalions”.

[Shakespeare, *Hamlet*]



Global Initiative Against Transnational Organized Crime

Transnational Organized Crime and the Impact on the Private Sector: The Hidden Battalions



Table of Contents

Introduction	1
Defining of Organized Crime and Illicit Trade	2
Typology of Organized Crime in the Private Sector	4
Key Findings	10
Recommendations	17
Industry Case Studies	
 Financial Services	18
 Technology	26
 Consumer Goods and Retail	37
 Construction and Real Estate	44
 Transport and Logistics	54
 Natural Resources	62

Acronyms

AML	Anti Money Laundering
BASCAP	Business Action to Stop Counterfeiting and Piracy
BBA	British Bankers' Association
CAGR	Compound Annual Growth Rate
CIOB	Chartered Institute of Building
CSEA	Cyber Security Enhancement Act
DDoS	Dedicated Denial of Service
EFCC	Economic and Financial Crimes Commission
EITI	Extractive Industries Transparency Initiative
EMEA	Europe, Middle East and Africa
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCPA	Foreign Corrupt Practices Act
FMCG	Fast-moving Consumer Goods
FMD	Falsified Medicines Directive
FSR	Freight Security Requirements
HMRC	Her Majesty's Revenue and Customs
IEP	The Institute of Economics and Peace
ILO	International Labour Organization
IMIA	International Association of Engineering Insurers
IOCs	International Oil Companies
JMLIT	Joint Money Laundering Intelligence Taskforce
LEDCs	Less Economically Developed Countries
MEDCs	More Economically Developed Countries
NAFDAC	National Agency for Food and Drug Administration and Control
NCA	National Crime Agency
NOCs	National Oil Companies
NVDRS	National Violent Death Reporting System
OECD	Organisation for Economic Co-operation and Development
PPP	Public Private Partnership
PWYP	Publish What You Pay
SARs	The Suspicious Activity Reports
SCADA	Supervisory Control and Data Acquisition
STORs	Suspicious Transaction and Order Reporting
TAPA	Transported Asset Protection Association
TIC	Tenancy in Common
TOC	Transnational Organized Crime
TSR	Trucking Security Requirements
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office against Drugs and Crime
UNTOC	UN Convention on Transnational Organized Crime
WEF	World Economic Forum
WHO	World Health Organization
WTO	World Trade Organization



Introduction

Since the UN Convention against Transnational Organized Crime (UNTOC) was ratified in 2000, much focus has been given to understanding the challenges presented by the scale and seriousness of this concerted and insidious crime type. These analyses tend to attempt to quantify the size of illicit markets or the trafficking routes of illegal commodities. Yet, while some focus has been placed on mapping the criminal groups and gangs who facilitate or profit from organised crime, very little attention has been placed on studying or learning from the private sector.

TOC groups make exceptionally thorough use of private sector networks to commit, harbour, launder and facilitate crime. Research suggests that across the private sectors we have studied, the scale of organized crime is \$3.6-\$4.8 trillion.

This staggering private sector crime incidence appears to be under-recognised. Governments and law enforcers make relatively limited use of their private sector colleagues in monitoring, investigating and ultimately preventing TOC groups' infiltration of the private sector. The complex web of national responsibilities between different regulators and law enforcers, and indeed the complexity of the private sector itself, act as barriers to any accessible, transnational system of intelligence-sharing and remediation. The TOC groups committing these crimes suffer no such organisational and national barriers, and are run by individuals with no shortage of business skills and entrepreneurial flair.

Criminal activity at this level of economic impact has much wider ramifications than mere marginal losses to Profit and Loss statements: these crimes present fundamental barriers to sustainable development as defined in the UN Sustainable Development Goals.

This paper is based on a detailed review of six private sector industries. It brings together a combination of desk-based reporting and interviews with officials from relevant private and public industries. The report lays out in greater detail the evidence around the scale and nature of organised crime's infiltration of the private sector; it will examine the nature of responses highlighting both good practices and gaps; and, finally, it will provide some practical recommendations to be taken forward by the private sector, the public sector, and the two in collaboration.

These findings are a 'call to arms' for the international private and public sectors to transform their co-operation and teamwork. Both sectors have an exceptional level of expertise and will to defeat this level of injustice. The work that remains incomplete is the effective harnessing of these mutual skills.



1. Defining Organized Crime and Illicit Trade

Organized crime as a paradigm has nearly as many definitions as it has attempts to define it. The UNTOC focused on defining a criminal group, rather than providing a definition of organized crime itself. According to UNTOC, an organized crime group is:

“a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit.”

The UN's definition of TOC is built on a European approach of focusing on the illegal enterprise. The EU developed a grid of 11 characteristics in 1997, considering organized crime to be present if six characteristics were present of which 1, 3, 5 and 11 were considered mandatory:

1. Collaboration of more than two people;
2. Each with their own appointed tasks;
3. For a prolonged or indefinite time;
4. Using some form of discipline or control;
5. Suspected of the committing of serious criminal offences;
6. Operating on an international level;
7. Using violence or other means suitable for intimidation;
8. Using commercial or business-like structures;
9. Engaged in money laundering;
10. Exerting influence on politics, the media, public administration, judicial authorities or the economy;
11. Motivated by the pursuit of profit or power.

Whilst complex, this definition allows us some necessary flexibility. For example, for this paper we are focusing on organized crime, not limiting the scope to transnational organized crime. There is also danger in too tightly defining the nature of the organized crime group. As the United Nations High Level Panel on Threats, Challenges and Change noted in 2004,¹

“Organized crime is increasingly operating through fluid networks rather than more formal hierarchies, and the increasingly prevalent range of cyber-enabled crimes can be effectively conducted by a single perpetrator.”

One of the oddities of the study of organized crime's effect on, and use of, the private sector is why researchers and commentators, both from the public and private sector, so often focus solely on studying 'illicit trade', as opposed to the much broader and impactful 'organized crime'.

1 Organized Crime: A Contested Concept, by Letizia Paoli and Tom Van der Beken, 2014, in Oxford Handbook of Organized Crime



It is noteworthy that there are a plethora of reports and events by various bodies on illicit trade – by the UNODC, OECD and others – yet this research project found only one event focused on organized crime in the private sector: a UNODC meeting in Vienna in 2011.

Illicit trade refers very specifically to theft or copying, normally of a physical product and is defined by the WHO (for tobacco products) as:

“Any practice or conduct prohibited by law and which relates to production, shipment, receipt, possession, distribution, sale or purchase, [of product] including any practice or conduct intended to facilitate such activity”²

Perhaps because it is tangible and, to an extent, visible, commentators tend to focus their efforts on illicit trade much more readily than the broader organized crimes of fraud, money laundering, extortion, or even drugs and arms trafficking (which tend to be omitted from illicit trade coverage), although they do observe links between illicit trade and organized crime:

“With the combination of high profits and low penalties resulting from a greater social tolerance compared to other crimes, the illicit trafficking of counterfeit goods is an attractive money-making avenue for organized criminal groups. In some instances, the illicit trafficking of counterfeit goods is more profitable than other illegal activities, such as the trafficking and sale of narcotic drugs, people and weapons.”³

But focus on illicit trade can, unintentionally, focus attention on this one asset or intellectual product theft, and neglect the broader infiltration of organized crime in business. The scale of illicit trade is significant, but of organized crime, is greater. The recent World Economic Forum (WEF) Global Agenda Council on Illicit Trade (2012–2014) estimated all counterfeit trade to be worth \$650 billion.⁴ Our study of organized financial crime alone estimates its scale at \$2.1 trillion. And these figures only represent the market size of the crime and not the monetary impact on the private sector, the wider societal impact, or the consequent regulatory cost and burden (all of which are discussed later in this report.)

We also do not stick to the strict definition of “serious crimes”. UNTOC defines serious crimes as

“conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.”

Thus, the seriousness of the offence is judged wholly by the judicial remedy, not taking into account the gravity of the criminal act or its impact on society. In practice, relying on highly variable sentencing practices to define “serious crime” is flawed.

In short, we have adopted a practical definition of organized crime as that which is carried out by a group of people, suspected of serious criminal offences, over a prolonged period, motivated by profit or power.

2 Combating the illicit trade in tobacco products from a European perspective, WHO, Regional Studies Series, undated

3 UNODC The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime, FactSheet

4 State of the Illicit Economy Briefing Papers, WEF, 2015

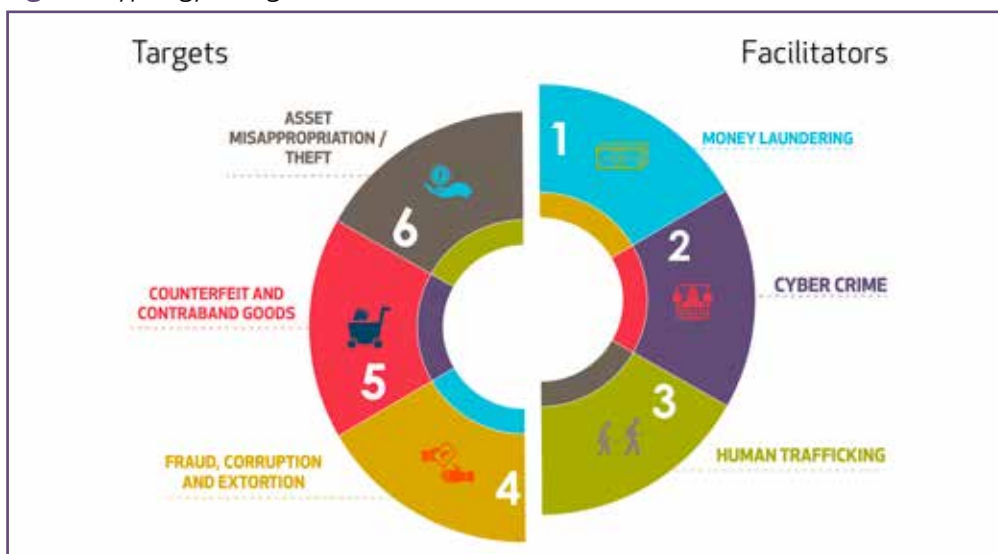


2. Typology of Organized Crime in the Private Sector

Our study of the literature on organized crime has been driven by a research focus on assessing crime according to the prevalence and impact each or any individual crime has on an underlying industrial sector.

These crimes are indeed well covered in literature and commentary by, for example, UNODC, OECD, WEF and many others, but the focus is invariably on a broad, albeit Global North, incidence of the crimes, but very rarely the private sector incidence (with the notable exception of money laundering, for obvious reasons). Moreover, each significant crime area has its own set of legislation and often a different corresponding enforcement regime in the public sector.

Figure 1: Typology of Organised Crime in Private Sector



This leads to a 'silo' focus on individual crime types, which is further perpetuated by fragmented legislation and regulation. Human trafficking legislation is represented, for example, by the UK Modern Slavery Act 2015 or the California Transparency in Supply Chains Act in the US. Money laundering, is legislated by the SARs regime from the Proceeds of Crime Act 2002, the Terrorism Act 2000, or STORs under the Market Abuse Regulation in the UK (each reporting to a different government body). Bribery and corruption are legislated by FCPA in the US or the Bribery Act in the UK.

The great irony is that the TOC groups who perpetrate these crimes have no such organizational divisions to impede them. Studies have shown that TOC groups which, say, smuggle counterfeit cigarettes, also indulge in trafficking and other crimes. Few are focused on a single crime. Research by the Counter Terrorism Institute in the Hague has shown that not only do TOC groups cross multiple crime areas, many overlap with terrorist activities. Two categories of organized crime, drugs and firearms trafficking, did not present directly in the literature, as the private sector experience of these crimes is either as unwitting financial or logistics providers for these crimes.



Money Laundering

Money laundering “involves taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities. Simply put, money laundering is the process of making dirty money look clean”⁵

Money laundering is not the ‘original’ crime. All these proceeds are from original ‘predicate’ crimes, from human trafficking, through extortion and fraud. Whilst it is a crime in its own right, it is important to note the danger of double-counting the money laundering incidence with the predicate crime.

One estimate of money laundering puts it at 2% of global GDP – c.\$1.5 trillion.⁶ The UN, in 2005, cited a range of \$500 billion to \$1 trillion for money laundering alone.⁷ To put this into context, given US dominance, half of this figure can be expected to have passed through US institutions, in other words \$250 billion to \$500 billion. Yet the lower of these figures is larger than the total estimate (in 20002) of \$209 billion of all criminal activity, not only organized crime: cocaine, fraud, heroin, prostitution, vehicle theft, robbery, etc.

In short, money laundering estimates appear to represent the broadest definition of the scale of organized crime. In that sense, it is the ‘mother’ of organized crime in the private sector, and our best efforts of sizing the money laundering market are a convenient shorthand to a definition of the sizing of the proceeds of organized crime itself.

Despite this, money laundering is often seen as a white-collar crime, and in terms of the outlook of the criminal justice sector, often ranks behind trafficking and sexual crimes because of their human impact. But in fact, following the money takes you into the heart of organized crimes:

“Money-laundering, particularly, is an ‘enabling crime’, facilitating organized crime (as well as terrorism) with social and economic costs to the UK estimated to be at least £24 billion a year It supports, among other crimes, drugs, people and firearms trafficking, organized illegal immigration, large-scale and high-volume fraud and other financial crimes, counterfeit goods (including medicines), organized acquisitive crime and cybercrime.”⁸

Asset misappropriation / theft

Asset misappropriation, put simply, mostly refers to stealing from businesses. Theft is most commonplace in the transport and logistics and construction sectors. Cargo crime is one of the biggest supply chain challenges for manufacturers of high-value, high-risk products and their logistics service providers.⁹ Industry experts estimate cargo thefts cost as much as \$30 billion in

5 Risks and Methods of Money Laundering and Terrorist Financing. Association of Certified Anti-Money Laundering Specialists (ACAMS). 2007.

6 Bloomberg, “Why the World is so Bad at Tracking Dirty Money” February 2015

7 Essay: Money Laundering, Michael Levi and Peter Reuter, University of Chicago, 2006

8 Future Financial Crime Risk, Lexis Nexis Risk Solutions for BBA, Nov 2015

9 Transport Asset Protection Association (TAPA) <http://www.tapaonline.org/about-us>



losses each year worldwide. Whilst often insured, this crime has significant economic repercussions to consumers, businesses and, of course, victims of the consequential other crimes it funds.

The construction industry is highly susceptible to asset appropriation, and it remains the most highly reported crime in the industry – 76% of respondents to a 2014 crime survey in the construction and engineering sector reported suffering asset theft, the highest of any sector surveyed.¹⁰

As far back as 2005, sources in America estimated the loss to the US construction industry of plant and equipment exceeded \$1bn a year not including consequential losses. These losses, including hire of replacement equipment, loss of business, worker and client claims for resulting damage and injuries, increased insurance premiums¹¹ and the replacement of expensive equipment¹², can multiply these direct costs by a factor of ten – £800m a year estimated in the UK¹³ and more US\$9bn in Europe in 2015.¹⁴

Counterfeit (and contraband) goods

Whilst thought of as being a consumer goods crime, counterfeiting is rife in a broad range of sectors, in particular technology products and pharmaceuticals, to devastating effect.

A 2016 study for the OECD by Business Action to Stop Counterfeiting and Piracy (BASCAP)¹⁵ estimated a rise of global counterfeiting to \$461 billion, or 2.5% of world trade, with music, movies, software, clothing and accessories, and cosmetics/perfume being the most frequently counterfeited products.

In terms of counterfeit pharmaceuticals, the incidence is more targeted at specific developing countries. Whereas in developed economies counterfeits may account for less than 0.2 percent of the market¹⁶, developing markets are often beset by 30% fakes, as a UNODC report showed for anti-malarial drugs in Africa. More than 120,000 people a year die in Africa as a result of fake anti-malarial drugs alone, says the WHO, either because the drugs were substandard or simply contained no active ingredients at all.¹⁷ According to a report by Global Financial Integrity, unrecorded oil sales may amount to over 500,000 barrels a day, or 183 million barrels per a year.¹⁸

10 Fighting corruption and bribery in the construction industry, PwC, 2014

11 Plant Theft costing UK Construction Industry over £800 Million a Year. Construction National. <http://www.constructionnational.co.uk/security/1953-plant-theft-costing-uk-construction-industry-over-p800-million-a-year>

12 Crime in the construction industry, CIOB, 2007

13 Allianz Cornhill in December 2016

14 Plant Theft costing UK Construction Industry over £800 Million a Year. Construction National. <http://www.constructionnational.co.uk/security/1953-plant-theft-costing-uk-construction-industry-over-p800-million-a-year>

15 Trade in Counterfeit and Pirated Goods, Mapping the Economic Impact, OECD/EUIPO, 2016

16 Illicit Trade in Counterfeit Medicine, Dr. K Lybecker, Colorado College, 2015

17 Counterfeit drugs: 'People are dying every day'. Matthew Wall. BBC News. 27 September 2016 <http://www.bbc.co.uk/news/business-37470667>

18 The Threat of Organized Crime to the Oil Industry, Future Directions International, 29 November 2012



Fraud and extortion

With a strong link to TOC groups, the financial, construction and real-estate industries remain highly penetrated by fraud. In the financial sector, card fraud has risen dramatically as the use of payment cards became commonplace since the 1970s. Total card fraud losses in the EU in 2013 were €1.33bn, in US €4.148bn. Card Fraud is usually organized by criminal groups rather than individuals. Whilst fraud losses are, in many cases, insurable events, the costs of cover are subsequently built into financial product costs which, in turn, penalize the individual and the institution.

The impact of extortion is increasingly felt across the full gamut of industry sectors, particularly construction, technology and financial services. Although, it is hard to quantify in hard terms the impact of extortion on the construction industry, one estimate suggests extortion could account for, of 20–30 per cent of lost project value.¹⁹ The impact of this kind of financial loss on projects, particularly in the developing world, highlights the degree to which crime can inhibit progress in less economically developed countries (LEDCs).

Extortion-driven hacking attacks cost the average American firm \$15.4 million per a year, double the global average of \$7.7 million. The most costly cybercrimes were those carried out by malicious insiders, dedicated denial of service (DDoS) and web-based attacks. The global financial services and energy sectors were hit the worst, with average annual costs of \$13.5 million and \$12.8 million, respectively.²⁰

Human trafficking

High-volume, low-skilled labour enterprises, such as construction and building, have the highest penetration of trafficking incidence in the private sector. Here, the private sector itself is sometimes at fault. One construction manager described his sector in the following, less than favourable, terms:

“Our sector is rife with human rights abuses. Bonded labour, delayed wages, abysmal working and living conditions, withholding of passports and limitations of movement are all forms of modern slavery. Many in positions of influence and power are turning a blind eye to obviously forged documents, even on large-scale projects. In doing so, they are not only colluding in exploitation, they are supporting organized crime.”²¹

Forced labour and human trafficking are also found in natural resources and allied industries. Of the 14.2 million trafficking victims exploited for labour, 7.1 million (50%) forced labour victims work in construction, manufacturing, mining or utilities.²² The costs of combatting this crime for businesses is growing. Companies covered by the French Duty of Care law, the Dutch Due

19 Corruption and collusion in construction: a view from the industry, Engineers Against Poverty, 2014 (Also source below)

20 The Rising Costs of Cyber Crime, Ponemon Institute Cost of Cyber Crime Study, 2016, <http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/>

21 Modern Slavery: The Dark Side Of Construction, CIOB, 2015, <https://policy.ciob.org/wp-content/uploads/2016/02/CIOB-Research-The-Darkside-of-Construction.pdf>

22 Human Trafficking by the Numbers, Human Rights First, January 2016



Diligence Child Labour Law, and the pending Swiss Responsible Business Initiative, must implement human rights due diligence in their supply chains.²³

To combat this, companies need to invest in ethical supply-chain audits and due diligence – an entire advisory market has grown to serve this market, at considerable cost to corporates. The fines for breaches are up to €30 million in France and €820,000 in the Netherlands.²⁴

Cyber Crime

For ease of navigation, we have studied cybercrime in our technology section, but it remains a facilitating channel for all six sectors.

As one interviewee in the study said:

“Cyber crime is a bigger threat to me than a physical attack on our facilities. Ransomware and hacking to steal our IP or gain information about our negotiating position are real and current problems”²⁵

Hacking attacks cost the average American firm \$15.4 million per year. A subset of hacking, Dedicated Denial of Service (DDoS) attacks focus on bringing down a company or government website, making it inaccessible to customers for as long as the attack is underway. Malware is considerably more widespread; a 2016 UK study²⁶ suggested that 21% of firms with more than 250 employees and 19% of those with 100 to 250 employees had been hit by malware attacks in the previous 12 months.

In 2015, the Internet Watch Foundation identified over 68,000 URLs containing child sexual exploitation and abuse (CSEA) images hosted online on 1,991 domains. These five top level domains (.com .net .ru .org .se) accounted for 91% of all webpages identified as containing child sexual abuse images and videos – all of these were on the public web, not the dark web.

The tech sector suffers little financial loss from these illegal activities and, historically, regulation has largely protected ISP and communication providers from prosecution when their services are used for illegal activities by end users.

A global internet company said:

“We try to block terrorists and particularly child pornography on our sites because we are decent people and because we can’t

23 Mandatory reporting: Disclosure and due diligence laws. Human Rights Outlook 2017. Verisk Maplecroft. <https://maplecroft.com/portfolio/new-analysis/2017/03/15/human-rights-outlook-2017-mandatory-reporting-disclosure-and-due-diligence-laws/>

24 ibid

25 Interview feedback, Global Resources Company, 2017

26 Study commissioned by business internet service provider (ISP) Beaming, http://www.computerweekly.com/news/450300330/Cyber-attacks-cost-UK-business-more-than-34bn-a-year-study-shows_2016



risk the reputational hit we would take if it was found there."²⁷

But the reputational impact means major tech companies, particularly Google and Facebook, actually apply significant collaborative resources to weeding out criminal, terrorist and CSEA activity.

27 Interview with Global Internet Communications Company, 2017

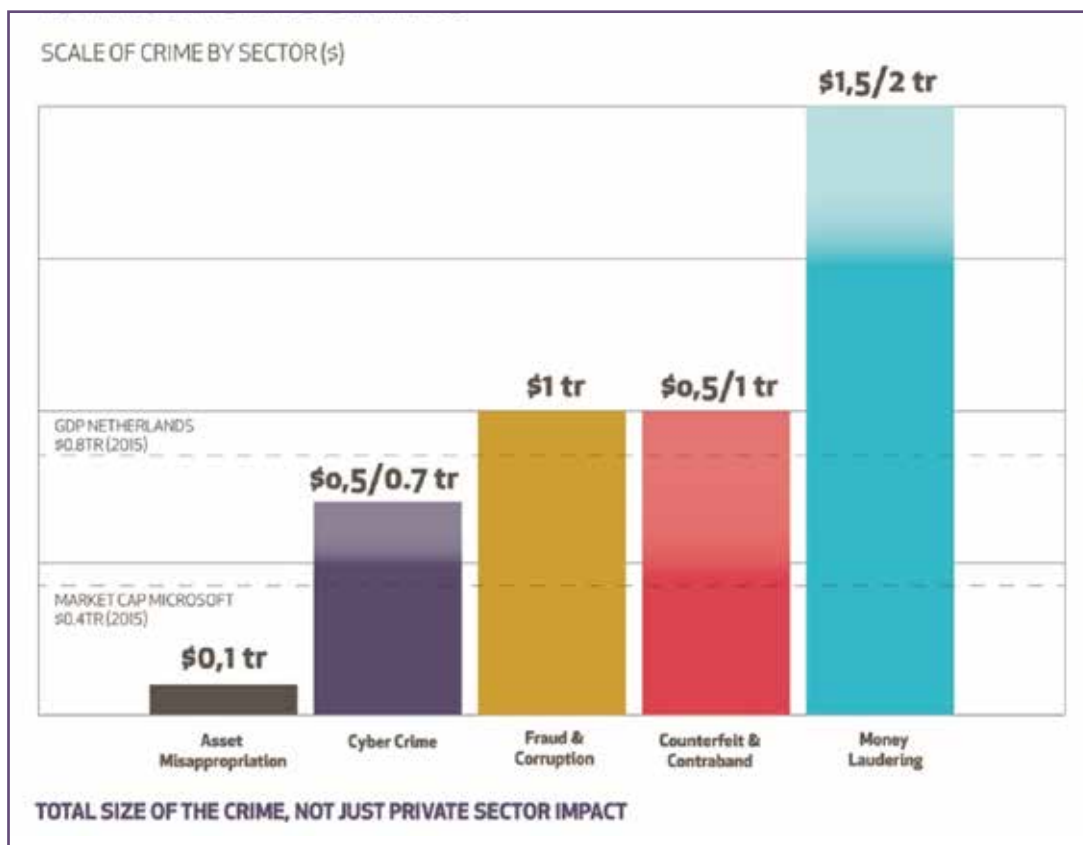


3. Key Findings

Finding #1: The Scale and Impact of Crime on the Private Sector is Truly Staggering

On a global basis the scale of organized crime is truly staggering. Research suggests that across just the six private sectors studied in this report – (i) financial services; (ii) technology; (iii) consumer goods and retail; (iv) construction and real estate; (v) transport and logistics; and (vi) natural resources – a conservative estimate of the value of organized crime was \$3.6-\$4.8 trillion, in 2015/2016, equivalent to 7% of global GDP.

Figure 2: The Scale of Crimes in Private Sector²⁸



These figures reflect the commercial value of crime in each sector, rather than the incurred losses to any individual party. This value acts as an effective market size of the individual crimes.

Money laundering on its own is valued at \$1.5 trillion, cybercrime at approaching half a trillion. A recent WEF Global Agenda Council on Illicit Trade 2012-2014 estimated all counterfeit trade to be worth \$650 billion²⁹, nearly half a billion specifically in retail goods. The flow of statistics is sobering: in 2003 the total income from US criminal activities was 7-8% of GDP, and fraud in construction is estimated at up to \$1 trillion, equalling 20-30% of total contract values in some parts of the developing world.

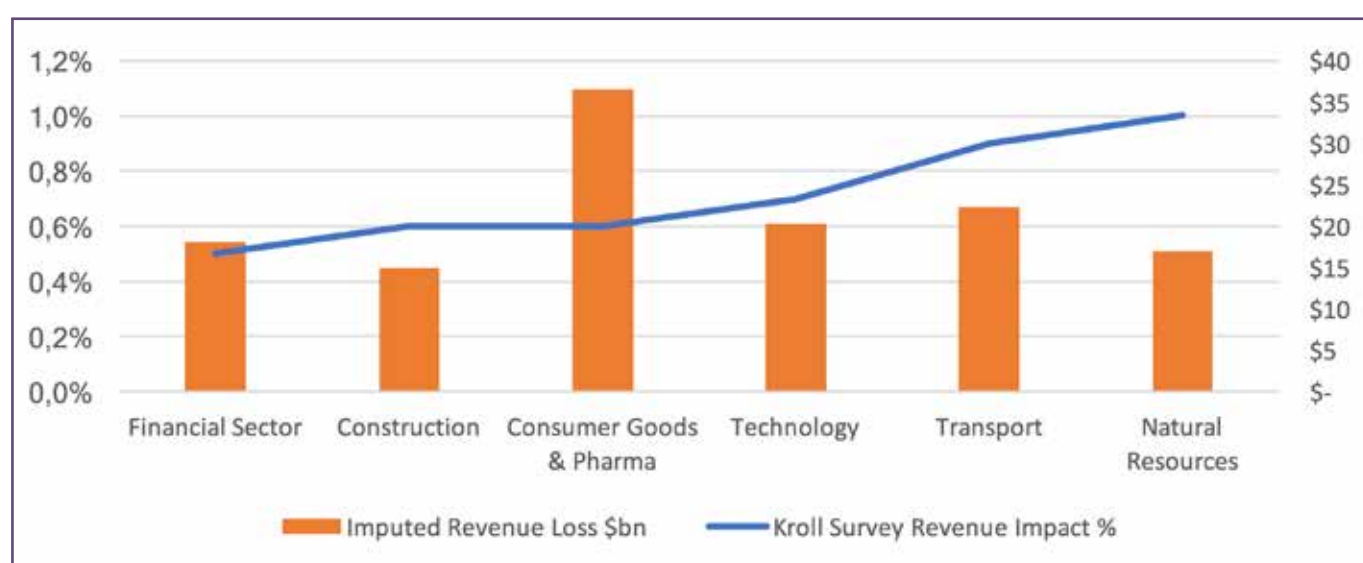
²⁸ Our analysis; sources: various, including OECD/EUIPO 2016, WEF Global Risks Report, Levi and Reuter

²⁹ State of the Illicit Economy Briefing Papers, WEF, 2005

Equating this crime 'sizing' to impact is problematic. Whilst this paper's remit focuses on the impact on the private sector actors, the overall impact of organized crime is multi-dimensional, and shared across the private and public sectors and society itself. The impact is broad, and includes:

- Direct revenue and profit impact on the private sector
- Reputational impact on the private sector and economy
- Impact, and cost of regulation to address crime occurrence, on the public and private sectors
- Revenue and taxation loss to the public sector
- Loss to, and impact on communities and society

Figure 3: Estimate of Financial Impact of Fraud and Crime on Sectors³⁰



The impact on the private sector – in terms of revenue loss – is estimated at c\$130 billion, from a crime survey conducted by Kroll across the sectors. Figure 3 shows the percentage and revenue impact of crimes in each individual sectors.

Although this paper does not seek to downplay other threats, it is notable that, while organized crime has arguably a greater societal impact in terms of mortality and lives damaged, it receives considerably less attention than terrorism.

IEP calculated the financial cost of terrorism at over \$52 billion in 2014, the highest figure ever. A conservative estimate of total transnational organized crime is \$870 billion a year. This is more than six times the amount of official development assistance and close to 7% of the world's exports of merchandise.³¹ In 2015 there were 28,328 deaths as a result of terrorist activity. During the same twelve months, 256,500 individuals were killed due to criminal activity (including gang crime, excluding domestic homicides). While not all of these would have been victims of organized crime, the scale shows the relative materiality of TOC-related

30 Global Fraud Report: Vulnerabilities on the Rise. Annual Edition 2015/16. Kroll. http://anticorruzione.eu/wp-content/uploads/2015/09/Kroll_Global_Fraud_Report_2015low-copia.pdf

31 Transnational Organized Crime: Let's put them out of business. UNODC. Accessed November, 2017. <https://www.unodc.org/toc/en/crimes/organized-crime.html>



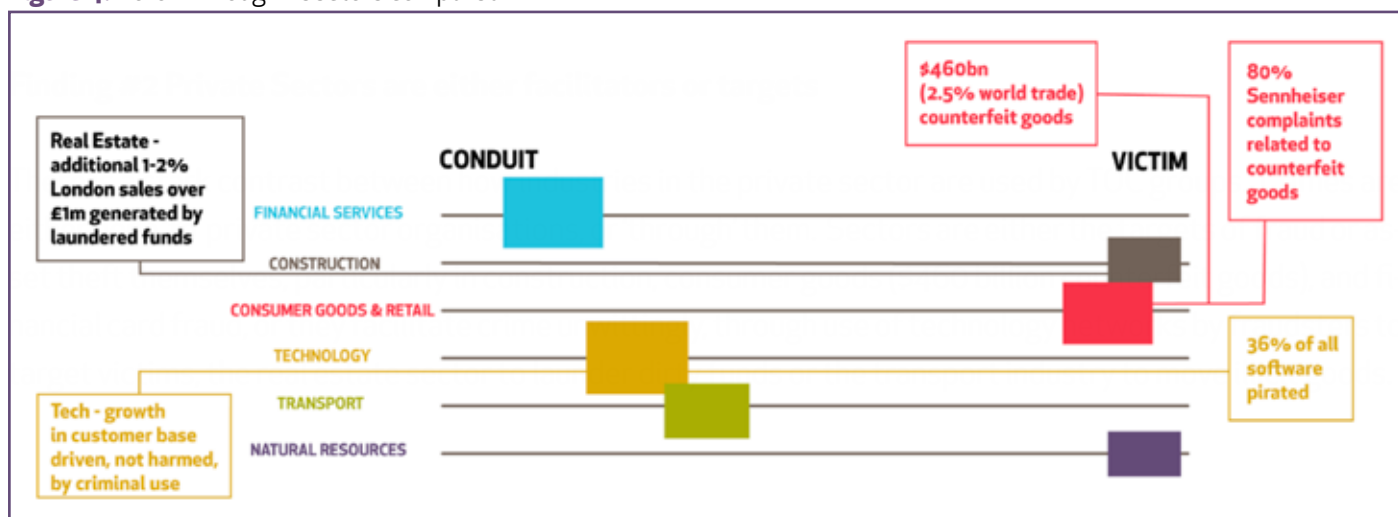
death and this does not account for the level of death or injury that could have been caused by fraudulent, substandard or counterfeit goods being promulgated across the globe.^{32 33 34 35}

Organised crime in the private sector presents fundamental barriers to sustainable development as defined in the UN Sustainable Development Goals. There are an estimated 45.8 million victims caught in situations of modern slavery globally.³⁶ Reportedly 120,000 people die each year in Africa due from taking fake anti-malarial drugs.

Finding #2: Private sectors are either facilitators or targets.

There are notable differences in the ways in which various industries are targeted by TOC groups. Crimes are either done 'to' private sector organisations, or 'through' them. Sectors are either the targets of fraud or asset theft themselves, particularly in construction, consumer goods (\$460 billion counterfeit goods), and financial card fraud, or they facilitate crime unwittingly, through the use of technology networks by fraudsters to target victims, the real-estate sector to launder dirty funds or the transport industry to move illicit goods.

Figure 4: 'To' or 'Through' - sectors compared



Construction and Natural Resources are, at a holistic level, the most 'victimised' industries. Asset theft and contract fraud directly target the construction companies; natural resources companies are targeted through oil theft and extractive theft; both are hit hard by racketeering and fraud. TOC groups operate globally in the construction industry, but the strength of the sector in emerging markets with lower regulation and greater demand for housing and infrastructure fuels much of the illegal activity. As

- 32 Using global statistics for deaths by violent means not committed by family members, friends or suicide (leaving criminal means, stranger attacks and gang crime) and excluding deaths due to terrorism and war, 256,500 were killed by criminal activity in 2015.
- 33 UNODC reported a global average intentional homicide rate of 6.2 per 100,000 population for 2012 - Global Study on Homicide 2013
- 34 National Violent Death Reporting System (NVDRS), USA, 2014 percentage
- 35 Armed Conflict Survey 2015, International Institute for Strategic Studies, 2015 = 180,000 deaths in conflict 2015
- 36 The Global Slavery Index 2016. Accessed November 2017. <https://www.globallslaveryindex.org/findings/>

an industry, construction is very susceptible to asset appropriation and this remains the most highly reported crime in the industry – 76% of respondents to a 2014 crime survey in the construction and engineering industry reported suffering asset theft, the highest of any sector surveyed.³⁷ Factors such as the constant turnover of staff, the mobility of the workforce and the temporary nature of project work make the industry an easy target for both opportunistic petty criminals and serious organized crime.³⁸

At the other end of the spectrum are the ‘conduits’ or unwitting ‘enablers’ of crime. Real estate, the downstream neighbour of construction, is a prime example of this. Money laundering through real estate is a crime that entirely uses the industry to facilitate the crime rather than targeting the industry, and it can be argued that the rise in both the volume of real-estate transactions and the increased value of them in fact benefits rather than harm this sector. Up to 1% of the London property market valued at over £1m was believed to be related to laundered funds in 2016. The FATF believes it is simpler and less risky for TOC groups to launder money through real estate than through the banking system in many important jurisdictions because governance regulations are considerably less onerous in property conveyancing than in banking.³⁹ Likewise, technology crimes, whether enabling fraud through online communications, illegal sales of goods and services through crypto markets, cyber-enabled and dependent crimes, such as romance scams or hacking and DDoS attacks, could not exist without the online industries, yet cause limited direct harm to those companies beyond reputational harm.

It is noticeable that regulation varies between the ‘victim’ and ‘enabling’ industries. Laws, albeit often toothless, are in place to criminalise the use of the private sector for technology or money laundering crime. The victim industries, however, are often reliant on existing laws around theft, or copyright infringement, which are not tailored to the activities of TOC groups and tend to have lower penalties for infringement.

Finding #3 Organized crime’s impact on the private sector is growing, not shrinking

Organized crime’s use of the private sector appears to be growing, not shrinking. This seems counter-intuitive to many, as the West’s perception is that the reduction of violent crime (see figure 5) has been accompanied by a reduction in other crimes. In fact, crime has simply ‘professionalised’, and there has been a shift from visible and violent crime towards those which are lower profile in terms of citizens’ perceptions and enforcement prioritisation. The value of counterfeit goods has risen from \$250 billion to \$461 billion⁴⁰ in the last 8 years and asset theft in the transport and logistics industry rose by over 90% 2015 to 2016.⁴¹

Over the last decade, anti-organized crime regulation has grown significantly, in the shape of legislation on criminal finances, bribery and corruption, money laundering and supply chain regulation. There is a sense that the regulation is not working, however. Money laundering seizures equated to 0.2% of all laundered funds in one study; and after the dark web’s Silk Road was taken

37 Fighting corruption and bribery in the construction industry, PwC, 2014

38 Crime in the construction industry, CIOB, 2007

39 Money Laundering Schemes in Real Estate, Corporate Compliance Insights, 17th February, 2016; Money Laundering, Global Financial Integrity, November 2016; Money Laundering & Terrorist Financing Through The Real Estate Sector, FATF, 2007

40 Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD/EUIPO, 2016

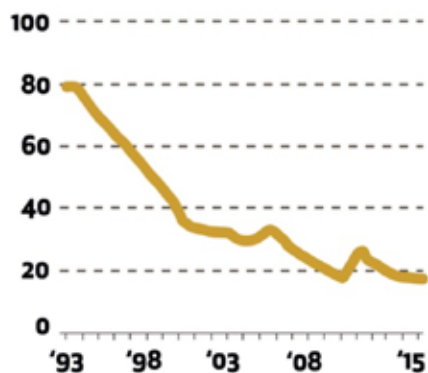
41 Dealing with the threat of rising cargo crime, TAPA – Vigilant, February 2017



down, many sites sprang up to take on and indeed grew the trade. General fraud surveys report rising incidence of crime.

Figure 5: Perception of violent crime

VIOLENT CRIME PER 1000 PEOPLE (12+) IN THE USA



- ▲ • Counterfeit & contraband goods have increased by 10.7% CAGR between 2007 and 2013⁽¹⁾
- ▲ • A 40% increase in modern slavery victims identified in 2015 compared to 2014 (across all sectors)⁽²⁾
- ▲ • Cargo theft by 'fictitious pickup' spiked 70 percent between 2011 and 2013, asset theft up 90% 2015 - 2016⁽³⁾
- ▲ • Internet based 'personal fraud' increasing 10% year on year⁽⁴⁾

Note 1: % saying there is more crime in the US than a year ago
 Note 2: 2006 BJS estimates not comparable with those in other years
 Source: Gallup, Bureau of Justice Statistics

Source: (1): OECD
 (2): The Modern Slavery Act Review, July 31st, 2016
 (3): TAPA, 2015
 (4): Australian Competition and Consumer Commission, 2015

Finding #4 Direct impact of Crime Disproportionately felt in the Global South

The direct impact of much crime is disproportionately felt in LEDCs. Sweatshops flourish in South Asia; trafficking of labour and sex workers originates predominantly in Africa, Asia and Eastern Europe; corruption in natural resources damages production in Africa and the Caucasus; technology fraud is driven from Eastern and Southern Europe, West Africa and the Middle East.

Pharmaceuticals counterfeiting, a life-threatening criminal activity, has a significantly higher incidence in developing countries. Whereas in developed economies counterfeits may account for less than 0.2 percent of the market⁴², developing markets are often beset by 30% fakes, as a UNODC report showed for anti-malarial drugs in Africa.

While the direct damage from organized crime is disproportionately felt in the LEDCs, the MEDCs are intrinsically linked to the crime at every stage, both as perpetrator and victim.

The ownership and management of the major firms in these sectors that are abused in the Global South by TOC groups tend to lie in the Global North. The construction companies that employ the bulk of trafficked and enslaved workers are headquartered in the US, the UK and Western Europe. The technology companies that, albeit unwittingly, facilitate tech fraud are in Silicon Valley, the retail giants that purchase from sweatshops and use unwilling labour are often headquartered in Europe and the US, where

42 Illicit Trade in Counterfeit Medicine, Dr. K Lybecker, Colorado College, 2015



purchasing power for their goods is greatest. The corporate responsibility, legal liability, reputational impact of crimes that damage people and societies in the Global South are borne by companies in the Global North.

The abuse of the often weaker regulatory regimes in the Global South by TOC groups further increases the risk for the private sector operating in these areas. Crime groups are known to flourish in unstable and fragile states, the same states where rapid economic growth, exploding population base and rampant demand for construction and consumer goods drive demand for global private sector input.

Globalization is increasing the 'attack surface' for TOC groups. Kidnapping for ransom is heavily skewed towards workers in the developing world. Although the majority of hostages are returned alive, it is at a high price and kidnapping is fast becoming an insurance-backed 'business', which is factored into production costs. New technology has led to the application of new ideas in a traditional crime environment: ransomware takes the principles of kidnapping without any of the risks associated with a physical hostage.

Compounding the complications of policing ever lengthening supply chains is the increasing prevalence of counterfeit components in goods sold across the world – fake semiconductors in defibrillators, fake components in car engines and viruses on imported smart phones – all of which are predominantly manufactured and sold in the Global North, but contain components from the Global South.

Finding #5 Responses: Confrontational rather than Collaborative

Despite the monumental scale of organized crime in the private sector, we see that NGOs, governments and the private sector tend to look at crimes in isolation, rather than TOC groups as a threat overall, and so the scale of the threat is obscured. We found significant variability in the reporting of different crimes in different sectors, and in remedying crime. For example, money laundering is heavily regulated in the financial sector, yet potentially under-reported in the luxury and real-estate sectors. Human trafficking is well-recognised in the natural resources and construction industries but less in other sectors. Illicit trade of goods is a significant focus of consumer and pharmaceutical companies yet illegal oil trading receives very little coverage.

Despite the history of investigation and remediation of organised crime, there are very few examples of successful public and private sector co-operation against TOC groups. Private sector organisations complain that communication with the law enforcement sector is one-way. They claim that the regulatory reporting burden, designed to combat crime, can act as a deterrent to co-operation. Some 1.5 million suspicious activity reports (SARs)⁴³ were submitted in 2009 in the US under FATF rules. One example of good two-way co-operation is the UK's Joint Money Laundering Intelligence Taskforce, although as an initiative it is in its infancy. We found few examples of meaningful organised co-operation in other sectors, although there were examples of good informal intelligence sharing among the private sector players, or between the private and public sectors (technology, tobacco, pharmaceuticals, logistics).

.....
43 Money Laundering, Michael Levi and Peter Reuter, University of Chicago, 2006



Moreover, the tobacco and drink industries has recently become beset by an adversarial tone, given the adjacency of the public-health debate. It is perhaps noteworthy that in one good example – technology companies voluntarily targeting and removing CSEA images from their sites – regulation ‘protects’ the technology providers. The actions are driven by reputational awareness and pure goodwill.

Conversely, tangible results have been seen when industries take the lead on disrupting the work of TOC groups independently of the public sector. Unsurprisingly, this is most evident in the sectors where the most material direct financial impact is felt – transport being a notable example. TAPA the Transported Asset Protection Association, a network of 600 transport companies, sets global security standards to protect high-value consumer goods travelling on international roads. Research shows that Transport Asset Protection Association (TAPA) members, when fully engaged with TAPA security standards, incur significantly lower theft loss levels than the industry average – three times lower in a benchmark logged in 2010.

This is a systematic failure but it is largely because there has been a failure to align and then leverage the mutual skills of the public and private sectors. Public sector enforcers are used to demanding assistance rather than asking for help; private sector organizations can seem self interested and impossible to corral.

In contrast, the success of public–private sector co-operation in fighting terrorism is encouraging. Hashtag recognition on social media, ‘bomb in a box’ prevention by logistics companies and tracking of terrorist funds through the financial system all offer examples for public/private co-operation that those tasked with countering organized crime can only aspire to at present.



5. Recommendations

Given the extremely high (and growing) cost of organized crime to the private sector, and the disappointing level of public and private sector remediation, we could make very many substantive recommendations for improved action. But these would require system change, or a scale of funds that would seem unrealistic. We therefore present a more limited set of actionable recommendations, which can provide a first step towards effectively harnessing the underused combined skills of the public and private sectors.

With a few notable exceptions (counterfeit goods in developed countries and certain cybercrimes), the analysis of the incidence of organised crime in or affecting the private sectors covered is woefully thin, and lacking in both comprehensiveness and rigour. The real downside of this is that neither the public nor the private sector recognises the problem.

- We recommend a concerted effort to measure and communicate the incidence of organised crime using a consistent methodology that examines the full spectrum of private sector incidence and cost from organised crime. This could be achieved through a dedicated 'data observatory' that draws from data sources from industry, law enforcement and academia.

The degree of co-operation between public and private sectors is exceptionally low, perhaps more so now than when UNTOC was finalized in 2000.

- We recommend a series of sector-specific joint events, attended by regulators, law enforcers and the private sector to identify the potential for further co-operation.
- Following sector specific strategies, we recommend a cross-sector dialogue is pursued to enable learning from alternative approaches, along key themes
- Industry representative bodies, particularly in financial and consumer goods, have pursued a broad agenda. Industry bodies should do more to offer leadership and innovation in combatting organised crime in their supply chains – a good example being the TAPA.

The potential for technology to safeguard supply chains from organised crime theft and corruption is not significant, yet few examples exist of physical supply chains successfully secured by technology.

- We recommend a cross-industry dialogue to establish 'test cases' for systemic supply-chain protection using technologies such as product level track and trace, authentication marking and labelling, and accreditation/verification of supply chain participation.





Industry: Financial Services

How does this industry break down into segments; what is the size, scale and geographic spread of each segment?

The financial sector, or more properly, the financial services sector, has become an industrial behemoth that dominates many Western economies. According to the OECD, the industry makes up 20-30% of total service market revenue.⁴⁴ Extrapolating a McKinsey 2011 estimate of financial services revenue, we can derive a 2014 market size of \$11 trillion. Using 2014 IMF figures for the global economy of \$77.6 trillion, this equates to a staggering 16.9% of global economic worth (by GDP).

Breaking this down. The banking segment splits into commercial (retail and business) and investment banking. The insurance sector covers brokerage, underwriting and re-insurance. Investment services is characterised as a separate segment covering investment management, hedge funds and custody services. The long tail of 'other' financial services cover the card market segment, private and venture funding, foreign exchange and many other segments. Despite being a service industry, its importance as an export market is growing, with overseas financial centres creating hubs of capability, the UK being a prime example.

The industry is overwhelmingly biased towards Western economies, and as a result, so is this paper. As a proxy measure, World Trade Organization (WTO) trade figures in 2014 show Europe making 60% of all financial services exports, North America 23% and Asia 15%. Starkly, Africa, the Middle East, Commonwealth of Independent States (CIS) and South and Central America each have 1% or less of global financial service exports.⁴⁵

As a specific example, to put London as a financial centre into international context, the UK has the largest insurance industry in Europe and the third largest in the world. Twenty percent of the world's foreign equity market is listed in London. London is the leading Western centre for Islamic finance. And it has \$2.4 trillion of foreign exchange turnover each day – 37% of global foreign exchange.

44 Investopedia

45 WTO, International Trade Statistics, 2015

Figure 6: World Exports of Financial Services by Region, 2013 and 2014 (\$ billions and %)

	Value		Share		Annual percentage change		
	2013	2014	2010	2014	2010-14	2013	2014
Exports							
WORLD	400	415	100.0	100.0	6	9	4
North America	92	95	23.3	22.8	5	9	3
South and Central America	5	3	1.0	0.7	-5	0	-41
Europe	239	248	60.9	59.4	5	8	4
European Union (28)	214	225	54.2	53.9	6	8	5
Commonwealth of Independent States (CIS)	3	2	0.5	0.5	5	35	-20
Africa	2	2	0.5	0.5	4	0	-8
Middle East	3	3	1.2	0.8	-6	7	16
Asia	57	64	12.5	15.4	11	11	13

What types of organized crime feature in this industry? Which geographies and segments are most affected?

Assessing the incidence and nature of organized crime in financial services remains a task made profoundly difficult by the lack of reliable reporting. Whilst the compliance and regulation of crime affecting financial services has grown into an industry in its own right, the actual information on the crimes themselves remains opaque.

The crimes that fall under the financial crime definition are much broader than the money laundering term often used as a shorthand, and include:⁴⁶

- money laundering
- bribery and corruption
- terrorist financing
- sanctions evasion
- tax evasion
- fraud

Interestingly, this list varies little in the financial sector, as a definition of key crimes. But it seems to be driven as much by the regulation and compliance framework around these crimes, as by the incidence of the crime themselves.

Despite this breadth, a great deal of commentary focuses only on money laundering, which acts as an intermediary crime in many respects, given that the proceeds are from a primary or predicate crime, such as fraud, theft or extortion. This is neatly summar-

46 Global Risk Update, RiskReward.Uk.Ltd, 2014



rised by British Bankers' Association (BBA):

"Money-laundering, particularly, is an "enabling crime", facilitating organized crime (as well as terrorism) with social and economic costs to the UK estimated to be at least £24 billion a year. It supports, among other crimes, drugs, people and firearms trafficking, organized illegal immigration, large-scale and high-volume fraud and other financial crimes, counterfeit goods (including medicines), organized acquisitive crime and cybercrime."⁴⁷

We do know that the penetration of financial services by organized crime is as high as any industry sector. A recent PwC survey reported that 45% of all financial services organizations polled globally had reported economic crime, compared to an industry average of 34%⁴⁸. In terms of this 'penetration', the sub-segment of banking, investment management and capital markets tied top place with the retail and consumer segment.

Of these financial crimes, respondents were able to break down crime by type:

- 67% was asset misappropriation (incl. fraud)
- 39% was cyber-crime
- 24% was money laundering
- 21% was accounting fraud
- 20% was bribery and corruption

This survey puts the more conventional fraud of misappropriation at a far higher level of incidence than the more often mentioned money laundering – but this incidence analysis doesn't take account of size of crime, so it is a volume rather than a value measure. The split between internally and externally committed fraud is 43%/57%, despite the introduction of stringent controls to detect 'insider' fraud. Within the financial sector fraud is often targeted at lower levels of lending or insurance activity, and therefore is not often perceived as organized crime – but that would often be quite wrong. Police sources in the UK suggest two-thirds of organized crime groups whose primary activity is fraud are also involved in other criminal activities.⁴⁹ Police have classified many fraud perpetrators as organized fraudsters due to evidence of this cross-cutting criminal activity.

47 Future Financial Crime Risks, Lexis Nexis Risk Solutions for BBA, Nov 2015

48 PwC, Global Economic Crime Survey, 2015

49 Michael Levi, Organized Fraud, The Oxford Handbook of Organized Crime, 2014, p.462



CASE STUDY

“When hackers broke into the computers of Bangladesh’s central bank in February and sent fake payment orders, the Fed was tricked into paying out \$101 million. But the losses could have been much higher had the name Jupiter not formed part of the address of a Philippines bank where the hackers sought to send hundreds of millions of dollars more. By chance, Jupiter was also the name of an oil tanker and a shipping company under United States’ sanctions against Iran. That sanctions listing triggered concerns at the New York Fed and spurred it to scrutinise the fake payment orders more closely, a Reuters examination of the incident has found.

It was a “total fluke” that the New York Fed did not pay out the \$951 million requested by the hackers, said a person familiar with the Fed’s handling of the matter. There is no suggestion the oil tanker or shipping company was involved in the heist.

[According to] the Reuters examination the payment orders sent by the hackers were exceptional in several ways, [including formatting and wording]. Yet it was the word ‘Jupiter’ that set the loudest alarm bells ringing at the New York Fed. Even then it appeared to react slowly.

By the time the fraud was discovered, the New York branch of the U.S. central bank had approved five of the payments. It took \$101 million from Bangladesh Bank and paid it to accounts in Sri Lanka and the Philippines – including \$81 million to four accounts in the names of individuals. Most of that \$81 million remains lost.”⁵⁰

But fraud against the financial sector is not always piecemeal. In 2016 a concerted cyber-attack against Bangladesh’s central bank revealed a significant weakness in the anti-fraud activity of both the Bangladeshi system, but, worryingly, also the New York Federal Bank.⁵¹

Our primary mechanism for assessing the use of financial sector channels for organized criminals is, unsurprisingly, through the assessment of money laundering, which captures a broad range of ‘predicate’ crimes (defined as all crimes attracting a sentence of one year or more).⁵² A landmark study in US in 2004 put total income from criminal activities as \$224bn, or \$779bn with tax evasion included, tracking a rise from 7 to 8% of US GDP by 2000. It is reasonable to assume that the financial sector at least ‘touches’ a great deal of these illegal proceeds, either as a depository, fraud mechanism or laundering route. Indeed UNODC have been credited as saying the majority of the \$352bn proceeds of the illegal drug trade (in 2009) had been absorbed into the economic system.

Interestingly, the direct effect on the financial sector is very often reputational and compliance-led. Whilst there are no reliable

50 Reuters How the New York Fed fumbled over the Bangladesh Bank cyber-heist; Krishna N. Das and Jonathan Spicer, July 21, 2016, 10:30 a.m. GMT

51 Ibid.

52 Michael Levi, Money Laundering, Oxford Handbook of Organized Crime, 2014 p.421





global estimates of losses directly by institutions, fines for AML, sanctions and tax avoidance violations at twenty of the world's biggest banks have totalled more than \$17.5 billion in the last seven years. This staggering cost should be seen in the light of the effectiveness of the regulatory regimes to combat these crimes, which remains, at best, heavily asymmetric.

What is our estimate of the direct financial impact on this industry by segment, by crime type? What are the implications?

Of the macro estimates of financial crime, few are viewed with strong credibility, but one estimate of money laundering puts it at 2% of global GDP – c.\$1.5 trillion.⁵³ The UN, in 2005, cited a range of \$500 billion to \$1 trillion, again for money laundering.⁵⁴

Card fraud has risen dramatically as the use of payment cards became commonplace since the 1970s. But improved security has brought the rates down in many Western economies. In the UK a card fraud ratio in 2008 of 0.101% fell to 0.059% in 2013. But in US the rate is still 0.104%. Total card fraud losses in EU in 2013 were €1.33bn, and in the US €4.148bn.⁵⁵ Whilst often seen as non-organized crime, in fact card fraud often involves sophisticated attacks by co-ordinated teams, as seen in last year's cash machine attack in Japan.⁵⁶

Cash worth 1.4bn yen (\$13m; 8.8m) has been taken from cash machines in Japan using credit cards created with data stolen from a South African bank. The money was withdrawn in less than three hours from 14,000 convenience store cash machines across Japan. The withdrawals targeted 7-Eleven cash machines, which unlike most in Japan accept foreign cards. South Africa's Standard Bank estimated its total losses at \$19.25m. Police suspect more than 100 people were involved across Japan.

Other fraud crimes include VAT carousel fraud, which in the UK alone in 2006 was thought to be £1 in every £10, and insurance fraud from 'staged motor accidents' at £348 million.

Online bank fraud has been estimated at c.£40m in the UK, but mortgage fraud, in a disputed estimate, has been reported in the £1 billion range.

Given the relative size of these fraud examples, in their billions compared to the \$0.5 trillion and upwards estimates of money laundering, it is no surprise that so much focus is given to the combating the latter.

But attributing figures to individual parties becomes complex. As Deloitte point out,⁵⁷ the impact on financial institutions can be a mixture of direct loss, fines for non-compliance and reputational damage.

53 Bloomberg, "Why the World is so Bad at Tracking Dirty Money" February 2015


54 Michael Levi and Peter Reuter, Essay: Money Laundering, University of Chicago, 2006

55 Payments Cards and Mobile, Card Fraud Report 2015

56 BBC News: Japan ATM scam using fraudulent cards nets \$12.7m 23 May 2016

57 Deloitte Insight on Financial Crime





How is the industry legally regulated to combat organized crime? What is the effectiveness of this regulation when compared to the costs? What examples or case studies exist of positive co-operation and remediation of organized crime in the public and private sectors?

The regulatory regimes that govern the probity of financial institutions are a complex combination of global, regional and national systems. Regulatory regimes are concerned in the main with money laundering, sanctions, tax evasion and fraud, and in most countries each category of crime falls to different government organisations. This paper does not attempt to review the breadth or depth of regulation, rather it provides a means to highlight some examples of the most significant regulatory activities and their effectiveness.

Arguably, the most significant global regulatory initiative in the financial sector is the FATF which collects together the efforts of 34 governments, mainly within the OECD, the Gulf Cooperation Council (GCC) and EU. Suspicious activity reports (SARs) remain the primary source of AML information. SARs reporting is an industry in itself. In 2009, 1.52 million SARs were filed by the US, half of them by financial institutions, while currency transaction reports are ten times greater.⁵⁸

There are some key examples of success in countering laundering – HSBC paid \$1.92 billion in fines related to Mexican drug cartel laundering. But the overwhelming conclusion of the key study in this area, by Levi and Reuter,⁵⁹ is that AML procedures snare just a small fraction of criminal income flows. Figures from a UK review suggested that the proportion of SARs that generated any significant benefit to prosecutions and conviction-based asset confiscation was under 1%. Extrapolating success rates in the US, compared to the market sizing of money laundering suggest that:

“A generous estimate of seizures would amount to a mere 0.2 per cent of all laundered funds”⁶⁰

Of course, seizures represent only one form of disruption of organized crime, and therefore a conviction rate might be a safer starting point. Levi and Reuter’s ‘guesstimate’ on this is 6.7%. Against a conviction rate for drug dealing of 25-30%, money laundering looks like an attractive option. This raises a question about the enforcement effort, which is clearly directed more against the traffickers.

Fraud researchers note that the analytical and research literature on fraud is sparse, reflecting governments’ view of its “marginal status...as a crime problem”⁶¹ This might explain the Bangladeshi case’s lack of apparent controls.

58 Michael Levi and Peter Reuter, Essay: Money Laundering, University of Chicago, 2006

59 Ibid

60 Ibid

61 Ibid





CASE STUDY

“The heist revealed that the New York Fed lacked a system for spotting potential fraud in real time – even though such systems are used elsewhere – instead relying at times on checking payments after they were made, usually for problems such as violating U.S. sanctions
Months of bitter finger-pointing over who is to blame for the fiasco have damaged the sensitive diplomacy of correspondent banking, where big Western institutions are entrusted with safeguarding the treasures of smaller economies. Bangladesh Bank is now preparing a legal case to seek compensation for what it says were failures by the Fed, according to a source close to the Asian bank. It also claims that errors by SWIFT, a messaging system used to make international bank transfers, made the bank vulnerable to hackers.”⁶²

The crucial observation here is that the only reason this fraud was picked up before \$1bn was lost was because of the (incorrect, as it turned out) spotting of a sanctions risk – the fraud risk itself went unnoticed.

“Fraud is often seen as simply the cost of doing business in the Financial Sector, particularly in the credit card business” – former senior bank executive

The costs of compliance for financial institutions, naturally, given this much activity reporting, are significant. For AML alone, one estimate puts US institutions’ compliance expenditure at \$3 billion.⁶³

Against this background of massive compliance requirements involving huge costs but with relatively small detections, there are occasional signs of very positive collaboration between enforcers and the financial institutions. In the UK the NCA has pioneered a Joint Money Laundering Intelligence Taskforce JMLIT, to move from ‘one way’ communication of SARs to a peer intelligence sharing model:


“The JMLIT initiative was announced in 2015. A collaboration between the NCA, Home Office, British Bankers’ Association, financial services experts and 10 of the biggest UK banks, it is designed to improve intelligence sharing between all parties. A central hub allows banks to share information such as suspicious activity on accounts not just with the enforcement agencies, but also with other banks – through the NCA, which will act as a conduit. The hope is it will give banks a more complete picture of activity to identify crime.”

A cautiously optimistic evaluation of the JMLIT pilot concluded positive aspects of networking, but also highlighted some significant barriers to co-working. No evidence of a decrease in actual money laundering was presented.

62 Reuters, How the New York Fed fumbled over the Bangladesh Bank cyber-heist; Krishna N. Das and Jonathan Spicer, July 21, 2016, 10:30 a.m. GMT

63 Michael Levi and Peter Reuter, Essay: Money Laundering, University of Chicago, 2006





The organisations involved invested significant resources... to make the envisaged partnership a reality – overcoming substantial obstacles to do so... A striking 98% of survey respondents rated the JMLIT as ‘very’ or ‘slightly’ successful, which is particularly high in light of the challenges they had to overcome. The most notable obstacle was the legal impediments to the sharing of information between parties which will require legislative/legal remedies. Other frequently noted challenges were: the lack of adequate technological systems and processes to support the JMLIT’s work, particularly within the [NCA’s] Operations Group; the lack of clarity of the governance structure and respective roles of the Management Board, Strategic Group and Operations Group; and communications amongst those three groups.⁶⁴

Despite a positive start, the future of JMLIT is in doubt. The Home Office recently announced the continuation of JMLIT and the ongoing sponsorship of the Joint Fraud Taskforce, which claims to have closed thousands of bank accounts linked to fraud. In other countries, differing degrees of public–private partnerships have emerged, notably in New Zealand, Dubai, Singapore, Hong Kong and US. But evidence of real progress is worryingly thin. UNODC’s Commission on Crime Prevention and Criminal Justice, at its 19th session in May 2010, requested UNODC to examine the efforts made by Member States to take over public–private partnerships as a mechanism for combating transnational crime and to identify priority areas for the strengthening of such partnerships. But this initiative produced few concrete actions or collateral. A private-sector-originated working group discussed, in 2012, successful PPPs in the financial crime area, but again the initiative appeared to founder, and had little public-sector engagement.

One US example provided good feedback given the scale of outreach, but appears not to have been followed up:

In March 2012, the US Treasury concluded over two years of discussion on customer due diligence (focused on beneficial ownership) within the US government, and with private sector and international counterparts. It then launched an aggressive outreach campaign. In an effort to engage stakeholders—including banks, broker-dealers, futures commission merchants, and mutual funds—and in order to cultivate broad understanding and support for a comprehensive and well-informed rule-making process, the Treasury held an extended comment period on the proposed new rule with the stated goal of creating effective policy with minimal burden to industry.

Frustratingly, while examples of successful public-private initiatives are rare, evidence of their having a demonstrable effect on crime are even rarer.

64 FTI Consulting, JMLIT Pilot Review 2015



Industry: Technology

How does this industry break down into segment? What is the size, scale and geographic spread of each segment?

The technology industry is broad, covering the manufacture and distribution of hardware and software and the provision of internet and phone communications.^{65 66}

The pace of technological advances has transformed nearly all industry and service sectors globally, and the TOC 'industry' is no exception. The internet in particular has both enabled existing criminal enterprises and created opportunities for a raft of new criminal enterprises. Over 40% of the global population has access to the internet; in 1995, figure was less than 1%. In 2005 there were one billion users, by 2014 three billion had connected. The pace is of growth is exponential – approximately ten new people gain access to the internet every second.⁶⁷ Nearly \$1.5 trillion was spent on internet communications in 2016.⁶⁸

Historically, internet use has primarily been the privilege of developed nations. In 2014 nearly 75% (2.1 billion) of all internet users in the world lived in just twenty countries, nearly all high GDP developed nations; the remaining 25% were distributed among the other 178 countries,⁶⁹ each representing less than 1% of total users. This is rapidly changing: among the top twenty countries, India has both the lowest penetration at 19% but the highest yearly growth rate and similar growth is being seen across Africa and less developed parts of Asia.⁷⁰

Like internet use, access to mobile-phone networks is changing the communications landscape, levelling the playing field for countries that do not have developed telecoms infrastructures and opening up national and international communication to all, including TOC groups. In 2015 there were more than 7.6 billion mobile connections worldwide and operator revenues of more than \$1 trillion. With regional subscriber penetration rates of only 43% in sub-Saharan Africa compared to 85% in Europe, the scope for growth in the developing world is clear. By the end of 2017, 30.9% of the world's population, nearly a third, will have access to an internet-enabled smartphone and, therefore, be potential victims of internet-enabled crime through their mobile phones.⁷¹

As with any industry that produces a physical product, counterfeiting and IP theft are material threats to manufacturers and de-

65 Some definitions also include IT services

66 Investopedia, 2017

67 Internet Live Stats, 2016


68 Global IT market size: Facts and Figures, Accelerance, 2015
<http://www.accelerance.com/research/global-it-market-size-facts-and-figures>

69 Internet Users. Internet Live Stats. Accessed November 2017. <http://www.internetlivestats.com/internet-users/>

70 Global IT market size: Facts and Figures, Accelerance, 2015
<http://www.accelerance.com/research/global-it-market-size-facts-and-figures>

71 Statista 2017-01-11





velopers. The global market for technology is significant, worth \$3.52 trillion in 2015.⁷² Consumers often buy based on brand and reputation, making this market highly attractive to counterfeiters. Over \$750 trillion dollars was spent on hardware and devices globally in 2015, and a further \$300 billion on software.

What types of organized crime feature in this industry? Which geographies and segments are most affected?

The exploitation of the internet is particularly interesting for the way in which it is used to facilitate the activities of organized crime groups rather than as a direct target. Of all the sectors studied, technology and the internet take a leading role in the unintended facilitation of TOC activity. Looking in particular at the split between cyber-enabled and cyber-dependent crimes, it is clear that there has been rapid growth in the scale and scope of both.

Cyber-dependent crimes, those that could not exist without technology, include hacking, DDoS attacks, the use of malware and 'phishing'. These crimes use the technology sector, but attack industries across the market and the negative impact on the latter is far greater. Where these crimes do impact the technology sector, it tends to be through reputational harm and related loss of advertising revenue rather than direct damage.

Hacking, the unauthorized access to and use of a computer system, provides extensive opportunities for TOC groups. In addition to taking financial advantage of the privileged information stored on company and public sector servers hackers are increasingly using encryption and ransomware to extort money from victims and evade detection.

"Cyber crime is a bigger threat to me than a physical attack on our facilities. Ransomware, and hacking to steal our IP or gain information about our negotiating position is a real and current problem" – Interview feedback, Global Resources Company, 2017.

Once in place hackers can spend weeks or even months inside a company's systems, making use of information and setting up so-called 'back doors'. These illicit entry points to the servers can then be revisited or sold to other TOC groups with different capabilities.

"For example, if I hack into a major law firm and then realize that this law firm has direct communication channels with the Fortune 50, then I can leapfrog from this law firm into all of those entities" – Tom Kellermann, Chief Security Officer, Trend Micro.⁷³

DDoS attacks focus on bringing down a company or government website, making it inaccessible to customers for as long as the

72 Global IT market size: Facts and Figures, Acclerence, 2015

73 An inside look at what's driving the hacking economy. Harriet Taylor. CNBC. 5 February 2016
<http://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-economy.html>





attack is underway. Although sometimes committed for ideological reasons, it is often done for ransom, with the attack persisting until a significant ransom has been paid. A recent study⁷⁴ suggests that 46% of companies hit by a DDoS attack had received a ransom note.

Whereas direct hacking requires an individual or group to actively target a specific network, malware can be sent simultaneously to millions of email accounts with no particular need for focus. It simply requires someone inside the company to inadvertently (or sometimes deliberately) allow the malware into the system from the inside by opening an attachment with an embedded malware virus or worm. Once inside the system the malware can retrieve information or embed further code in the same way as a hacker.

Although far less focused than hacking, the damage done by malware is considerably more widespread. A 2016 UK study⁷⁵ suggested that 21% of firms with more than 250 employees and 19% of those with 100 to 250 employees had been hit by malware attacks in the previous 12 months.

The internet has also been a boon for 'old school' crime. Cyber-enabled crimes are those that existed prior to the rise of the internet – fraud, scams, imagery of child abuse and exploitation, illegal trade and money laundering – but which have become easier and more widespread since. The anonymous nature of internet communication has made fraud ever more feasible. Business email scams target businesses working with foreign suppliers and customers to prompt unauthorized wire transfers of funds; personal email scams target the general public, and particularly professionals associated with financial and lending institutions, real-estate companies, and law firms using compromised emails to request payments to fraudulent locations.

Internet-based romance scams are particularly insidious, again capitalizing on the global, anonymous nature of the internet. It is a fast-growing crime, which in the UK jumped by nearly 16 per cent, when more than 3,500 people came forward to disclose incidents.⁷⁶

While this paper has discussed the disproportionate impact of technology fraud on the 'Global North', this is an area where the impact is felt worldwide:

"Within South Africa, a report released by the Southern African Banking Risk Information Centre (SABRIC) in 2010 ranks South Africa as the 3rd most victimised country, after the US and UK, with regard to online banking manipulation or phishing."⁷⁷

In 2015, the Internet Watch Foundation identified over 68,000 URLs containing child sexual exploitation and abuse (CSEA) ima-


74 Incapsula Survey: What DDoS Attacks Really Cost Businesses, 2014

75 Study commissioned by business internet service provider (ISP) Beaming, <http://www.computerweekly.com/news/450300330/Cyber-attacks-cost-UK-business-more-than-34bn-a-year-study-shows,2016>

76 Commander Chris Greany, UK Police National Economic Crime Co-ordinator, 2015 <http://www.telegraph.co.uk/news/uknews/crime/11960852/Cost-of-online-dating-scams-jumped-16pc-last-year-say-police.html>

77 Hubschle, A., 'The dark side of the Internet: Cybercrime', Institute for Security Studies, 1 March 2011, <http://www.iss.co.za>. Quoted in *Globalisation and transnational organised crime in South Africa, 2012*





ges hosted online on 1,991 domains. Of these, five top level domains (.com .net .ru .org .se) accounted for 91 per cent of all webpages identified as containing child sexual abuse images and videos – all of these are on the public web, not the dark web. This does not suggest that there is not an equivalent or greater quantity of CSEA material on the dark web, but it highlights the degree to which it exists in plain site on commercially backed servers. 78% of CSA were held on image hosting sites in 2015, with a further 10% held in cyber lockers.⁷⁸

Unlike the previous crimes, 'cryptomarkets' which facilitate illicit purchasing and trade, are part of the "dark web": sites only accessible through browsers such as Tor, which route communications via several computers and layers of encryption, making them almost impossible for law enforcement to track. Buyers and sellers make contact using email providers such as Sigaint, a secure dark-web service, and encryption software such as Pretty Good Privacy. They settle up in bitcoin, a digital currency that can be exchanged for the old-fashioned sort and that offers near-anonymity during a deal.

Online gaming and gambling are growing money laundering routes. In the online gaming market hackers acquire gaming currencies using malware, phishing, and by using deception to gain users' log-in information or through direct exploitation of the game servers themselves. The stolen virtual money is then sold to other gamers – once the gaming currency has been sold in exchange for legitimate online currency, usually bitcoins, the stolen currency has become legitimate and can be moved into standard banking channels as 'clean' untraceable money.

The anonymity of online gambling sites further supports money laundering – whether a TOC group deliberately 'loses' dirty money during a poker game to a separate online identity owned by the same TOC group, which then declares the money as legitimate gambling winnings, or simply uses unregistered gambling sites to break up the money trail for investigators, increasing quantities of money are being passed through online gambling sites.⁷⁹

In addition to the direct attacks of the technology sector by TOC groups through piracy and counterfeiting of technology and software, and the use of technology by these groups to commit crime (cyber-enabled and cyber-dependent) there is increasing evidence, of TOC groups using technology to evade detection and to facilitate the committal of non-tech crimes. In 2015 Police Scotland described the use of apps and encrypted messaging as "the biggest challenge facing police focused on breaking up organized crime groups".⁸⁰

For every technological success in fighting crime, like the use of digital photo DNA analysis fingerprinting, which has cut the time it takes to assess and log CSEA images by 75%, law enforcement agencies like Europol have highlighted the challenges posed by the rapid uptake of new technologies by TOC groups, which is not always replicated by the law enforcement teams trying to track them.⁸¹

78 Internet Watch Foundation, Annual Report 2015, <https://www.iwf.org.uk/assets/media/annual-reports/IWF%202015%20Annual%20Report%20Final%20for%20web.pdf>

79 Gambling Commission, 2016

80 Organized gangs using technology to evade police, BBC, 29/12/15 <http://www.bbc.co.uk/news/uk-scotland-35190233>

81 The Future of Organized Crime, Challenges and Recommended Actions, Europol 2011





“International trade, an ever-expanding global transport infrastructure and the rise of the Internet and mobile communication have engendered a more international and networked form of serious and organized crime” – Soren Pedersen, Spokesman, Europol (2013)

The technology industry is targeted by TOC groups in the same way as many other sectors: where items of value are made there will be groups that attempt to profit by counterfeiting these items. The counterfeiting of technology hardware and devices is a material crime and has serious consequences for manufacturers. Within the technology sector this applies both to physical hardware and to the pirating of software.

“At one point we estimated that almost 80% of all the complaints we received were due to the fake products [being sold] illegally under our brand-name,” Peter May, Marketing Director, Sennheiser UK, 2013

Research⁸² suggests that around 36% of all software currently in use has been stolen or being used illegally, much of it counterfeited and sold illegally:

“A 2011 raid by Haidian District Public Security Bureau in Beijing, China, found more than 360,000 partially finished Certificates of Authenticity (COAs). The product names and product identification had not been added, but they estimated that, when finished and packed, they would have been worth CNY 513.5 million (USD 79 million). In the same raid law enforcement discovered counterfeit products and finished COAs valued at approximately CNY 10.4 million, or USD 1.6 million. This included 4,400 channel original equipment manufacturer (OEM) products for Dell, HP and Lenovo: in other words, the software that you have bundled with your computer.” – Interpol, 2012⁸³

Counterfeiting of hardware often starts with the recovery of elements of discarded technology disposed of by the developed world and transported to the ‘trash heaps’ in the developing world. Components and materials from discarded phones, laptops and other hardware are harvested, either to resell the valuable raw materials or often to reassemble into near-identical counterfeit goods – either then sold as the finished article on the grey market, or reinserted into the supply chain to become part of other, legitimate goods.⁸⁴

“Technology is a vast industry, with a lot of touchpoints with [organized crime groups], but the most important thing for me is counterfeiting, groups copying and selling fake versions of our goods. This is dangerous for the consumers, for society, and hits us hard in terms of profit and reputation” – Interview Feedback, Global IT Products Firm, 2016

The cost of using counterfeit technology can be material: manufacturers unknowingly using sub-standard counterfeits risk financial losses and damage to brand image. More seriously, failures of medical, aerospace, automotive, military or similar types

82 Business Software Alliance, 2016

83 Interpol Casebook, 2015

84 General Works, 2015

<https://www.govtechworks.com/counterfeit-tech-marks-another-front-for-security-vigilance/#gs.=rbYf7c>





of equipment can result in injury and loss of life.⁸⁵

There have been recent accounts of counterfeit semi-conductors being found in an automated external defibrillator, resulting in a defibrillator over-voltage condition, which would have effectively electrocuted a patient, a counterfeit semiconductor which failed in a power supply used for airport landing lights, a batch of counterfeit microcontrollers intended for use in braking systems in high-speed trains in Europe and a batch of counterfeit microprocessors intended for use globally in automated medication applications, including intravenous (IV) drip machines.⁸⁶

“When parts fail unexpectedly in our vehicles we now take them back to our factory and take a forensic look at them – we have to make sure that something we have bought from an OEM supplier and put into a car is exactly what we thought it was, what it was supplied as – we know that sometimes even in our cars counterfeit components can enter the supply chain through sub contractors and we simply can’t afford for that to happen. The risk to our reputation is too great.” – Interview feedback, German car manufacturer, 2017

In addition to the issues directly surrounding counterfeited goods is the ability for these goods to be used to perpetrate further crimes. In January 2015 Trojan malware was found in counterfeit smartphones, including fake Samsung GS4s imported into the US from China. Not only were the phones’ handsets themselves not genuine, they carried further threats to the user – malware, embedded in a ringtone app, that allowed attackers to phish personal information and start downloads of additional malware through Google Android application package files. Later in 2015 Microsoft investigators found counterfeit Windows Operating System software on a number of new laptops purchased in China. They also found viruses, including the aggressive Botnet virus Nitel, on 20 percent of the machines.⁸⁷

“Counterfeit [technology] can contain malicious logic, backdoor vulnerabilities or both, and they can compromise ‘the confidentiality, integrity, or availability of the end-system and the information it contains.’” – GAO, 2015

What is our estimate of the direct financial impact on this industry, by segment and by crime type? What are the implications?

Research estimates that crimes in cyberspace, including those outlined here, will cost the global economy \$445 billion in 2016 – more than the market cap of Microsoft (\$411 billion), Facebook (\$314 billion) or ExxonMobil (\$332 billion) — according to an estimate from the World Economic Forum’s 2016 Global Risks Report.

85 ‘How to Combat Counterfeit Semi-Conductors’, ECN Mag, 2015
<https://www.ecnmag.com/article/2015/05/how-combat-counterfeit-semiconductors>

86 Semi-Conductor Industry Association, 2017,
http://www.semiconductors.org/issues/anticounterfeiting/anti_counterfeiting/

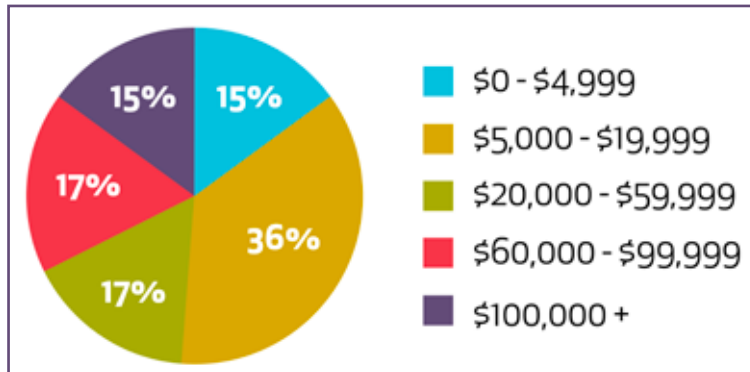
87 GAO, quoted in General Works, 2015
<https://www.govtechworks.com/counterfeit-tech-marks-another-front-for-security-vigilance/#gs.=rbYf7c>





Hacking and DDoS: According to a new report by Hewlett Packard and the US-based Ponemon Institute of Cyber Crime, hacking attacks cost the average American firm \$15.4 million per year, double the global average of \$7.7 million. The most costly cyber-crimes were those carried out by malicious insiders, DDoS and web-based attacks. The global financial services and energy sectors were the worst hit, with average annual costs of \$13.5 million and \$12.8 million, respectively.⁸⁸

Figure 7: The per hour cost of DDoS Attacks



About 49% of DDoS attacks last between six and 24 hours. This means that with an estimated cost of \$40,000 per hour, the average DDoS cost can be assessed at about \$500,000 – with some running significantly higher. Costs are not limited to the IT group; they also have a large impact on units such as security and risk management, customer service, and sales.⁸⁹

The average direct costs of a security breach on small businesses are \$38,000, according to a study from Kaspersky Lab. This total includes the costs of downtime, lost business opportunities and the professional services small businesses hire to mitigate the security breach.

The research shows that, on average, small businesses can expect to pay \$10,000 in professional services following a cyber attack. These services can include the hiring of IT security consultants, risk-management consultants, lawyers, physical security consultants, auditors and accountants, management consultants, and public relations consultants.⁹⁰

Fraud: Romance scams, a particularly odious internet fraud, have been a lucrative sideline for TOC groups. In the UK in 2016 admitted losses (it is clear that many people are too embarrassed to report their experiences) topped £33m, up from £29.1m in 2015.⁹¹ There is a similar picture in the North America, where US victims reported a collective loss of \$50.4 million in 2011,

88 The Rising Costs of Cyber Crime, 2016 Ponemon Institute Cost of Cyber Crime Study, <http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/>

89 Incapsula Survey : What DDoS Attacks Really Cost Businesses <https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf>

90 Worried About a Cyberattack? What It Could Cost Your Small Business. Chad Brooks. Business News Daily. 12 October, 2015 <http://www.businessnewsdaily.com/8475-cost-of-cyberattack.html#sthash.jT8oGUjZ.dpuf>

91 Commander Chris Greany, UK Police National Economic Crime Co-ordinator, 2015 <http://www.telegraph.co.uk/news/uknews/crime/11960852/Cost-of-online-dating-scams-jumped-16pc-last-year-say-police.html>





Canadian victims lost more than \$15million in 2013⁹². Romance scams are the number one scam in terms of financial losses in Australia, costing AUS\$27.9 million, a 10% increase on 2014.⁹³

CSEA: Direct costs to companies of CSEA are limited. In fact, the increased traffic could be argued as a positive for ISPs. However, the practical impact is higher, with staff and technical time required to take down sites that are found to be hosting or supporting CSEA, and significant reputational risk if brands are linked to CSEA. In 2003, MSN implemented restrictions in their chat rooms purportedly intended to help protect children from adults seeking sexual conversations with them. In 2005, Yahoo! chat rooms were investigated by the New York State attorney general's office for allowing users to create rooms whose names suggested that they were being used for this purpose. Yahoo! agreed to "implement policies and procedures designed to ensure" that such rooms would not be allowed.

Purchasing and trade: According to the FBI, Silk Road made a total of \$1.2bn between 2011 and 2013.⁹⁴ The marketplace is widely understood to be the fist 'killer app' for bitcoin, and drugs still make up a large proportion of transactions made using the digital currency today. While combined daily volumes hit \$650,000 in 2016 (averaged over 30-day windows) researchers say the total is generally stable at \$300,000 and \$500,000 a day.⁹⁵

Since the launch of the Silk Road in 2011, dark-web markets, including Silk Road 2, Evolution and Agora, have represented a shadowy and much-maligned corner of the internet. And the secretive nature of such sites makes them difficult to study. But in 2016 a study was undertaken to assess the scale of dark web trading.⁹⁶ In total the deals examined between December 2013 and July 2015 were worth around \$50m. Of those drugs, in particular MDMA (ecstasy) sold the most by value, while marijuana was the most popular single product, with around 38,000 sales. Legal drugs such as oxycodone and diazepam (Valium) were also popular.

Money laundering: It is close to impossible to calculate what proportion of total money laundered worldwide is specifically gaming- and gambling-related as so many money laundering schemes use multiple routes to evade detection – online activity plus real-estate or financial fraud.

Counterfeiting and piracy: Rochester Electronics has commented extensively on the issue and believes that semiconductor counterfeit activity is upward of \$3 billion annually.⁹⁷

EU Customs data estimated that in 2015 counterfeit electronic, computer, phone, AV, machine and broader technology equip-

92 FBI, money.cnn.com, <http://www.whoishostingthis.com/blog/2015/09/22/online-dating-scams/>

93 Australian Competition and Consumer Commission, 2015

94 USA vs Ross William Ulbricht 'Dread Pirate Roberts', 13 MAG 2328

95 Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, Kyle Soska and Nicolas Christin, Carnegie Mellon University

96 A researcher using the pseudonym Gwern Branwen cast some light on them. Roughly once a week between December 2013 and July 2015, programmes he had written crawled 90-odd cryptomarkets, archiving a snapshot of each page. The Economist has extracted data from the resulting 1.5 terabytes of information for around 360,000 sales on Agora, Evolution and Silk Road 2. <http://www.economist.com/blogs/graphicdetail/2016/07/daily-chart-8>

97 How to combat counterfeit semiconductors. Peter Marston. ECN. Advantage Business Media. 20 May, 2015 <https://www.ecnmag.com/article/2015/05/how-combat-counterfeit-semiconductors>





ment worth €61.5m entered the EU⁹⁸ and is one of the top fifteen most counterfeited sectors, and stated that this view of the importance of technology hardware to the global counterfeiting market is backed up by the “World Customs Organisation and the US Customs and Border protection whose data clearly reveals that electrical machinery and equipment are now the most frequently counterfeited products”.⁹⁹ In 2014 counterfeit technology hardware (computers and accessories, electronics and parts, optical goods) worth \$207million was seized, representing 17% of all goods seized.¹⁰⁰ In 2008 counterfeit computer and electronic goods made up 8% of all counterfeit seizures within the EU.¹⁰¹


How is the industry legally regulated to combat organized crime? What is the effectiveness of this regulation when compared to the costs? What examples or case studies exist of positive co-operation and remediation of organized crime in the public and private sector?

Historically regulation has largely protected ISP and communication providers from prosecution when their services are used for illegal activities by end users. Section 230 of the Communications Decency Act in the US states that “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” thereby absolving ISPs of liability for actions of end users, however later case law from the California Court of Appeal has established that held that CDA Section 230 does not apply to distributor liability, meaning that a defendant who had notice of a defamatory statement must stop publishing it or face liability.¹⁰² Similar regulation in the UK through the Defamation (Operators of Websites) Regulations 2013, part of the Defamation Act 2013, states operators of web sites ‘are not liable for defamation claims against them for user generated content (e.g. comments on a forum posted by users) provided they take certain actions within reasonable timeframes when notified of the offending content. Where the author cannot be contacted, (e.g. if the posting is anonymous or the user has supplied obviously bogus contact details), the website operator must take the content down or they can be liable’.¹⁰³

“Our focus is on preventing criminal activity on our network. We have dedicated departments of people, and dedicated streams of technology finding and blocking content that is illegal – terrorist support, child pornography, scams, and so on, and also unpleasant – racism etc. We do that as part of our corporate policy, not because of any regulation. The law in pretty toothless in our area to be honest” – Interview with Global Social Media Company, 2017

-
- 98 Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact. OECD/EUIPO. 2016. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Mapping_the_Economic_Impact_study/Mapping_the_Economic_Impact_en.pdf
 - 99 Written evidence submitted by the Anti-Counterfeiting Group (ACG) (DEB 50). UK Parliament. October 2016. <https://publications.parliament.uk/pa/cm201617/cmpublic/digitaleconomy/memo/DEB50.pdf>
 - 100 Intellectual Property Rights, Seizure Statistics, Dept. of Homeland Security, 2015 <https://www.cbp.gov/sites/default/files/documents/2014%20IPR%20Stats.pdf>
 - 101 EU, 2008 https://www.unodc.org/documents/data-and-analysis/tocta/8.Counterfeit_products.pdf
 - 102 Barrett v. Rosenthal, 114 Cal. App.4th 1379 (2002)
 - 103 Daily Hansard, 19 Nov 2013 : Column GC37 - Defamation (Operators of Websites) Regulations 2013





A greater influence is the reputational impact of being seen to facilitate or fail to prevent illegal activity, particularly in sensitive areas like CSEA. In 2005 Yahoo! closed its internet chatrooms after an exposé by Houston TV station KPRC showed that Yahoo! chatrooms with clear and unambiguous names (Girls 13 And Under for Older Guys and 9-17-Year Olds Wantin' Sex) were being hosted by the ISP. Although a \$10m lawsuit against Yahoo! failed, as it was not deemed legally responsible, a number of major advertisers, including Pepsi, State Farm, Georgia Pacific Corp, Countrywide Mortgage and T-Mobile, stopped working with Yahoo! in response to the claims and the company lost material revenue.¹⁰⁴

“We try to block terrorist and particularly child pornography on our sites because we are decent people and because we can't risk the reputational hit we would take if it was found there. It's not a legal thing, it's a decency and reputation thing” – Interview with Global Internet Communications Company, 2017

More recently there has been greater voluntary collaboration between technology and communications providers in the areas of CSEA and terrorist activity, though still little in other areas of internet-based or internet-enabled criminality. The success of the UK-based Internet Watch Foundation in reducing CSEA sites has been strongly driven by the co-operation of global technology sites rather than regulation or legal action.

“The UK now hosts just a small volume of online child sexual abuse content – 0.2% of the global total. In 2015 we took action on 68,092 webpages displaying illegal child sexual abuse images and videos, hosted on websites around the world. We took action on 135 webpages hosting images and videos in the UK and issued 34 takedown notices. We might send one notice for several webpages and content may have already been removed by the time we get authorisation from the police. We're proud to say that the relatively low number of UK hosted child sexual abuse imagery shows how the online industry is helping make the UK a hostile environment for this criminal content to be hosted. Today 0.2% of the world's known online child sexual abuse imagery is hosted in the UK. When we started in 1996, that figure was 18%.”¹⁰⁵

CASE STUDY – CSEA payment

Elliptic, a bitcoin startup based in London, and the Internet Watch Foundation (IWF), a charity monitoring child abuse on the web, are partnering to suppress the use of BTC in online child pornography. Recently, the IWF provided Elliptic a database of bitcoin addresses that they identified with child porn. With this information, Elliptic can identify those illegal activities on the block chain (bitcoin's public ledger of transactions). James Smith, CEO of Elliptic, said this regarding their involvement: “This is the first time anybody has started identifying these crimes in bitcoin and flagging them up in a system like ours. This is a great step... towards our goal of getting rid of any sort of illicit activity in bitcoin.”

Elliptic counts the biggest US and European bitcoin exchanges as clients and also provides evidence to federal agencies in the United States and Europe for major investigations involving bitcoin. Accor-

104 Yahoo closes user-created chat rooms over sexual conduct. Wikinews. 24 June, 2005.

https://en.wikinews.org/wiki/Yahoo_closes_user-created_chat_rooms_over_sexual_conduct

105 Internet Watch Foundation, 2016





ding to the firm, their status could make them “uniquely take action”.

The BTC startup will integrate IWF’s database into their own transaction-monitoring systems and will alert clients when they see transactions from the bitcoin addresses flagged by IWF.

Internet Watch Foundation Chief Executive Susie Hargreaves made this statement:

“Over the past few years, we have seen an increasing amount of bitcoin activity connected to

purchasing child sexual abuse material online. Our new partnership with Elliptic is imperative to helping us tackle this.” Deep Dot Web, 2016

In some cases, the desire to work with the authorities is present, but is thwarted:

“We want to work with the police in America to put Amber Alerts on our platform, to help get the message out faster. This was our idea, and we are ready to go, but the authorities don’t have technology that can interface with ours, theirs is too old. We are trying to find a way around this” – Interview with Global Social Media Company, 2017

In December 2015 four of the biggest technology and social media companies came together to create a database of terrorist and extremist hashtags so that as soon as one company identified a hashtag related to terrorism it would be logged and shared with the others. Google, Facebook, Twitter and Microsoft have stated their intention to work together to identify and remove extremist content on their platforms through the information-sharing initiative.

“Starting today, we commit to the creation of a shared industry database of “hashes” — unique digital “fingerprints” — for violent terrorist imagery or terrorist recruitment videos or images that we have removed from our services. By sharing this information with each other, we may use the shared hashes to help identify potential terrorist content on our respective hosted consumer platforms. We hope this collaboration will lead to greater efficiency as we continue to enforce our policies to help curb the pressing global issue of terrorist content online.” – Facebook statement, 5 December 2016

Most notably, and perhaps disturbingly, this has been originated and created by the four companies working with a counter-terrorism NGO, without involvement of government or law enforcement. Given that in October 2016 the US Department of Justice stated that “most young terrorist recruitment is linked to social media”,¹⁰⁶ it would seem that this should have been an obvious partnership for the government to pursue. It does, however, highlight the potential for the private sector to work proactively and independently to fight criminal activity worldwide.

106 John Carlin, US Department of Justice, October 2016





Industry Consumer Goods and Retail

How does this industry break down into segment? What is the size, scale and geographic spread of each segment?

At its simplest definition, the consumer goods sector relates to items purchased by individuals rather than by manufacturers and industries. The sector includes companies involved with food production, packaged goods, clothing and beverages, personal care, automobiles and electronics. For the purposes of this study we have focused on fast-moving consumer goods (FMCG) categories.

The top countries in terms of total household (incl. consumer) financial consumption expenditure are¹⁰⁷ the US \$12.2 trillion; China \$4.2 trillion; Japan \$2.4 trillion; UK \$1.8 trillion; and Germany \$1.8 trillion.

As an industry, consumer goods is larger even than the financial sector, with global retail sales in excess of \$20 trillion. By 2025, a staggering 4.2 billion people will be part of the consuming class.¹⁰⁸ For the first time ever, the number of people with discretionary income will exceed the number still struggling to meet basic needs. Consumption growth, however, is not even. It is happening much faster in certain categories and markets. In Shanghai the skin-care category will grow three times as fast in absolute terms as in all of Malaysia, based on 2010–20 compound annual growth rate (CAGR).

The FMCG segments forecast to be the fastest growing are:

- Prepared food in China by nearly 21%
- Beverages in Mexico by 16.9% annually
- Household products in India and South Africa by almost 21% and 12% respectively
- Beauty products in Turkey by close to 20%
- Beauty and food service in the US by over 5%
- Non-alcoholic drinks in the UK by some 4%

The world pharmaceutical market was worth an estimated \$794,393 million¹⁰⁹ at ex-factory prices in 2015. The North American market (USA & Canada) remained the world's largest market ahead of Europe and Japan.

There is rapid growth in the market and research environment in emerging economies such as Brazil, China and India, leading to a gradual migration of economic and research activities from Europe to these fast-growing markets. In 2015 the Brazilian and Chinese markets grew by 14.0% and 7.0% respectively, compared with an average market growth of 5.9% for the total European market and 8.5% for the US market.

107 The World Bank

108 McKinsey, Tough choices for consumer-goods companies, Jim Brennan, Greg Kelly, and Anne Martinez, Dec 2013

109 The World Market in Pharmaceuticals, EFPIA, 2016





In 2015 North America accounted for 48.7% of world pharmaceutical sales compared with 22.2% for Europe. According to IMS Health data, 58% of sales of new medicines launched during the period 2010–2015 were on the US market, compared with 23% on the European market (top five markets). The fragmentation of the EU pharmaceutical market has resulted in a lucrative parallel trade. This benefits neither social security nor patients and deprives the industry of additional resources to fund Research and Development. Parallel trade was estimated to amount to €5,589 million (value at ex-factory prices) in 2015.

In the consumer and pharmaceutical sectors a small number of global players have shown increasing dominance. In pharma Pfizer, at \$43 billion is the largest, followed by Novartis \$42 billion, Roche \$39 billion and Merck \$35 billion. In consumer markets Procter and Gamble dominate at \$65bn, Unilever at €53bn and L'Oréal €25bn.

What types of organized crime feature in this industry? Which geographies and segments are most affected?

The consumer goods and pharma industries are so ubiquitous, pervasive and global that they offer organized criminals myriad opportunities for financial gain. Key categories of crime in these sectors include:

- Counterfeit goods – illegal copying of trademark protected products
- Fraud and corruption – extortion, bribery, theft of assets, funds theft
- Money laundering – moving money gained from predicate crimes
- Human trafficking – illegal labour and modern slavery practices

Counterfeiting is the most well researched of these criminal markets. The UNODC covers counterfeiting specifically, and quotes a global market size of \$250 billion¹¹⁰ or 1.9% of world trade, from a comprehensive study by OECD in 2008.¹¹¹ Counterfeiting is without doubt a major component of organized crime in consumer goods markets. A 2016 study for OECD by BASCAP updated the 2008 paper, and estimated a rise of global counterfeiting to \$461 billion, or 2.5% of world trade. Although the two estimates are not directly comparable, they do follow a similar methodology.¹¹² For the EU the proportion of trade rises: total counterfeit and pirated products to the EU amounted to \$116bn in 2013, or 5.1% of EU imports.¹¹³

According to statistics from the World Customs Organization, the US Government and the EC, much of the world's counterfeit products can be traced back to China. In 2008, the World Customs Organization, reporting on data collected from 121 countries, found that 65% of the total of counterfeit shipments detected departed from mainland China, accounting for some 241 million pieces seized globally. Hong Kong was the departure point for another 8 million, bringing the figure above two-thirds of the global

110 Transnational organized crime: the globalized illegal economy. UNODC. Accessed November 2017.
<https://www.unodc.org/toc/en/crimes/organized-crime.html>

111 OECD project on counterfeiting and piracy 2008, 2009

112 OECD Trade in Counterfeit and Pirated Goods, Mapping the Economic Impact, 2016

113 Ibid





total.¹¹⁴

Tobacco and alcohol follow a slightly different pattern, where counterfeiting exists, but the greater criminal focus is on 'contra-band' markets (legitimate products trafficked across borders for tax/excise arbitrage opportunities). Estimates for the annual state and local US tax loss caused by the illicit trade in tobacco products range from \$2.95 to \$6.92 billion. For the EU, proceeds from the illicit trade in tobacco products range from €7.8 to €10.5 billion annually. The most recent estimate of the global tax lost, conducted in 2006, estimates the tax loss due to the black market is between \$40 and 50 billion annually, with illicit actors often the beneficiary. Based on the most recent data, it is estimated that the global illicit cigarette trade was 10.7% of total sales, or 600 billion cigarettes, in 2006.

In terms of counterfeit pharmaceuticals, the incidence is more targeted at specific developing countries.

Whereas in developed economies counterfeits may account for less than 0.2 percent of the market¹¹⁵ developing markets are often beset by 30% fakes, as a UNODC report showed for anti-malarial drugs in Africa.

The Pharmaceutical Institute documented 3,002 incidents of pharmaceutical counterfeit crime during 2015 – the highest annual incident total ever recorded. Counterfeiting incidents increased by 14% over 2014. Continuing a trend that has developed over the last few years, incidents of illegal diversion increased significantly. The number of verified diversion incidents increased by 74% over the prior year as diversion incidents reached its highest recorded total of 1,106 incidents.¹¹⁶

Significantly less reported is fraud, and corruption. Yet according to a PwC global survey in 2014, 49% of retail and consumer goods companies have suffered economic crime during the last two years, compared to only 37% across all other industries. Asset theft is the primary type of reported economic crime.

Procurement fraud and bribery and corruption are also major issues.¹¹⁷ According to the Deloitte India Fraud Survey, 2014, around 54 percent of survey respondents belonging to the consumer products sector said they had most frequently experienced theft/diversion of goods, and bribery and corruption over the last two years.¹¹⁸

Kroll's 2015/16 Global Fraud Report also offer disturbingly high fraud incidence. The consumer goods sector had a reported incidence of fraud by respondents of 72%, and the pharmaceutical and healthcare sector of 69%. Total financial loss in consumer goods was 0.6% of revenues compared to 0.8% for pharma/health. Consumer goods companies felt highly vulnerable (over 20%) to vendor and supplier fraud, and thefts of assets. Pharma and healthcare clients to corruption/bribery, and information theft.¹¹⁹

114 UNODC, Counterfeit Products, Reader

115 Illicit Trade in Counterfeit Medicine, Dr. K Lybecker, Colorado College, 2015

116 PSI Situation Report 2015, May 2016

117 PwC Retail and Consumer Goods Sector Analysis of PwC's 2014 Global Economic Crime Survey

118 Deloitte India, Fraud Risks in the consumer products and retail sector, 2014

119 Kroll, Global Fraud Report 2015/16, Vulnerabilities on the Rise





Money laundering is common in the consumer sector – particularly in high-value goods such as jewellery, automotive and yachts. According to Transparency International, the high-value retail sector has major money laundering compliance issues.

“Enforcement is low and its understanding of the rules and threats are poor”.

Transparency International (TI)

In the UK, while 1,294 high-value dealers are registered with HMRC, there is no fit and proper test assessing the supervised population, and the level of anti-money laundering enforcement was the lowest of all the sectors reviewed. The number of dealers who are registered is also probably too low, according to Transparency International (TI). Suspicious reports from the high-value retail/dealer luxury sector were 331 in October 2013 – September 2014, but still only amounted to 0.09 per cent of the total, and this figure compares starkly to financial institutions’ 321,851.¹²⁰

Human trafficking is a significant issue in consumer markets. The International Labour Organization makes a clear connection between counterfeiting and labour exploitation.¹²¹ As far back as 1996, the ILO reported on labour and the clothing industry noting,

“few (clandestine workshops) pay any respect to labour legislation and many hire illegal migrants. Many are involved in counterfeiting products from famous trademarks”.

In a subsequent report from 2000, the ILO stated that clandestine workshops:

“employ large numbers of illegal immigrants, who have specialized in copying and pirating well-established brand names”.

Furthermore, these are generally marked by labour practices that are contrary to the most rudimentary principles of respect for human rights at work, including confiscation of immigrant workers’ identity papers and housing illegal workers in hazardous and unhealthy dormitories. Other accounts of counterfeiting and labour exploitation also exist. One investigative reporter, whose writing on the fashion industry includes first-hand experiences with counterfeiting workshops, discusses the presence of exploited labour – in particular situations involving the excessively cruel and criminal treatment of children as young as six – in various countries where workers are forced to assemble counterfeit goods.

120 UK luxury sector targeted over money laundering, FT, November 23rd 2015

121 Focus on: The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime. UNODC.
https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf





What is our estimate of the direct financial impact on this industry, by segment and by crime type? What are the implications?

Whilst estimates of counterfeiting are plentiful, up to the \$461bn level, an estimate of the total effect of organized crime on the consumer sector is hard to come by. Kroll's Fraud report cites respondents in the consumer sector estimating the fraud effect of 0.6% of revenues, which would equate to a staggering \$120bn. In pharmaceuticals the figure was 0.8% which would equate to \$6.36bn.

How is the industry legally regulated to combat organized crime. What is the effectiveness of this regulation when compared to the costs? What examples or case studies exist of positive co-operation and remediation of organized crime in the public and the private sector?

Regulation of counterfeit or illegal products has been slow. Most regulation is focused on consumer safety and health, and very little focuses on countering the criminal effect. Much of the consumer and pharmaceutical industries' protection from intellectual property theft comes from the patent, trademark and design laws, that govern ownership. The registration of intellectual property is an industry in itself, with EU trademarks, for example, now reaching 100,000 a year in 2014.

But enforcement of this protection is down to border policing – which since the financial crisis has been under significant financial strain, and therefore under-resourcing. Comparing the total seizures to total illicit trade, more than 40 million products suspected of violating an intellectual property right were detained at the EU's external borders, with a value of nearly €650 million, in 2014.¹²² But in the same period the OECD's estimate of counterfeit goods was €85bn. This suggests a detection rate of only 0.7%.

Informal co-operation between to the public and private sectors, to counter counterfeits and illicit trade is relatively good. The OECD's Taskforce for Charting Illicit Trade is a good example, as are initiatives by World Customs Organisation, and international trade fora. But there is no explicit mechanism for information sharing or joint investigation, and experiences of positive investigative co-operation between public and private sectors remain anecdotal.

In pharmaceuticals, the counterfeit problem is well recognised, but actual remediation efforts in developing countries, where the problems are most severe, are woefully low. In 2006 the WHO created a global initiative, the International Medical Products Anti-Counterfeiting Taskforce (IMPACT) to provide a global approach to solving the problems of pharmaceutical counterfeiting. Unfortunately, the initiative was derailed by linguistic disputes over the definition of counterfeit drugs.

"This struggle over language and the paralysis that resulted are indicative of the tremendous challenges that characterize the battle to combat pharmaceutical counterfeiting."¹²³

122 Customs Union: Number of counterfeit goods seized by EU authorities continued to rise in 2015. European Commission. 23 September 2016. http://europa.eu/rapid/press-release_IP-16-3132_en.htm

123 Illicit Trade in Counterfeit Medicine, Dr Kristina Lybecker, March 2015





Interestingly money laundering, whilst seen as a material threat in these sectors, does not always fall under the government requirements for suspicious activity reporting. In the UK, AML controls require almost all financial institutions to file suspicious activity reports, but these apply only to 'high value dealers' in the retail category – those who accept payments for more than €15,000 in cash.¹²⁴

CASE STUDY

The most prominent success story in the developing world fight against counterfeit medicines is that of Nigeria and the NAFDAC (National Agency for Food and Drug Administration and Control). The agency is a pioneer in the fight against spurious medicines in West Africa. In 2001, an estimated 80 percent of the medicines sold within Nigeria were counterfeit or substandard. In 2002, within the six principal drug markets across Nigeria, 68 percent of medicines were unregistered by the agency. The study was repeated in 2003 with an 80 percent reduction in the number of unregistered medicines. By 2006, the share of counterfeit drugs had dropped from 41 percent (2001) to 16 percent (2006). The efforts to combat pharmaceutical counterfeiting in Nigeria began with a single policy: restricting pharmaceutical imports to only two airports and two seaports, each staffed by NAFDAC officials. This was followed by the discovery of several Chinese and Indian drug manufacturers suspected of producing and exporting fake drugs in Nigeria, which resulted in the termination of the importation of those products. NAFDAC then established independent contracts with regulatory authorities in China and India to oversee exports to Nigeria. As described by UNICRI, the efforts undertaken since 2001 have markedly improved the security of the Nigerian pharmaceutical supply chain.¹²⁵

In the fight against illicit products, regulation of supply chains is beginning to emerge, albeit slowly. For example, in tobacco The Framework Convention on Tobacco Control Protocol's aims are explicit – to eliminate all forms of illicit trade in tobacco products by requiring parties (i.e. countries) to take measures to control the supply chain of tobacco products and to cooperate internationally on a wide range of remediation measures.¹²⁶ This move is reflected in EU's Tobacco Products Directive, which requires track and trace systems to be in place by 2019.

In the European pharmaceutical industry in January 2013, regulators in Europe adopted the European Falsified Medicines Directive (FMD), which aims to prevent falsified medicines from reaching patients by introducing harmonised, pan-European safety and control measures.¹²⁷

In terms of the effect of ethical supply-chain practices, including the effect of the anti-slavery legislation, the academic press is

124 Guidance: Money laundering supervision for high value dealers. HM Revenue & Customs. UK Government. 3 June 2013 <https://www.gov.uk/guidance/money-laundering-regulations-high-value-dealer-registration>

125 Illicit Trade in Counterfeit Medicine, Dr Kristina Lybecker, March 2015

126 KPMG, Track and Trace in Tobacco, 2014

127 Ibid





mixed. Long after factory audits were introduced, the Rana Plaza catastrophe hit in 2013,¹²⁸ in which a garment factory collapsed in Bangladesh, killing at least 1,133, with a further 2,500 injured and many left severely disabled. Interestingly there is little specific Western regulation of this issue. So the best regulations are local, and national:

“I believe the Bangladesh Fire and Safety Accord is the best hope we have of improving safety in that country. Essentially built from the rubble of Rana Plaza, it is a contract between the retailers and the trade unions in Bangladesh. It’s a legally binding, five-year pact that makes independent safety inspections of factories and public reporting on them mandatory. The first list of 1,500 Bangladesh factories to be inspected has just been published.”¹²⁹

128 How ethical are high-street clothes? Lucy Siegle. The Guardian. 6 October 2013

<https://www.theguardian.com/environment/2013/oct/06/ethical-high-street-clothes-supply-chain-bangladesh>

129 Lucy Siegle, Guardian, 6 October 2013





Industry: Construction and Real Estate

How does this industry break down into segment?

What are the size, scale and geographic spread of each segment?

The construction industry, from the commissioning and contracting to build, through to the sale and resale of the finished assets has long been a lucrative and highly attractive market for TOC groups. The sector covers both residential and commercial development, alongside the massive infrastructure projects increasingly being commissioned worldwide.

Its scale – the global industry was valued at US\$8.5 trillion in 2015 and is forecast to be worth US\$10.3 trillion in 2020¹³⁰ and resistance to local economic downturns - the continual push of the increasing global population demanding the creation of new residential, commercial and infrastructure developments, make it a financially rewarding destination for legitimate business and criminal activity alike. The sector’s exponential growth shows no sign of halting with growth accelerating from an average of 2.7% a year in real terms in 2011-2013 to 3.8% in 2015 to 3.9% to 2020.

TOC groups operate globally in the construction industry, but the strength of the sector in emerging markets with lower regulation and greater demand for housing and infrastructure fuels much of the illegal activity. Emerging markets accounted for more than half of the world’s construction output for the first time ever in 2012 and by 2020 it will have a 56% share. By 2020 emerging markets are forecast to record a 5.3% annual expansion, compared to 2.2% for established economies.¹³¹ Alongside the US, China and India will account for 57% of all global growth in the construction and engineering market by 2030.

“Construction is likely to be one of the most dynamic industrial sectors in the next fifteen years and is utterly crucial to the evolution of prosperous societies around the world. The numbers within this report are huge and that translates as creating vast numbers of new jobs and creating significant wealth for certain countries across the globe” –

Fernando A. González, Chief Executive of global building materials company CEMEX.

The favoured money laundering route of the majority of TOC groups, real-estate (residential and commercial construction) is the single largest asset group in the world. The total value of all developed real estate on the globe reached US\$217 trillion in 2015,¹³² nearly three times the value of global GDP in 2015.

“To give this figure context, the total value of all the gold ever mined is approximately US\$6 trillion, which pales in comparison to the total value of developed property by a factor of 36 to 1. The value of global real estate exceeds – by almost a third – the

130 When measured at constant 2010 prices and exchange rates (real 2010 US\$). Construction Intelligence Center’s Global 50

131 Global Construction 2030, Global Construction Perspectives and Oxford Economics, 2015/2016 <http://www.prnewswire.com/news-releases/global-construction-market-worth-103-trillion-in-2020-50-largest-most-influential-markets-292235961.html>

132 Around the World in Dollars and Cents, Trends in International Real Estate, 28 January 2016, Savills Worldwide <http://pdf.euro.savills.co.uk/global-research/around-the-world-in-dollars-and-cents-2016.pdf>



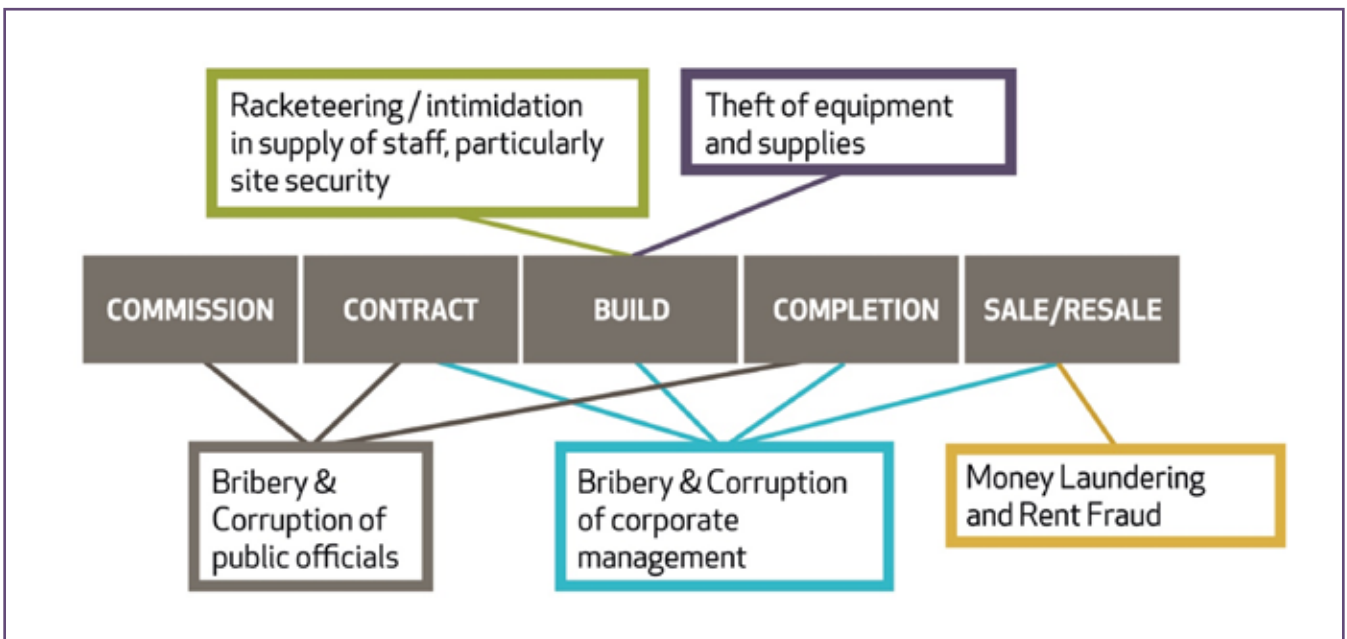
total value of all globally traded equities and securitised debt instruments put together and this highlights the important role that real estate plays in economies worldwide.” – Yolande Barnes, Head of Savills World Research.

The geography of cross-border real estate trading provides opportunities for TOC groups. Inward investment from overseas is more material to European real-estate markets than Asian and American ones. Cross-border deals now account for 8 in every 18 EMEA deals. Prior to the global financial crisis in 2007/8, Asia was a greater target for overseas real estate investment with one in every two domestic deals bought by investors outside the region however it is now echoing the Americas, where one deal in every ten is traded outside the region. This cross-border nature of acquisitions increases the ability of TOC groups to move money between opaque entities, capitalise on property value hotspots and blur the financial trail left for investigators.

What types of organized crime feature in this industry? Which geographies and segments are most affected?

While a popular perception of the ‘traditional’ transnational organized crime group might focus on activities concerning drugs, arms and prostitution, these groups have deeply entrenched links to established, legitimate sectors, including construction.

Figure 8: Activities of TOC Groups in the Construction and Real Estate Sector



The financial rewards available in a major construction project raise attractive opportunities for criminal activity at every stage, from bribery and corruption of officials to grant zoning for construction and contracts awarded to specific construction firms, through theft of high value equipment and stock from building sites to money laundering and financial fraud through the sale and resale of the completed properties.

Construction is very much a sector that suffers from TOC activity, rather than facilitates it. The opposite applies to Real Estate.



The construction industry is highly susceptible to asset appropriation crime and it remains the most highly reported crime in the industry – 76% of respondents to a 2014 crime survey in the construction and engineering sector reported suffering asset theft, the highest of any sector surveyed.¹³³ Factors such as the constant turnover of staff, the mobility of the workforce and the temporary nature of project work make the industry an easy target for both opportunistic petty criminals and serious organized crime.¹³⁴ In a 2015 survey of construction companies operating worldwide, 43% of respondents stated that site burglaries and plant theft were believed to be the activity of TOC groups.¹³⁵

“We padlock the gates at night to stop casual thieves but they are not our real concern. The loss of some supplies or even the occasional bit of equipment is factored into our costs. An attack by a properly organized crime group is different – no standard security measures or guards will stop that and it can cost us a fortune. It is an increasing problem, even on mid-size rural jobs” – Interview with UK construction company, 2017

Plant theft in particular is enabled by the nature of construction sites. Sites have long periods of inactivity at nights and at weekends, are transient with cost focused rather than sophisticated security structures around a site, and the security guarding teams in place can have their own issues with TOC (see later in this report). Further, the bulk of valuable plant and equipment is not covered by a central registration system, so there is no repository of identifying information for recovered items and disposal on the legitimate used equipment market, as well as the “black” market is straightforward.¹³⁶

Alongside the theft of high-value plant and equipment, theft of high-value components from construction and fully operational infrastructure sites is becoming an increasing problem as scrap metal prices rise. Copper prices have increased more than four-fold over the last fifteen years¹³⁷

“Copper thieves are threatening US critical infrastructure by targeting electrical sub-stations, cellular towers, telephone land lines, railroads, water wells, construction sites, and vacant homes for lucrative profits”. – FBI, 2011

While, historically, stolen copper was sold to scrap metal merchants tightening of regulation¹³⁸ has seen a rise in the activities of TOC groups who are not only able to circumvent the laws more easily but can also offer higher prices offset by their ability to offer economies of scale:

“Indeed, the crackdown by police on scrap-metal merchants, is believed to have resulted in the rise in prominence of organized Roma gypsy criminal gangs, who ship stolen metal directly out of the country.¹³⁹ One ton of top-quality pure bright cop-

133 Fighting corruption and bribery in the construction industry, PwC, 2014

134 Crime in the construction industry, CIOB, 2007

135 2015 CVS Headline Tables, UK Home Office, 2015

136 Construction Industry Theft Summit, Construction & Mining Equipment Industry Group & Civil Contractors Federation

137 Moore Research Center Inc, 2014

138 For example the Scrap Metal Dealers Act in 2013 in the UK

139 Undercover with copper-cable thieves who are costing Britain £770million a year. Chris Rogers. Daily Mail. 19 February 2012 <http://www.dailymail.co.uk/home/moslive/article-2101462/Copper-cable-theft-costing-Britain-fortune.html#ixzz-4VGmQbLqX>





per – that could get us 4,000 notes from a scrapyard – but we got £5,700 from the gypsies [Roma Organized Crime group].”
Convicted copper thief, UK 2015

In addition to the loss of plant and equipment, the construction industry is also susceptible to extortion through to the unwelcome and unwanted imposition of additional ‘workers’ at the behest of TOC groups. It is often difficult to ignore or refuse these criminal demands, whether they involve forcing security services on a project or ‘finding’ labourers to join the workforce. The mafia’s control over the US construction industry, particularly along the East Coast in the 1970s – 1990s is well documented, but the threat is still live in many other well-developed nations, particularly in the area of security service racketeering. Typically, these organisations force their services onto construction sites, which have little choice but to accept the security on offer. Damage to the site and threats of violence against staff have occurred when site managers tried to refuse these security services.¹⁴⁰

There are further issues with human trafficking of site labourers. As a significant employer of short-term, contracted workers and with major projects often located in less well-regulated high-growth emerging markets, construction has been a clear target for people trafficking and enslaved workforces. Research by the Chartered Institute of Building highlighted the ‘dark side’ of the construction industry:

“Our sector is rife with human rights abuses. Bonded labour, delayed wages, abysmal working and living conditions, withholding of passports and limitations of movement are all forms of modern slavery and the systematic exploitation of millions of vulnerable migrants. Human exploitation is a global issue, embedded both in the developed and developing world. And it’s just as prevalent in construction as in other industries, from northern Canada to New Mexico, from Japan to Jaipur, from Europe to the UAE. [M]any in positions of influence and power are turning a blind eye to obviously forged documents, even on large scale projects. In doing so, they are not only colluding in exploitation, they are supporting organized crime!”¹⁴¹

Bribery and corruption have long pervaded the construction industry, and the construction sector is widely reported as one of the most corrupt globally. The procurement and completion of large-scale construction projects demands co-operational and interaction between the multiple parties, and the balance between activities that legally facilitate this process and those which are tainted by concepts of bribery or corruption is not always clear.¹⁴²

“We are currently running one of the largest construction projects in Europe, and we are fighting hard to make sure there is no corruption, bribery or forced labour involved. With multiple sub-contractors and agents this is very hard – we know the risk is there, it always will be on a large construction job” – Interview with global natural resources company, 2017

Public works and construction repeatedly top the charts of Transparency International’s Bribe Payers’ Index, perceived as the

140 Crime in the construction industry, CIOB, 2007

141 Modern Slavery: The Dark Side Of Construction, CIOB, 2015
<https://policy.ciob.org/wp-content/uploads/2016/02/CIOB-Research-The-Darkside-of-Construction.pdf>

142 Bribery and Corruption in the Construction Industry: Challenges for International Construction and Engineering Projects,” Construction Law Journal, 2013





sector most likely to engage in bribery.¹⁴³ Research covering global construction companies in 2014 suggested 49% of respondents had faced bribery or corruption crimes within the previous 24 months, compared to 27% across all sectors,¹⁴⁴ and 64% of engineering and construction executives saw bribery and corruption as the highest risk of operating globally. More than one in four (29%) acknowledge that they've been asked to pay a bribe and 38% say they've lost an opportunity to a competitor who they suspect paid a bribe.¹⁴⁵ In addition to bribing officials to win construction contracts there is evidence of bribery to persuade safety inspectors to pass substandard work as acceptable¹⁴⁶ and of construction companies choosing or being forced to falsify staff work records to overcharge end customers.¹⁴⁷

Like construction, its downstream neighbour the Real Estate sector is a favoured target of TOC groups. It is believed that real estate is one of the most commonly used methods of money laundering by TOC groups. The FATF is clear that it is simpler and less risky for TOC groups to launder money through real estate than through the banking system in many important jurisdictions because governance regulations are considerably less onerous in property conveyancing than in banking.¹⁴⁸

Money laundering through Real Estate schemes is facilitated by weak governance and oversight schemes in key geographies.¹⁴⁹ The challenges of establishing 'beneficial ownership' of a property as opposed to simply the name of the offshore company that is on the deeds is often beyond the capabilities of a real estate company, and if some efforts have been made it is hard to prove the real estate company has been negligent and so prosecutions are rare. Further regulatory gaps and deficiencies play into the hands of buyers and sellers seeking anonymity and shade, and can be summarized below:

- Lack of due diligence and Know Your Client checks: US, UK
- No reporting requirements for real-estate brokers and lawyers: Australia
- Land Registry not required to list beneficial ownership of properties, only the 'title holder': UK
- Transactions undertaken by lawyers on behalf of clients protected under solicitor/client privilege: Canada, anywhere using British Law systems
- Foreign companies and nationals able to buy property without an in-country presence: UK
- In-country crime prevention bodies unable to process volume of reports: UK
- Requirement for hard currencies, desire for growth, lack of regulatory sophistication and capacity: Kenya, South America, Asia

143 Corruption and collusion in construction: a view from the industry, Engineers Against Poverty, 2014

144 Fighting corruption and bribery in the construction industry, PwC, 2014

145 Ibid.

146 Inspectors Accept Bribes to Pass Unsafe Buildings, <http://blog.capterra.com/construction-fraud-stories/>

147 Hunter Roberts Scams Schools in New York, <http://blog.capterra.com/construction-fraud-stories/>

148 Money Laundering Schemes in Real Estate, Corporate Compliance Insights, 17th February, 2016; Money Laundering, Global Financial Integrity, November 2016; Money Laundering & Terrorist Financing Through The Real Estate Sector, FATF, 2007

149 Money Laundering Schemes in Real Estate, Corporate Compliance Insights, 17th February, 2016 <http://www.independent.co.uk/news/business/news/london-property-market-real-estate-money-laundering-over-seas-foreign-buyers-mps-a7138176.html>, 15th July, 2016 Global Agenda Council on Organized Crime, WEF, 2011





To a lesser extent real estate also provides opportunities for TOC groups to benefit financially from redevelopment and repossession of properties, particularly through intimidation and extortion. The Yakuza crime groups have a history of 'jiange' – harassing tenants to move out of a building they want to purchase and redevelop. The groups across the world are active in the illegal occupation of houses and apartments by threatening landlords or house owners who may object by controlling auctions of repossessed houses and apartments and purchasing properties at well below market price.¹⁵⁰

Unlike other sectors, the construction industry is primarily a direct target of TOC groups. Its use to either directly or indirectly facilitate other crimes is more limited. On occasion plant theft may be undertaken to order to provide the hardware for another crime, such as the theft of backhoe loaders to facilitate the theft of automated teller machines (ATMs) from banks, or the partial destruction of cash-in-transit vehicles to allow access to the cash compartment of the secure vehicle. In their failed attempt to steal diamonds from the Millennium Dome in London, an organized crime group in 2000 used a stolen backhoe loader to break through security gates and into the Dome.¹⁵¹

Or, anecdotally, to dispose of TOC group generated corpses...

"Marvin is sure [Jimmy] Hoffa's body rests in the concrete footing of the Renaissance Center, which was under construction at the time of his disappearance. The story Marvin heard from Detroit mobsters is that after Hoffa was snatched and killed, practically every union carpenter in and around the city was called in to rush the construction of wooden forms needed for pouring concrete at the Renaissance project. As soon as the forms were in place, the concrete flowed, tons of it; ahead of schedule. Never before or since has he heard of his union brothers working so diligently to get a project done." – excerpt from 'The Weasel: A Double Life in the Mob, by Adrian Humphreys, published by Wiley.

Unlike construction, money laundering through real estate is a crime that entirely uses the industry to facilitate the crime rather than target the industry. Indeed it can be argued that the rise in both the volume of real-estate transactions and the increased value of them benefits rather than harms this sector.

What is our estimate of the direct \$ impact on this industry, by segment and crime type? What are the implications?

A snapshot quantification of the value of plant theft shows just how material the impact of this crime, largely driven by TOC groups, can be. A review conducted in the UK by market leading insurer Allianz Cornhill in December 2016 revealed in 2015 that 'over £70 million of construction plant had been stolen from construction sites in the last year'. Similarly, research in Australia into the cost of equipment theft in the construction industry indicates that it may be as high as \$50 million a year across the country.¹⁵² As far back as 2005, sources in America estimated the loss to the US construction industry of plant and equipment

150 Yakuza activities: extortion, welfare scams and involvement in companies, construction, real estate and banks. Jeffrey Hays. Facts and details. 2009 <http://factsanddetails.com/japan/cat22/sub147/item810.html>

151 The National Plant & Equipment Register, UK

152 Construction Industry Theft Summit, Construction & Mining Equipment Industry Group & Civil Contractors Federation





exceeded \$1bn per annum, not including consequential losses. These consequential losses, including hire of replacement equipment, loss of business, worker and client claims for resulting damage and injuries, increased insurance premiums¹⁵³ and the replacement of expensive equipment¹⁵⁴ can multiply these direct costs by a factor of ten – equivalent to £800m a year estimated in the UK¹⁵⁵ and more US\$9bn in Europe in 2015.¹⁵⁶ In the UK and India the primary focus of copper theft has been railway lines and electrical infrastructure, respectively. In the UK the theft of copper cables has cost Network Rail £43 million in three years, with a wider cost to the UK economy of an estimated £770 million a year.

While it is hard to quantify in hard terms the impact of bribery and corruption on the construction industry, estimates of 20–30 per cent of project value lost through corruption are widespread and sobering.¹⁵⁷ “This means that by 2030, unless measures are introduced that effectively improve this situation, close to \$6 trillion could be lost annually through corruption, mismanagement and inefficiency”¹⁵⁸ The impact of this kind of financial loss on projects, particularly in the developing world, highlights the degree to which crime can inhibit progress in the Global South.

“...building companies... gave around 2.5% of “won” government contracts to friendly governmental officials and to the Mafia, who orchestrated many of these deals”¹⁵⁹

It is similarly hard to separate the financial cost of racketeering to construction companies from the overall cost of corruption. However the social cost is clear – sub standard and inexperienced workers have more accidents, facilitate more theft and are more likely to suffer or cause situations leading to injury and death than regular employees.

Research into the scale of money laundering through Real Estate schemes varies globally, but is universally significant. The estimated amount of money laundered globally in one year is 2 - 5% of global GDP, or \$800 billion - \$2 trillion in current US dollars. Though the margin between those figures is huge, even the lower estimate underlines the seriousness of the problem governments have pledged to address. Calculating the amount of money laundered through real estate is hard, not least because ensuring it is not double counted with the financial sector is impossible. However to give an idea of scale, it is estimated the £180m of suspicious property transactions investigated between 2004 and 2016 in London represented less than 1% of the true amount of laundered money, suggesting £18bn over the period, or 2% of all London properties traded.¹⁶⁰ Extrapolating this, the total amount laundered through real estate worldwide in 2015 could be estimated at £15bn.¹⁶¹

153 Plant Theft costing UK Construction Industry over £800 Million a Year. Construction National. <http://www.constructionnational.co.uk/security/1953-plant-theft-costing-uk-construction-industry-over-p800-million-a-year>

154 Crime in the construction industry, CIOB, 2007

155 Allianz Cornhill in December 2016

156 European Confederation of Equipment Distributors, Theft of Construction Plant & Equipment, International Association of Engineering Insurers (IMIA), May 2005

157 Corruption and collusion in construction: a view from the industry, Engineers Against Poverty, 2014 (Also source below)

158 Executive Director, CoST International Secretariat, WEFForum, February 2016

159 5 Shocking Commercial Construction Fraud Stories. Rachel Burger. Construction Management. 6 January, 2016. Republished by Capterra Construction Management Blog <http://blog.capterra.com/construction-fraud-stories/>

160 Based on London transaction values from 2004 – 2015, HMRC Annual UK Property Transaction Statistics, 2016

161 Based on total property sales of £723bn, Savills, 2016





- The Global Illicit Financial Flows Report estimates that China, Russia and India are the top three countries receiving ill-gotten money moving out of the US Chinese nationals form the largest group of foreign buyers of Australian real estate, with nearly \$6 billion in 2013. Indians and Russians are among the largest non-Arab investors of real estate in Dubai. Between 2012 to 2014, Indians alone invested more than 44 billion dirhams in the Dubai real estate market (more than US\$12 billion).¹⁶²
- £100 billion is laundered through the UK each year.¹⁶³
- £180 million of property in the UK is investigated for proceeds of corruption since 2004, estimated to be 1% of the total.¹⁶⁴

How is the industry legally regulated to combat organized crime? What is the effectiveness of this regulation when compared to the costs? What examples or case studies exist of positive co-operation and remediation of organized crime in the public and private sectors?

Scattered regulation globally is making some headway in addressing trafficking and racketeering in the construction sector, though it is close to impossible to determine the impact of regulation, which in many cases is only 24 to 36 months old. In summary, while the intention to address trafficking and slavery in supply chains, including those in the construction industry, is clearly present it is ‘too soon to tell’ if it is having an impact.

Since 2015 elements of legislation are taking effect around the world that will force larger companies to be more accountable for their supply chains and for the presence of trafficking and slavery victims within their workforces. As these laws will force organisations to take responsibility for human-rights issues both at home and abroad, their influence is expected to increase and to become far-reaching over the longer term. However to date it has been patchy and largely ineffective.

The California Transparency in Supply Chains Act 2010, which came into effect in January 2012, requires certain companies to report on their specific actions to eradicate slavery and human trafficking in their supply chains. A review¹⁶⁵ conducted in 2015 found that 47% of companies that had responded to the requirements of the Act had not met the reporting requirements. As the identities of companies covered under the Act have not been published research, has not been able to determine how many have simply not reported anything at all. To date there have been no prosecutions under this Act .

There have been some examples of success in at least quantifying the problem. The UK Modern Slavery Act of 2015, which received Royal Assent in March 2015, covers slavery, servitude, forced or compulsory labour and human trafficking, and is expected

.....
 162 Global Illicit Financial Flows Report, Global Integrity, 2015
 163 Home Affairs Select Committee, Independent, July 2016
 164 UNODC, Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crimes, Oct 2011
 165 Five Years of the California Transparency in Supply Chains Act, Know The Chain, September 30th 2015





to have a particular focus on the construction sector due the type and level of staffing and company relationships.¹⁶⁶ Similar to the Bribery Act of 2010, it will apply to all large businesses carrying out business in the UK, including partnerships and companies registered overseas, and their worldwide operations. A one-year review conducted in July 2016 suggested there was a 40% increase in modern slavery victims identified in 2015, compared to 2014 (across all sectors).¹⁶⁷

Unlike trafficking, there has been no regulation suggested or enacted to challenge plant theft, arguably the most material TOC-related issue for the construction industry. The most successful efforts globally to combat plant theft have focused on improving the 'traceability' of stolen items and have been created by private-sector companies and industry bodies. Under a joint initiative announced by the Construction & Mining Equipment Industry Group and the Civil Contractors Federation in mid 2008, the two organisations joined forces in a programme to have all new and much existing equipment marked with a whole-of-vehicle-marking microdot spray application, known as DataDotDNA. Police throughout the world have around-the-clock access to this database.

"Adoption of the DataDotDNA initiative by a significant proportion of the industry's importers and wholesalers was seen as being a major positive step in the right direction," – Ray Carroll, Executive Director of the National Motor Theft Reduction Council (NMVTRC).

A similar initiative in the UK to mark copper cabling used in infrastructure construction with Smart Water launched in 2010 has yielded positive results in both tracing stolen cable, but more importantly, deterring theft in the first place.

The UK Bribery Act 2010 has been one of the more material pieces of legislation impacting bribery and corruption in the construction sector, not least because it explicitly includes provisions covering corrupt activity conducted outside the UK, but it took six years to secure its first conviction, which was, unsurprisingly, in the construction industry.

"The Serious Fraud Office has successfully secured its first conviction under section 7 of the UK Bribery Act 2010. On 19 February 2016, Sweett Group PLC, a UK-based construction and professional services company, was convicted for the offence of failing to prevent its subsidiary Cyril Sweet International from paying bribes on its behalf. The unlawful conduct took place over a three-year period from 2012 to 2015 in the United Arab Emirates."¹⁶⁸

In other countries, national investigations have had greater impact, at least in terms of the number of prosecutions and convictions. The Charbonneau Commission in Montreal, set up to investigate corruption in the Montreal construction sector, found that 'the corruption spread up to the highest level of government. The scandal goes back fifteen years, starting with contractors bribing city officials for contracts.'¹⁶⁹ Since its publication in 2015 the Mayors of Laval and Montreal have resigned, as has the interim Mayor of Montreal. All three have been arrested and charged with multiple counts of criminal activity. An addition 30 people

166 Construction legislation update: Modern Slavery Act 2015, Eversheds Sutherland, January 2016

167 The Modern Slavery Act Review, July 31st, 2016

168 First Ever Corporate Conviction Under The UK Bribery Act. Robert Starr. Walker Morris. 5 May 2016 <https://www.walkermorris.co.uk/publications/brief-walker-morris-legal-update-may-2016/first-ever-corporate-conviction-uk-bribery-act/>

169 The Mafia takes over Montreal's Buildings <http://blog.capterra.com/construction-fraud-stories/>





in Laval province alone have also been charged with corruption and other offences as a result of the four year investigation.¹⁷⁰

Similarly, in terms of money laundering, regulation is fragmented and often unfocused. In the UK money laundering in the financial sector is governed by the National Crime Agency, while money laundering in real estate is policed by HMRC, perhaps explaining why in 2015, 83.4% of SARs related to money laundering were submitted by banks and 0.09% by estate agents.¹⁷¹

Greater success has arguably been seen where regulation has been used, albeit often indirectly. The house price bubble in Vancouver had seen house prices rise meteorically – a benchmark detached house increasing in value by 38.7% during 2015 alone.¹⁷² It is widely accepted that this has been driven by buyers from mainland China entering the market, and there has been strong suggestion that this includes a significant proportion of money laundering activity

“An in-depth review of Canada’s anti-money-laundering efforts has uncovered serious concerns that organized crime is using the country’s hot real estate sector to illegally funnel cash. The report¹⁷³ makes special note of real estate as an area of the economy with a high risk of illicit activity, one of a few weak spots in what the report calls a comprehensive federal regime to combat money laundering and terrorist financing.” – FATF 2016

Measures introduced in August 2015 tax overseas buyers 15% on top of the value of the property being purchased successfully took the heat out of the market – average detached house prices fell 20% during September 2015, but are also believed to have had a marked impact on money laundering activity (though this is now believed to have been diverted to Seattle and Toronto rather than eradicated).

170 The Charbonneau Commission’s Underappreciated Contributions to Fighting Corruption in Quebec. Daniel Binette. The Global Anticorruption Blog. 15 January, 2016 <https://globalanticorruptionblog.com/2016/01/15/the-charbonneau-com-missions-underappreciated-contributions-to-fighting-corruption-in-quebec/>

171 Suspicious Activity Reports (SARs) Annual Report 2015, National Crime Agency

172 Greater Vancouver Real Estate Board, 2016

173 Canada’s Measures to Combat Money Laundering and Terrorist Financing, FATF 2016





Industry: Transport and Logistics

How does this industry break down into segment? What are the size, scale and geographic spread of each segment?

The transport and logistics sector is a wide-ranging industry covering the transportation of goods or people from one place to another. The transportation sector is made up of airlines, railroads and trucking companies and is a sub-sector of logistics, the general management of how resources are acquired, stored and transported to their final destination. The illicit movement of people, particularly those being trafficked, is widely covered in research and literature; this paper will focus on the movement of goods and the associated activity by TOC groups.

In our increasingly global lives the import and export of consumer goods, the movement of natural resources and fuels from source to plant and the trends for components to be manufactured in an entirely different country to the end product means logistics and transport of goods is a burgeoning sector.

Around 90% of world trade is carried by the international shipping industry. There are over 50,000 merchant ships trading internationally, transporting every kind of cargo.¹⁷⁴ The remaining 10% of goods traded splits roughly three-quarters by road, 20% rail and c.7% inland waterways in Europe.¹⁷⁵¹⁷⁶ In the US, with its larger landmass, the 10% of non-maritime shipment is split broadly 50% by rail and 38% by road,¹⁷⁷ the remainder by domestic air and other means. The role of air transport, both international and domestic, is a small proportion of freight transport. Air cargo represents no more than 0.5 per cent of the weight of all international cargo, and around 30 percent of the total global shipment value.¹⁷⁸

Cargo and freight transport splits between slow and cost-effective for heavy, bulky goods – primarily transported by sea and road, fast and expensive for high-value and time-critical goods – by air, and high-volume, smaller parcels by post and fast parcel ‘courier’ companies.

What types of organized crime feature in this industry? Which geographies and segments are most affected?

‘Asset appropriation’ or, theft, is the dominant crime against this sector, and is increasingly perpetrated by sophisticated TOC

174 Shipping and World Trade. International Chamber of Shipping. Accessed November, 2017 <http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade>

175 Freight transport statistics. Statistics Explained. Eurostat. 17 May 2017. Accessed November, 2017 http://ec.europa.eu/eurostat/statistics-explained/index.php/Freight_transport_statistics

176 Rail freight transport. Wikipedia. Accessed November, 2017 https://en.wikipedia.org/wiki/Rail_freight_transport

177 Freight Rail Overview. Federal Railroad Administration. U.S. Department of Transportation. Accessed November, 2017 <https://www.fra.dot.gov/Page/P0362>

178 Top Freight Airlines. Freight Filter. Accessed November, 2017 <http://freightfilter.com/top-freight-airlines/>





groups. While maritime freight dominates total volumes of cargo moved, it is a relatively safe method of transport. Globally, over 85% of all major cargo thefts occur during road transportation.¹⁷⁹

“Cargo is any commercial shipment moving via trucks, planes, rail cars, ships, etc., from point of origin to final destination. If merchandise is stolen at any point in between—highway, truck stop, storage facility, warehouse, terminal, wharf, etc.—then it’s considered cargo theft”¹⁸⁰ – FBI 2016

The largest impact is on the industry due to criminal activity – approaching two-thirds of all reported crimes - is the loss of cargo, though on occasion the truck and / or trailer can also be lost, around 13% of all crimes. This however is less common, and in many cases where the truck or trailer are lost they are found again undamaged once the cargo has been removed.¹⁸¹

“Stolen cargoes have a higher value than the trucks carrying them and this accounts for the fact that 70% of the stolen vehicles are found still intact” – TAPA Report on Freight Crime in Saudi Arabia, 2015

The days of ‘highway robbery’ are fading: 59% of all road transport losses in the US are suffered while the goods are stationary – in distribution centres (23%), and parking lots, truck stops and unsecured yards. On road hijacking happens, but is still relatively rare. In EMEA on road hijacking accounts for less than 2% of all road cargo-related crime.¹⁸² However, hijacking does still occur, and when it does is increasingly ruthless. Organized criminals target what they regard as vulnerable cargo loads as they move on roads in all parts of the world. In one of the most recent incidents a truck driver in the Philippines lost his life in a violent theft-driven attack.¹⁸³

“The world of cargo crime is no longer about an opportunist individual snatching a product from a box in a warehouse. Today, we are dealing with gangs of organized criminals that are often armed and prepared to go to any lengths as we saw as recently as September with the murder of a driver during a hijack of his vehicle in the Philippines. Vehicles are attacked whilst being parked up overnight, at motorway service stations and even while moving and, in some countries, this may start with truck drivers being stopped by what turn out to be authentic-looking but bogus law enforcement officers.”¹⁸⁴

Technology is advancing every aspect of business today, and this applies as much to transport and logistics as any other sector. Fraud, or ‘fictitious pickups’ are becoming increasingly common. Old-fashioned cargo theft, physically breaking into a trailer, container or warehouse, has declined, as thieves are becoming more technologically aware.

“Fictitious pickups” in which a criminal steals a carrier’s identity to then bid for carrier jobs on brokerage websites and simply drive off with the cargo and trailer are increasingly popular. Fictitious pickups accounted for 12 percent of all cargo theft losses

179 TAPA

180 Inside Cargo Theft. A Growing, Multi-Billion-Dollar Problem. Federal Bureau of Investigation (FBI). 2010
https://archives.fbi.gov/archives/news/stories/2010/november/cargo_111210/cargo_111210

181 TAPA 2016

182 US cargo thefts rise 7 percent; Memorial Day could see spike. The Journal of Commerce (JOC). 2015
http://www.joc.com/trucking-logistics/us-cargo-thefts-rise-7-percent-memorial-day-could-see-spike_20150515.html

183 TAPA

184 Ibid





in the last quarter. From 2011 through 2013, cargo theft by fictitious pickup spiked by 70 percent, climbing from 59 reported incidents to 101 losses.¹⁸⁵

We're moving from straight-out cargo theft and pilferage to cyber crime. That's the next generation, and what we'll be dealing with over the next 10 years" – Keith Lewis, vice president of operations at CargoNet

Alongside crimes that directly profit from targeting the transport and logistics sector are those that use the sector to further the aims of TOC groups – in this case the inappropriate use of transport and logistics companies to move illicit goods and persons, usually without the knowledge of the company in question. Often the additional security measures involved in using a third-party transport company rather than smuggling on person or in private vehicles act as a deterrent but it is still a frequent route, particularly for small, high-value packages.

CASE STUDY

"One of the M.O.'s that's on the increase is in a sense identity theft—impersonating another company. The tactic is known as a fictitious pickup. It starts with loadboards—websites like Dat.com and Truckstop.com where shipping brokers list loads in need of delivery. Though the contents of those loads aren't listed, canny thieves can spot the valuable ones based on certain details: Loads requiring high insurance minimums, loads requiring a team of drivers, or loads coming out of particular locales, such as technology corridors. Then, using falsified credentials to pose as legitimate truckers, criminals contract to carry the load, drive their own truck to a warehouse or distribution center, and simply pick it up. It can be days before cargo owners even know they've been robbed." Nick Erdmann, Transport Security, 2015

A 2015 survey¹⁸⁶ by the FATF suggested that 42% of cash smuggled across borders for money laundering purposes was carried hidden in cargo, breaking down 19% in mail and fast parcel sectors and 14% in air cargo. The remainder was split 5% in maritime/containerized cargo and 5% in 'other' cargo.

Like cash the easy portability of drugs shipments has made mail and fast parcel shipping services popular methods for transportation.

"The sheer mass of letters and packages being transported through USPS, Fed Ex, UPS and others gives the drug traffickers a certain level of protection because not every package can be inspected. They choose rush delivery options to further decrease the chances of detection because the pressure to deliver on time reduces the risk of time-consuming package checks"

185 US cargo thefts rise 7 percent; Memorial Day could see spike. The Journal of Commerce (JOC). 2015 http://www.joc.com/trucking-logistics/us-cargo-thefts-rise-7-percent-memorial-day-could-see-spike_20150515.html

186 FATF, Cash Money Laundering, 2015





– American Addiction Centers, 2017¹⁸⁷

Although interviews suggested that fast parcel companies were aware of the risk of their services being used for illegal shipments they were more concerned about the risk of dangerous, than illicit, cargo. Whether by air, sea or land, drug cartels slip their illicit drugs into the US with the constant stream of legitimate cargo entering the country legally. From disguising them among produce to hiding them inside dog food bags, the traffickers have an endless supply of imports to choose from.

“Traffickers often hide drugs among legitimate cargo in maritime containers, a fraction of which are inspected. Analysis of commercial maritime seizure data for 2004 through 2009 indicates that cocaine and marijuana are most often smuggled in commercial maritime vessels from Caribbean locations, such as the Dominican Republic, Haiti, and Jamaica, into East Coast ports in Florida and New Jersey.”

UK research suggests that heroin trafficked via Pakistan to the UK is most often sent directly by parcel, air courier or maritime container; or to have been trafficked by sea into eastern or southern Africa for onward movement. Traditionally, most of the cocaine destined for Europe, including the UK, has crossed the Atlantic by ship and entered via Spain. The most significant method currently used to smuggle bulk amounts is in maritime container ships arriving in European hub ports, such as Antwerp and Rotterdam, before being moved into the UK. The use of other maritime methods, such as yachts, general cargo vessels, air couriers and cargo, are also significant.¹⁸⁸

When the dark web market site Silk Road was brought down in 2013 the degree to which it used legitimate mail services, most commonly the US Postal Service, to facilitate the final consumer transaction was revealed. Delivering 2 billion pieces of mail annually meant that the chances of a package being opened were small, and the fact that letters and parcels can be posted anonymously in any one of millions of postboxes further decreased the chance of the seller being caught.

Conversely, for high bulk, heavy shipments, such as ivory and illegal wildlife movements, maritime shipping takes precedence.

Since 2009, nearly two-thirds of the large ivory seizures by number, and three-quarters by weight, have transpired as containerized shipping through seaports. Container shipping represents the most cost-effective transport option for moving a heavy commodity and the risk of detection is relatively low.¹⁸⁹

Attempting to transport illicit and illegal goods through legitimate cargo carriers is the predominant use of the industry by TOC groups and is discussed in detail above. However over the last twelve to eighteen months the use of commercial transport vehicles in acts of terrorism has become more visible. Heavy commercial vehicle theft has increasingly been in the spotlight since the Berlin Christmas market attack in December 2016. This attack highlighted how easy it is to steal a semi-truck and cause mass

187 United States Drug Enforcement Administration – Drug Movement Into and Within the United States February 2010 <http://www.justice.gov/ndic/pubs38/38661/movement.htm>

188 National Crime Agency, 2017

189 <http://www.traffic.org/storage/W-TRAPS-Elephant-Rhino-report.pdf>, quoted in Transportation in Illegal Wildlife, Criminal and civil liability in the transportation chain, DLA Piper, 2015





casualties.¹⁹⁰

What is our estimate of the direct financial impact on this industry, by segment and by crime type? What are the implications?

Cargo crime is one of the biggest supply-chain challenges for manufacturers of high-value, high-risk products and their logistics service providers.¹⁹¹

Industry experts estimate cargo thefts cost as much as \$30 billion in losses each year worldwide, with \$10bn a year in the US alone and \$8.2bn in EMEA. Cargo theft has many victims, from employees (i.e., drivers, warehouse workers) who can be hurt during an armed hijacking or robbery, to retailers who lose merchandise, to consumers who pay as much as 20 percent more to make up for cargo theft, to state and local governments who lose sales tax revenue and to insurance companies, manufacturers, and shipping companies. This estimate may well be conservative as many companies don't report cargo crimes (to avoid bad publicity, higher insurance rates, damage to reputation, embarrassment, etc.). The exact financial losses aren't known.¹⁹²

Theft takes place across the full range of cargo types. Any product being shipped is potentially a target, but cigarettes, pharmaceuticals, and especially computer/electronic components, are current high-value favourites being re-sold on the black market.¹⁹³ Food and beverage products, although having lower value per item, are also popular as they are untraceable – once they have been stolen there is no way of tracking them or identifying the stolen goods if found.

“Products with a low unit value are just as attractive to cargo thieves – often organized criminal gangs – because of the high volumes they move in. And, these products are often easier to dispose of and less traceable.” – TAPA 2016

In 2016, analysts recorded 623 stolen tractors and 732 stolen trailers in the U.S. and Canada. Tractor thefts are up 8 percent year-over-year, and trailer thefts are up 4 percent year-over-year. CargoNet recorded \$114m in stolen cargo across 554 cargo theft incidents — for an average loss value of \$206,836.97. Apply this average to the events with a missing value, and the loss value would equal \$172.9m.¹⁹⁴

As discussed, maritime losses while at sea are relatively low: overall annual losses as a result of piracy are estimated to be 0.001 to 0.002 per cent of the total cargo value involved.¹⁹⁵ Oceans Beyond Piracy estimates the direct cost of piracy to be around

190 CargoNet SupplyChainBrain

191 TAPA

192 TAPA

193 Inside Cargo Theft. A Growing, Multi-Billion-Dollar Problem. Federal Bureau of Investigation (FBI). 2010 https://archives.fbi.gov/archives/news/stories/2010/november/cargo_111210/cargo_111210

194 CargoNet SupplyChainBrain

195 Obstacles to global shipping: Piracy and terrorism. World Ocean Review. 2010 <http://worldoceanreview.com/en/wor-1/transport/piracy-and-terrorism/>





\$148m in ransoms, with further costs in insurance premiums and re-routing of ships of up to \$6bn.¹⁹⁶

How is the industry legally regulated to combat organized crime? What is the effectiveness of this regulation when compared to the costs? What examples or case studies exist of positive co-operation and remediation of organized crime in the public and the private sector?

Legislation specifically applying to cargo transport and protection is limited. There have been examples of regulation and legislation having an impact – in the US state of Georgia for example a new statute, the GA Cargo Theft Statute, changed the relevant legislation from ‘receiving stolen property’ to a specific cargo related crime with penalties of up to 30 years in prison and fines of \$1m. Georgia was previously a state that experienced a particularly high rate of cargo theft, but, since the new statute was introduced, reported cargo theft fell by 64 per cent.¹⁹⁷ However regulation like this is rare.

Far more effective and far-reaching has been the standards set by global trade organisations. TAPA, a network of 600 transport companies, has set global security standards to protect high-value consumer goods traveling on international roads including the Trucking Security Requirements (TSR) which is updated every year.¹⁹⁸ TSR has proven to be extremely effective for TAPA members in helping to eradicate what is a growing problem for manufacturers and global supply chain service providers. The Association previously took similar action in 2001 when it launched its original Freight Security Requirements (FSR) to protect warehouse operations from attacks by criminals. Today, FSR is recognized as the world’s leading standard for securing freight centres. Having significantly reduced incidents involving warehouses, TAPA has since seen a dramatic increase in road-based crime, which has driven the need for the TSR standards.¹⁹⁹

“The new and enhanced TAPA Truck Security Requirements, which includes mandatory certification, supports the users and providers of trucking services, providing a common standard of security measures and taking into account the different ways these services are provided globally. When adopted, TSR is a mandatory standard and adherence to it is validated and auditable by a TAPA-approved and trained independent auditor. We believe that TSR certification will result in TAPA members globally seeing a continued reduction in crime involving vehicles, similar to the significant decline in losses from warehouse attacks witnessed by members that have FSR certified facilities”.²⁰⁰

Research shows that TAPA members, when supported by TAPA security standards, incur significantly lower theft loss levels than the industry average. Through participation in TAPA and the many opportunities for sharing crime intelligence, training, networking and its close co-operation with regulatory bodies and international law enforcement agencies, TAPA members learn to identify and understand security risks and how they can best be mitigated. TAPA’s 2010 Financial Benchmark report indicates that

196 Oceans Beyond Piracy.org

197 CargoNet SupplyChainBrain

198 TAPA

199 Ibid.

200 Ibid.





losses incurred by non-members are three times higher than for TAPA members. – TAPA 2016.²⁰¹

Although cargo companies are still used for the bulk shipment of illegal drugs, the regulatory network has acted as a deterrent for TOC groups seeking to distribute drugs via fast parcel services to the end consumer. Using the postal service in the US gives buyers and sellers several levels of protection from detection and prosecution - the US Postal Service must have a warrant to open your mail. Private couriers like UPS and FEDEX do not and while they also handle very high volumes they can open a suspicious package without requiring a warrant or legal permission. Furthermore, the US Postal Service, as a federal government agency, may only be policed by its own postal inspectors, the Drug Enforcement Administration (DEA), FBI etc. can police commercial shipments. From a buyers point of view, receiving a parcel in the mail has deniability, signing for a courier parcel confirms receipt and therefore makes it materially harder to claim innocence or ignorance. This has made fast courier services much less attractive than the postal service for drug transactions.

The law is complicated when it comes to apportioning liability for the unknowing carriage of illicit and contraband goods. International conventions such as CITES require the carrier to 'knowingly or recklessly make a statement' for the purpose of either obtaining a permit or making an import notification and where import/export and courier companies have been prosecuted under these laws they have tended to be companies owned and run by TOC groups, rather than third-party businesses.²⁰²

Customs and Excise Laws, including the Customs and Excise Management Act 1979 in the UK and the EU Customs Code, make those carrying illicit goods liable, but again prosecutions of third party carriers who cannot be shown to be complicit in the crime are extremely few and far between.

Liability for the movement of cargo where there are multiple links in the chain becomes even murkier. A chain of multiple parties, particularly in air or maritime freight management – the cargo owner, shipper, freight forwarder, carrier and so on will have many layers of indemnification between the various groups. Few shippers are large enough to fill a whole cargo ship or plane on their own and so a shipper will subcontract their duties to a freight forwarding company to deliver the goods to the consignee/importer.

Usually the shipper will be required to indemnify the freight forwarder from any risk or penalty involved in transporting the goods in question. Similarly, the shipper will be required to contract with the carrier that the goods are not illegal or dangerous - under the current civil liability regime, carriers, like freight forwarders, will usually operate on their own standard terms and conditions which place liabilities and responsibilities for the mis-description of goods on the shippers.²⁰³ An extract from the Maersk Line Standard Form Bill of Lading (Clause 14.3) makes this very clear:

“The Shipper warrants to the Carrier that the particulars relating to the Goods as set out on the reverse hereof have been checked by the Shipper on receipt of this bill of lading and that such particulars, and any other particulars furnished by or on behalf of the Shipper, are adequate and correct. The Shipper also warrants that the Goods are lawful goods, and contain no

201 Ibid.

202 In Cold Blood, Combatting Organized Wildlife Crime, EIA 2014

203 Transportation In Illegal Wildlife - Criminal And Civil Liability In The Transportation Chain, 2015





contraband, drugs or other illegal substances or stowaways, and that the Goods will not cause loss, damage or expense to the Carrier, or to any other cargo.”

Clauses 15.2 and 15.3: “The Merchant shall be liable for and shall indemnify the Carrier against all loss, damage, delay, fines, attorney fees and/or expenses arising from any breach of any of the warranties in clause 14.3 or elsewhere in this bill of lading and from any other cause whatsoever in connection with the Goods for which the Carrier is not responsible.

The Merchant shall comply with all regulations or requirements of customs, port and other authorities, and shall bear and pay all duties, taxes, fines, imposts, expenses or losses (including, without prejudice to the generality of the foregoing Freight for any additional Carriage undertaken) incurred or suffered by reason of any failure to so comply, or by reason of any illegal, incorrect or insufficient declaration, marking, numbering or addressing of the Goods, and shall indemnify the Carrier in respect thereof.”

Even where a third party carrier is solely responsible for the transport of illegal goods, proving liability has been extremely difficult and largely unsuccessful. The US Federal Government attempt in 2016 to prosecute FedEx for drug trafficking and money laundering for shipping pharmaceuticals sold illegally by online pharmacies was seen as a landmark case for third party carriers worldwide. Prosecutors charged FedEx with 15 counts related to trafficking controlled substances and misbranded drugs in July 2014, later adding three counts of conspiracy to launder money. After nearly two years of hearings and delays all charges were dropped against FedEx, on the grounds both that FedEx employees had actively and willingly sought to assist in the investigation into the illicit pharmaceuticals and that FedEx could not have been deemed to have had ‘knowledge’ of the legal status of the cargo being carried.²⁰⁴





Industry: Natural Resources

How does this industry break down into segment?

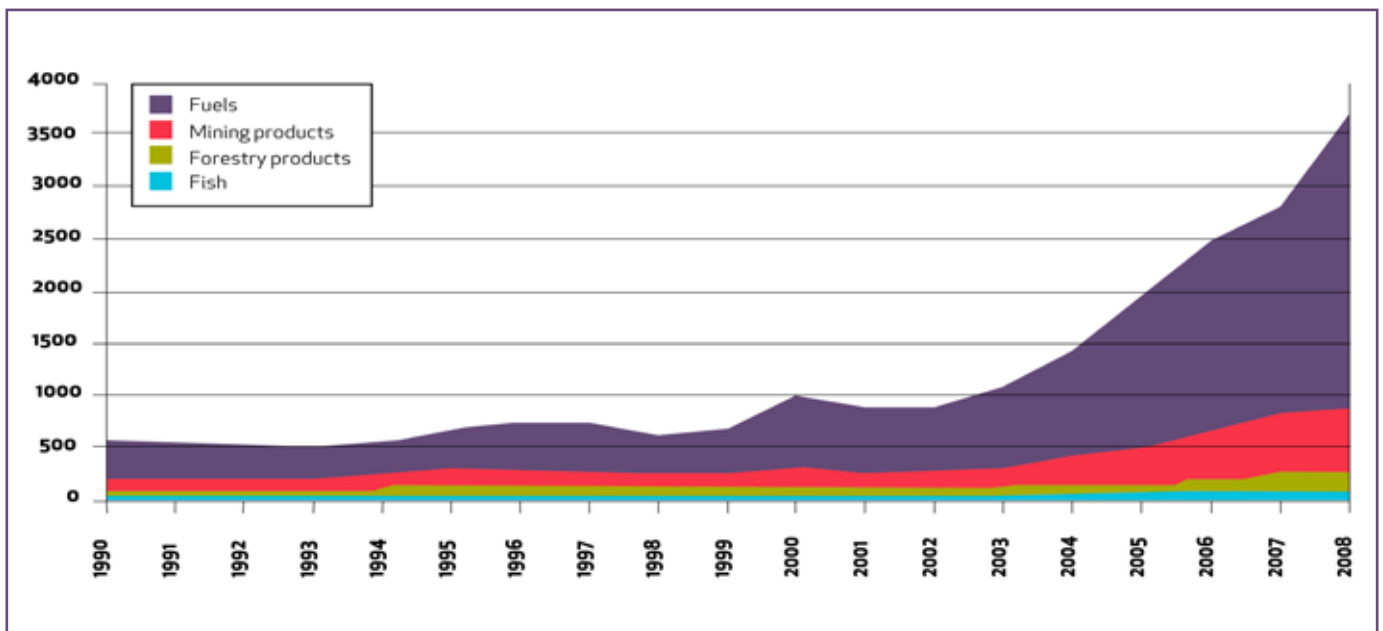
What are the size, scale and geographic spread of each segment?

Given the focus of organized crime, for our purposes, we have defined natural resources as oil and gas, and mining & minerals.

The oil and gas industry includes the global processes of exploration, extraction, refining, transporting and marketing of oil and gas products. The largest volume products of the industry are fuel oil and gasoline. Oil is also the raw material for many chemical products, including pharmaceuticals, solvents, fertilizers, pesticides, synthetic fragrances, and plastics. The industry is usually divided into three major components: upstream, midstream and downstream. Midstream operations are usually included in the downstream category. With reserves of 1,258 billion barrels,²⁰⁵ the global oil industry is thought to be worth c.\$1.2 trillion.²⁰⁶ The world consumes 30 billion barrels (4.8 km³) of oil per year, with developed nations being the largest consumers. The United States consumed 25% of the oil produced in 2007.²⁰⁷

Oil accounts for a large percentage of the world's energy consumption, ranging from a low of 32% for Europe and Asia, to a high of 53% for the Middle East (South and Central America (44%), Africa (41%), and North America (40%)).

Figure 9: World Natural Resources Exports by product, 1990-2008 (\$ billion)



205 WTO Trade Report, Natural Resources

206 World oil and gas industry revenue from 2009 to 2013 (in million U.S. dollars). Statista. Accessed November, 2017 <https://www.statista.com/statistics/215892/revenues-of-the-world-gas-and-oil-industry/>

207 The World Factbook". Country Comparison - Oil Consumption. Found at <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2174rank.html>



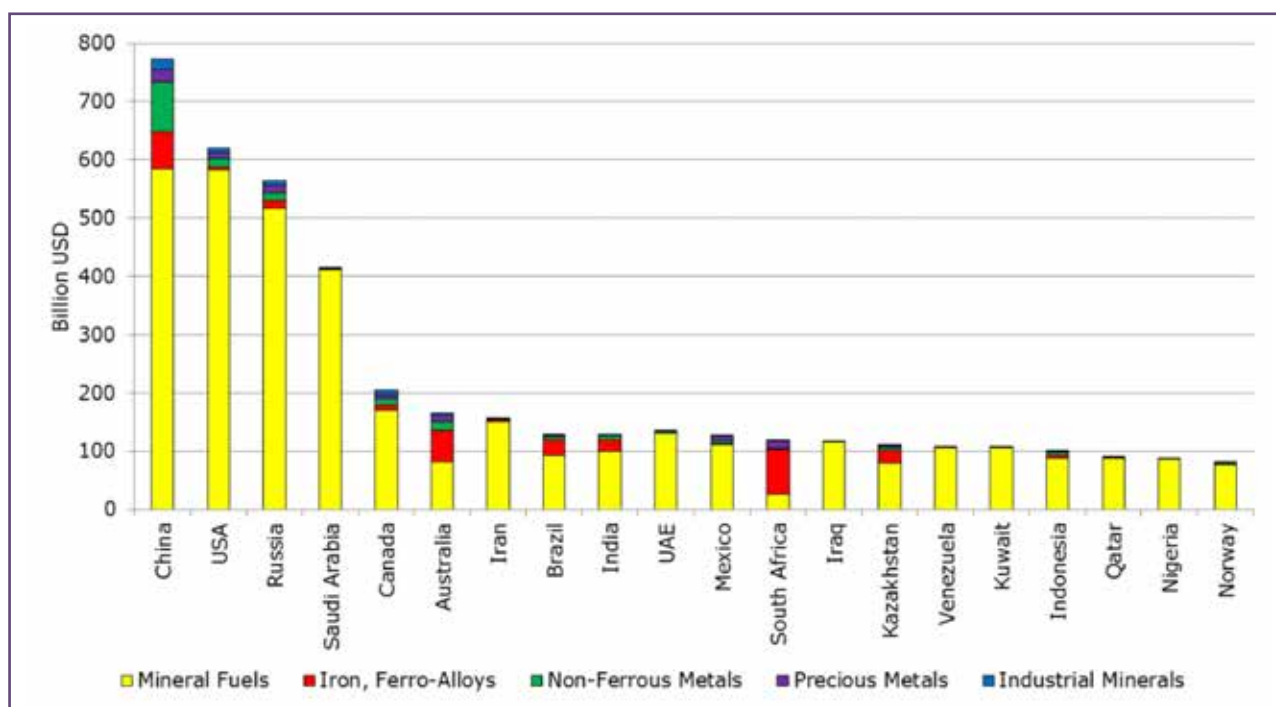


Oil companies used to be classified by sales as “supermajors” (BP, Chevron, ExxonMobil, ConocoPhillips, Shell, Eni and Total S.A.), “majors”, and “independents” or “jobbers”. In recent years, however, national oil companies (NOCs, as opposed to IOCs, international oil companies) have come to control the rights over the largest oil reserves; by this measure the top ten companies all are NOC.

Mining is the extraction of valuable minerals or other geological materials from the earth, usually from an orebody, lode, vein, seam, reef or placer deposits. Ores recovered by mining include metals, coal, oil shale, gemstones, limestone, chalk, dimension stone, rock salt, potash, gravel and clay. Mining exists in many countries. London is known as the capital of global “mining houses” such as Rio Tinto Group, BHP Billiton, and Anglo American PLC. The top miners’ revenues totaled \$435 billion in 2010. The mineral industry of Africa includes the mining of various minerals; it produces relatively little of the industrial metals copper, lead, and zinc, but has 40% of the world’s gold, 60% of cobalt, and 90% of platinum group metals.

For rare earth minerals mining, China reportedly controlled 95% of production in 2013.

Figure 10: 20 largest mineral-producing countries 2014 (without construction minerals, in M. metric.t)



Organized crime often focuses on, but is not limited to, precious minerals, such as diamonds. A review of sub-Saharan African countries in the early 2000s indicated that diamond mining often represented some 10 percent of national GDP and in several cases about 50 percent or more of total exports. In Thailand gem and jewellery exports were worth US\$12 billion in 2011 and accounted for more than 5 percent of the country’s total export earnings.

Gold is equally significant. It represented 7% and 16% of GDP in Tanzania and Mali, respectively in 2010. The African continent is responsible for 21% of world production and is estimated to have 60% of the world’s gold resources. In South America, gold has





recently overtaken sugar as Guyana's top export, generating over US\$1 billion in revenue. The global gold industry, measured in gross-value added revenue terms, is \$88.5 billion.²⁰⁸

What types of organized crime feature in this industry? Which geographies and segments are most affected?

The natural resources industry provides a rich source of criminal proceeds for TOC groups, and this is often underestimated, as Tim Boekhout van Solinge emphasises in his recent paper:

"The policy emphasis on conventional illegal goods such as illicit drugs draws attention away from these other, lesser known sources of illegal revenues. The case of the Taliban in Pakistan well exemplifies this neglect. While drugs are often assumed to be the main commodities funding this movement... timber, emeralds and other gemstones were for several years well into 2009 very important, if not the predominant, sources of income for this organization"²⁰⁹

It is no surprise that fraud, corruption and asset theft loom large as organized crimes in this domain. The 'resource curse' has a broader meaning when organized crime is taken into account. The term refers to the pattern of resource-rich developing countries performing poorly in terms of economic growth, inequality and human development. But in addition, these 'cursed' countries are more vulnerable to exploitation, theft and corruption.

One of the most significant crimes is, unsurprisingly, asset misappropriation and theft. There is a general economic theory that illicit trading is predominantly focused on high-value but easily transportable goods, such as technology, luxury goods and money. Yet, illicit trading is as rife in the oil industry as in conventional products, and has global reach and powerful TOC penetration.

Illicit and unrecorded crude oil trading occurs in several ways. Smuggling is the diversion or theft (usually of gasoline) unfettered to high-price markets. The incentives and opportunities for smuggling easily create a profitable enterprise, particularly with the rise in global energy prices over the last decade.

Mingling refers to the mixing of 'official' and 'unofficial' oil. In effect, criminals extract a quantity of crude oil beyond the amount licensed for the well head. With the acquiescence, connivance and facilitation of corrupt officials and others along the oil supply chain, they transport the oil to its destination. The illicit component is then sold on the black market. This practice is predominantly in Angola, Russia and Saudi Arabia and one gulf tanker captain suggested the profits of one trip were equal to the value of the tanker.

Bunkering refers to the direct theft of oil from ships and pipelines. Accordingly, bunkering is more complex than previously

208 Global direct and indirect gross value added (GVA) of the gold mining industry from 2000 to 2013. Statista. Accessed November, 2017. <https://www.statista.com/statistics/524149/global-direct-indirect-gva-gold-mining-industry/>

209 The Illegal Exploitation of Natural Resources, Tim Boekhout Van Solinge in The Oxford Handbook of Organized Crime





discussed processes: the risk of interdiction and the level of capability required to siphon oil from supply lines, mean that it tends to occur in a lower security environment. Accordingly, such operations are generally carried out by well-resourced organisations, such as insurgents in Iraq or Nigeria and drug cartels in Mexico.

According to a report published by Global Financial Integrity, unrecorded oil sales may amount to over 500,000 barrels a day, or 183 million barrels a year. With a 2012 mean price of \$93.75, this produces a black market for oil valued at over \$17 billion annually. However, it is worth noting that economic pessimism has recently depressed oil prices and these statistics could be significantly higher in a more positive financial environment.²¹⁰

As much as 400,000 barrels of oil a day are stolen in Nigeria. Experts estimate that \$400 billion of oil revenue has been stolen or misused since 1960. This equates to losses of US\$1.7 billion a month for Africa's largest economy, representing 7.7% of its GDP vanishing, or more than the country spends on education and healthcare. In Mexico, Pemex's Exploration and Production subsidiary admitted that fuel theft was growing at a rate of 30 per cent a year, for a total theft of 5,000 to 10,000 barrels per day. In Iraq oil smuggling was institutionalized in the days of Saddam Hussein; one U.S. Senate estimate is that the Ba'ath regime pocketed \$21.3 billion from the UN Food For Oil Program.

Gold is one of the most attractive substances to TOC groups, both from the view of outright theft and diversion, and trade-based money laundering. Crimes related to gold occur right along the supply chain, from the illegal sale of unrefined ore, through corruption and illegal mining (particularly artisanal), theft in the refining stage, and in the retailing and investment end of the chain.²¹¹

Although a global figure is difficult to derive, it is clear gold is outstripping 'traditional' drug markets in some areas: Colombia's drug cartels make \$1 to \$1.5 billion a year in wholesale proceeds from both heroin and cocaine, whereas illegally mined gold earned smugglers in the country between \$1.9 and \$2.6 billion a year. The story is similar in Peru: the value of illegal gold exports, approximately \$2.6 billion a year, now exceeds the value of country's cocaine trade—\$1 to 1.5 billion annually—by a wide margin.

But fraud, corruption and organized crime are not limited to asset misappropriation in these markets. In Kroll's fraud survey:

In addition to above-average levels of vendor or procurement fraud (23%), the [natural resources] industry has the second highest incidence of regulatory or compliance breach (17%) and of corruption (16%). The latter two help explain why the industry was in the last year by some margin the one most likely to be taken advantage of by criminal government officials, which occurred at 14% of firms which experienced a fraud and where the culprit was known. Although less extensive than the above crimes, the proportion of respondents from natural resources firms reporting misappropriation of funds (13%), money laundering (9%) and market collusion (4%) is the highest for any industry and, in each case, roughly double the average.²¹²

Corruption as a topic is so endemic in natural resources markets that it is difficult to identify 'clean' markets. As a major NGO in

210 The Threat of Organized Crime to the Oil Industry, Future Directions International, 29 November 2012

211 Money laundering/terrorist financing risks and vulnerabilities associated with gold, FATF, July 2015

212 Kroll, Global Fraud Report, 2015/16





the field of anti-corruption, Global Witness, comments:

Secrecy in this industry entrenches corruption and props up kleptocratic regimes.. Companies are complicit in this problem. By paying bribes and doing deals in secret, they distort markets and stop citizens from knowing the value of the wealth beneath their feet, or from reaping the benefits.²¹³

Cyber attacks on natural resources companies are significant. According to a study conducted by Dimensional Research in November 2015, 82% of oil and gas industry respondents said their organizations registered an increase in successful cyber-attacks over the past 12 months. Moreover, 53% of the respondents said that the rate of cyber-attacks has increased between 50 and 100 percent over the past month.²¹⁴ However, much of this activity is related to industrial espionage:

“A great deal of the cyber threat relates to state-sponsors attempting to gain secrets of upstream discoveries. We do suffer cyber fraud, but we’re more worried about the state sponsored efforts” – Oil industry security professional

Widely publicised attacks on SCADA systems have in turn been over-reported,

“We know of at least one case when a major leak event was reported as a cyber SCADA attack, when in fact it was a physical attack committed by insurgents that the government was trying to focus attention away from”.

– Oil industry security professional

Forced labour and human trafficking are also found in natural resources and allied industries. Of the 14.2 million trafficking victims exploited for labour, 7.1 million (50%) forced labour victims work in construction, manufacturing, mining or utilities.²¹⁵

The global AML process means that, in theory, AML procedures are in place in all of the nations under FATF’s purview. But, In reality procedures are relatively weak across many nations rich in natural resources, a good example being diamond trade-based money laundering:

“While cash is still commonly used in emerging and developing countries where diamonds are produced and traded, financial institutions such as banks are also involved in diamond trade in these countries. Accordingly, diamond dealers should be subjected to customer due diligence (CDD) procedures. However, the overall level of compliance of these countries with the FATF recommendations related to preventive measures for financial institutions is relatively low.”²¹⁶

.....
 213 Global Witness, 2017
 214 Tripwire 2016 Energy Survey: Oil and Gas
 215 Human Trafficking by the Numbers, Human Rights First, January 2016
 216 FATF Specific Risk Factors in Laundering the Proceeds of Corruption, FATF Report, 2012





What is our estimate of the direct financial impact on this industry, by segment and crime type? What are the implications?

At an aggregate level, the World Bank estimates a total 1.743% of world GDP is represented by natural resources.²¹⁷ Out of a total global GDP of \$74.152 trillion, this would mean that the total global value of natural resources is \$1.292 trillion. Using the Kroll survey's average percentage of revenue lost to fraud – in the case of natural resources a high 1%, this equates to \$12.92 billion.

How is the industry legally regulated to combat organized crime; what is the effectiveness of this regulation when compared to the costs? What examples or case studies exist of positive co-operation and remediation of organized crime in public and private sector?

Given the significant incidence of organized crime in resource-rich developing countries, the development community has rallied to produce several initiatives to combat TOC. In many ways, this makes it one of the most sophisticated sectors in terms of PPPs. But given the sheer scale of the problem, and the fragility of the states in which it occurs, progress has been slow.

In 2002 Global Witness co-founded the Publish What You Pay (PWYP) movement, which now includes over 800 organisations. PWYP campaigns to make companies declare the payments they make to governments in return for oil, gas and mining contracts. This enables citizens to ask whether their government has used the money going into state coffers wisely and fairly.

In 2014, the UK passed laws requiring companies to publish their payments for each of their projects, making it the first country to implement an EU-wide directive with the same objective. But in the US, the implementing rules for similar laws passed in 2010 are still being negotiated after being stalled by a group of oil companies intent on derailing them.

“Perhaps this area is avoided because it is ‘too political’. Before Wolfensohn’s ‘cancer of corruption’ speech, the IMF and World Bank shied away from engaging with corruption because it was ‘too political’. The thinking has since shifted, but it has not shifted far enough”.²¹⁸

“Another systemic approach to the resource curse has been advocated: distributing oil revenues directly, and equally, to all citizens in a producer country, then taxing them directly on their income. In Alaska and Alberta direct distribution of oil revenues is popular and successful. Could it possibly work in Africa?”.²¹⁹

In the rich literature around corruption and the resource curse, much is made of the Extractive Industries Transparency Initiative,

217 Total natural resources rents (% of GDP). World Bank. Accessed November, 2017 <http://data.worldbank.org/indicator/NY.GDP.TOTL.RT.ZS?end=2015&start=1997>

218 Nicholas Shaxson, *Poisoned Wells, and Oil, Corruption and the Resource Curse*, 2009

219 Ibid





EITI. Transparency and public accountability are core concepts in anticorruption policies. But in their study of EITI, Päivi Lujala and Levon Epremian challenge the assumption that increasing transparency and informing the public about natural-resource revenues will lead to more equitable revenue management.²²⁰

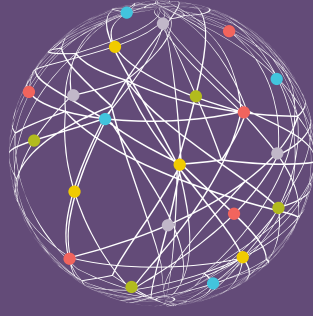
In one of the most cited countries in terms of natural resources and corruption, Nigeria, progress is being made. But the progress is piecemeal and the process has begun only very recently. One example is the Economic and Financial Crimes Commission (EFCC), the main anti-corruption institution in Nigeria:

The EFCC gained much influence and respect, especially under former commissioner Nuhu Ribadu, although the subsequent lack of substantial and visible success coupled with political wing-clipping under President Jonathan weakened the institution. Yet, knowledge (and condemnation) of corruption has intensified, and the EFCC has made important progress in recovering assets that are the proceeds of crime.²²¹

220 Corruption, Natural Resources and Development From Resource Curse to Political Ecology
Edited by Aled Williams and Philippe Le Billon, 27 January 2017

221 Nigeria: defying the resource curse - Inge Amundsen, in *ibid*





THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

www.globalinitiative.net



A NETWORK TO COUNTER NETWORKS