JUNE 2020

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

TRANSFORMATIVE TECHNOLOGIES

How digital is changing the landscape of organized crime

Lucia Bird | Thi Hoang | Julia Stanyard | Summer Walker | Simone Haysom

ACKNOWLEDGEMENTS

This paper incorporates inputs from a number of members of the Global Initiative Against Transnational Organized Crime. Thanks in particular to Prem Mahadevan for his invaluable review comments, and to the Global Initiative publications team.

ABOUT THE AUTHORS

Lucia Bird is a senior analyst at the GI-TOC. She researches and writes on a broad range of organized-crime types internationally, however her focus has been on human smuggling, human trafficking, drug trafficking and policy, and cybercrime.

Thi Hoang is an Analyst at the Global Initiative Against Transnational Organized Crime. She has been part of the Global Initiative team since February 2017. She is currently working on the Responsible & Ethical Business Coalition against Trafficking (RESPECT) Initiative, which serves as a platform for thought leaders, practitioners and policymakers, and to mobilize the business community as a strategic partner to tackle human trafficking.

Julia Stanyard joined the GI-TOC in October 2017 as an analyst and coordinator of the UNTOC-Watch Initiative. She graduated with a master's and bachelor's from Cambridge University. Her MPhil thesis was on the illicit antiquities trade and crime-prevention strategies taken to combat this trade, in comparison to other transnational criminal markets.

Summer Walker is a senior analyst and New York Representative at the GI-TOC. She has worked in New York and Berlin for international NGOs, development agencies and research institutes, and has published papers on drug policy, human trafficking, and organized crime. Prior to this, she worked at United Nations University in New York, running a drug policy project.

Simone Haysom is a senior analyst with the GI-TOC, with expertise in corruption and organized crime, and a decade of experience conducting qualitative fieldwork in challenging environments.

Cover photo: Reworked from kjpargeter/Freepik

Image credits: Markus Spiske/Unsplash; James Yarema/Unsplash; Nadine Shaabana/Unsplash; Jeanne Menjoulet/Flickr; Jacob Brogdon/Unsplash; Author's own; Book Catalog for www.shopcatalog.com/Flickr; Andre Francois Mckenzie/Unsplash

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland

www.globalInitiative.net

CONTENTS

ACRONYMS AND ABBREVIATIONS

CSAM	child-sexual-abuse material
CSE	child sexual exploitation
ECJ	European Court of Justice
GDPR	EU General Data Protection Regulation
ICOM	International Council of Museums
ICT	information and communications technology
IOCTA	Internet Organised Crime Threat Assessments
IWT	illicit wildlife trade
NPS	new psychoactive substances
VoIP	voice-over-internet protocol

GLOSSARY

Artificial intelligence The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent (i.e. human) beings.

Big data Extremely large data sets that can be analyzed computationally to reveal trends and patterns, often used to analyze human behaviour and interactions.

Cryptocurrency A digital currency secured by cryptography, making it almost impossible to counterfeit. Most cryptocurrencies are based on blockchain technology and are not connected to central banks.

Encryption The process of disguising information or data so that it is unintelligible to an unauthorized person. Manual encryption has been used since Roman times, but the term is now associated with the disguising of information using computers.

Blockchain The technology that underpins Bitcoin and other digital currencies, known as cryptocurrencies. Blockchain stores the records of transactions made with digital currencies and is composed of a series of 'blocks' of digital information stored together in a chain.

Internet of things The vast network of physical objects with embedded microchips, sensors and communications capabilities that link people, machines and entire systems through the internet.

INTRODUCTION

Advances in technology are continuing to transform the illicit-trade landscape as dramatically as they are changing its legal counterpart, particularly as the increasing dominance of online trade provides a means to connect customers to vendors in a way that is direct, discreet and often anonymous.

By focusing on how technological innovation has affected the dynamics of a number of established organized-crime markets, this study explores the growth in 'cyber-enabled' rather than 'cyber-dependent' crime.

While cyber-dependent crimes can only be committed through the use of a computer, cyber-enabled crimes are those that 'can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology'.[1] Social-media platforms and applications, for example, which are used by 46% of the world's population,[2] have become the 'command-and-control' networks of choice for those engaged in cyber-enabled crime.[3]

A key trend identified in Europol's annual Internet Organised Crime Threat Assessments (IOCTA) is a growing 'crime-as-service model' whereby specialist providers offer cyber services to organized-crime groups. This guarantees that cyber-enabled crime will continue to grow,[5] and that the use of online platforms and cyber tools in the context of established organized-crime markets will proliferate. Furthermore, offline organized-crime networks will become increasingly interconnected, with digital tools – ranging from encryption technology to mask communications to cryptocurrencies – used to facilitate anonymous transfers, thereby blurring the boundaries between online and

Developing countries, in particular, are benefitting from this technology leapfrogging.

offline criminal markets. This study considers how traditional 'offline' markets are leveraging the opportunities presented to them by not only the surface web, which includes e-commerce and social-networking platforms, but also by the dark web and the near-anonymous transaction capabilities it offers.

Over half of the world's population are now active internet users,[5] with the number of individuals accessing the internet through their mobile phones growing at an explosive rate.[6] Developing countries, in particular, are benefitting from this technology leapfrogging. Africa, for example, is expected to have access to the same levels of internet infrastructure as the EU within the next five years. A global increase in connectivity, and the use of smartphones that grant users immediate access to a range of online communication platforms, has had a significant impact on illicit-market dynamics.

This study explores the characteristics of the online presence of the following illicit markets: drug trafficking, human trafficking, migrant smuggling, the illicit wildlife trade (IWT) and the illicit trade in cultural property. It also outlines the key changes that the growth of technology has brought upon the market dynamics of each.

The growth of cyber-enabled organized crime does not occur homogenously across all jurisdictions. Differences in levels of internet penetration, capabilities and resources for enforcement against cyber-enabled crime, as well as varying degrees of tech-savviness among customers have shaped the growth of online criminal networks in different ways. Similarly, offline criminal market dynamics are key in determining how these markets are affected by the growth of technology. Nevertheless, analyzing the impact of the growth of online markets on each of the different crime types set out above permits certain overarching themes to emerge. This enables us to draw comparisons between different outcomes, and create contrasts between the various characteristics of online illicit markets.

One such theme is the pivotal role played by private-sector online service providers, including social-networking platforms, in sharing data with law enforcement and removing content related to illicit markets. This is something we explore further on, in our discussion of the role of the private sector in regulating online illicit markets. Here we consider whether or not we are on the brink of a new age of enforcement of the online sphere; one where there is an increasing amount of pressure on the private sector to police the internet.

In the final section of this report, we highlight the key characteristics of online illicit markets and cross-market ways in which technological innovation has changed market dynamics. The strands of analysis raised in each section are brought together and considered holistically. Such comparative analysis enables us to differentiate between the uptake of digital platforms and tools by criminal markets – such as the use of the dark web, which is particularly predominant in the trafficking of drugs and people – and to highlight commonalities, such as the universal emergence of social-networking sites as multi-purpose platforms that are used at each stage of the criminal supply chain.

We present the key challenges facing law enforcement with the growth of online illicit markets, and outline some ways forward, highlighting where technology can provide law enforcement with a new and under-explored entry point into investigations.

Some of the impacts, law-enforcement challenges and recommendations we outline are the same for each of the criminal markets. Where this is the case, these are highlighted only in the final section and not in the context of each of the individual criminal markets, except for in cases where they manifest in a particularly market-specific manner.

The COVID-19 pandemic is having significant impacts on both the scale and shape of cybercrime, and on how 'traditional' markets operate, and use digital tools. Nascent evidence demonstrates that some criminal organizations, unable to operate in the offline world due to COVID-driven movement restrictions, are exploring how to continue their profit-generating activities online. For example, in Honduras, a number of gangs that rely on revenues from extorting local businesses have seen their revenues dry up as businesses are forced to close due to government COVID measures, and gang members are unable to move freely to collect extortion monies. Law-enforcement agencies report that some gangs are exploring online markets to mitigate the revenue shortfall.[7] It is unclear how long the pandemic will last, but some of the behavioural adjustments it instils may well endure once it is over. Consequently, many of the dynamics around increasing reliance on online markets, tracked below, look set to accelerate through the COVID crisis and beyond.

This study seeks to offer an entry point for further research by consolidating a range of findings across different crime types and enabling a holistic analysis of the impact that technology is having on a range of cyber-enabled crimes.

The COVID-19 pandemic is having significant impacts on both the scale and shape of cybercrime.

DRUG TRAFFICKING

The online marketplace has created new ways of purchasing and selling illicit drugs, sales of which are particularly prevalent on the darknet. The volume of illicit drugs for sale and the revenue they are estimated to bring in are growing at a fast pace on the dark web.

Despite the fact that Silk Road, the best-known site for illicit drug sales online, was taken down in 2013, the growth of the market has not slowed down. According to one estimate, revenue from these sales tripled between the closing of Silk Road in 2013 and 2016.[8]

Recent research suggests that the dark web remains a niche market when compared to global trade estimates. In 2016, RAND Europe estimated that darknet market revenue for that year was between US$12 and US$20 million,[9] whereas estimates of global trade range between US$425 and US$625 billion.[10] One study from Germany found that 70% of online buyers surveyed had only made between one and five purchases,[11] supporting the suggestion that darknet markets are not yet taking over from offline purchasing methods for illicit drugs as a whole. Despite this, numerous indicators suggest that the online illicit drugs market is growing fast.[12]

As the global production of illicit drugs increases,[13] online marketplaces offer yet another space for people to access these drugs, and for dealers to distribute them. The online illicit drug market has its own dynamics that distinguish it from the offline trade. We explore this in more detail below.

The COVID-19 pandemic is having a significant impact on international drugs trafficking. When looking at how this will affect drug users, the country in question and socio-economic standing of the drug user will shape impacts. Wealthy and middle-class drug users are more likely to be able to shift sourcing

their product to online communications, such as WhatsApp (reducing risk of exposure to contagion, and circumventing lockdown measures). They are also more likely to be able to use dark web suppliers as local supply becomes more constricted owing to COVID-imposed movement restrictions, and consequently becomes less pure and potentially dangerously adulterated. Users who are very poor, or who have serious dependencies, and perhaps other co-morbidities, do not share this luxury of either self-isolation or remote communication. They will also be most affected by the diminishing purity of the drugs they use.

Current dynamics of the online illicit-drugs market

There are significant markets for illicit drugs on both the open or 'surface' web and on the darknet.

On the surface web, there are two predominant ways in which illicit substances are sold. The first is through online markets, which typically sell substances that are technically legal – called 'legal highs' or new psychoactive substances (NPS) – or they sell supplements or pharmaceuticals, such as performance-enhancing drugs.[14]

The second way is through social media, where substances are marketed and consumers can comment, message or contact the seller directly to make a purchase. Sellers advertise their illicit substances 'by posting, videos, photos and statuses onto their social media feeds or "stories" showing what drugs they have available, the price and quantity they are selling them for, and notifying users when they are open for business.'[15]

Facebook, Instagram and Snapchat are the public social-networking platforms most commonly used for the advertising of illicit drugs, predominantly cannabis, cocaine and MDMA. Transactions are also conducted over encrypted messaging platforms, such as WhatsApp.[16]

Darknet markets offer not only illicit and prescription drugs, but also a wide range of other goods, both licit and illicit (although predominantly the latter). Having said that, drug trafficking accounts for the majority of commerce on darknet markets, making up entire listings on many darknet sites.[17] Most vendors of illicit drugs are specialists and offer no other products.[18] On the darknet, illicit drugs are sold in a similar way to which legal products are sold online. One can search products, read reviews of sellers and their specific products, and conduct transactions on these sites.

Studies have suggested that darknet markets are predominantly used in 'last-mile' transactions in a small number of consumer countries.[19] Research conducted in 2018 by the University of Oxford found that 70% of trade on darknet markets took place in the US, the UK, Australia, Germany and the Netherlands.[20] Darknet markets have thus been characterized as 'global platform[s] used for regional retail trade.'[21]

A 2018 study of Abraxas, a darknet market with 463 sellers and 3 542 buyers of illicit drugs as of 2015, suggested that over half of the purchases were made by just 10% of the buyers, with the majority of the buyers making only a single purchase. This could suggest that low-level distributors are purchasing illicit drugs online for resale.[22]

Although, overall, darknet markets appear to play a larger role at the point of distribution of illicit drugs rather than at the point of wholesale production or supply,[23] there is some differentiation among the types of illicit substances. For example, this trend is much stronger for cocaine and cannabis than for NPS and prescription drugs, where a share of online offerings originated in producing regions.[24] This could be linked to a greater overlap between countries of production and countries of consumption with regard to NPS and prescription drugs. However, for all drug categories studied, the online market for illicit drugs has been found to be shaped more significantly by the location of consumers than by where producers are located.[25]

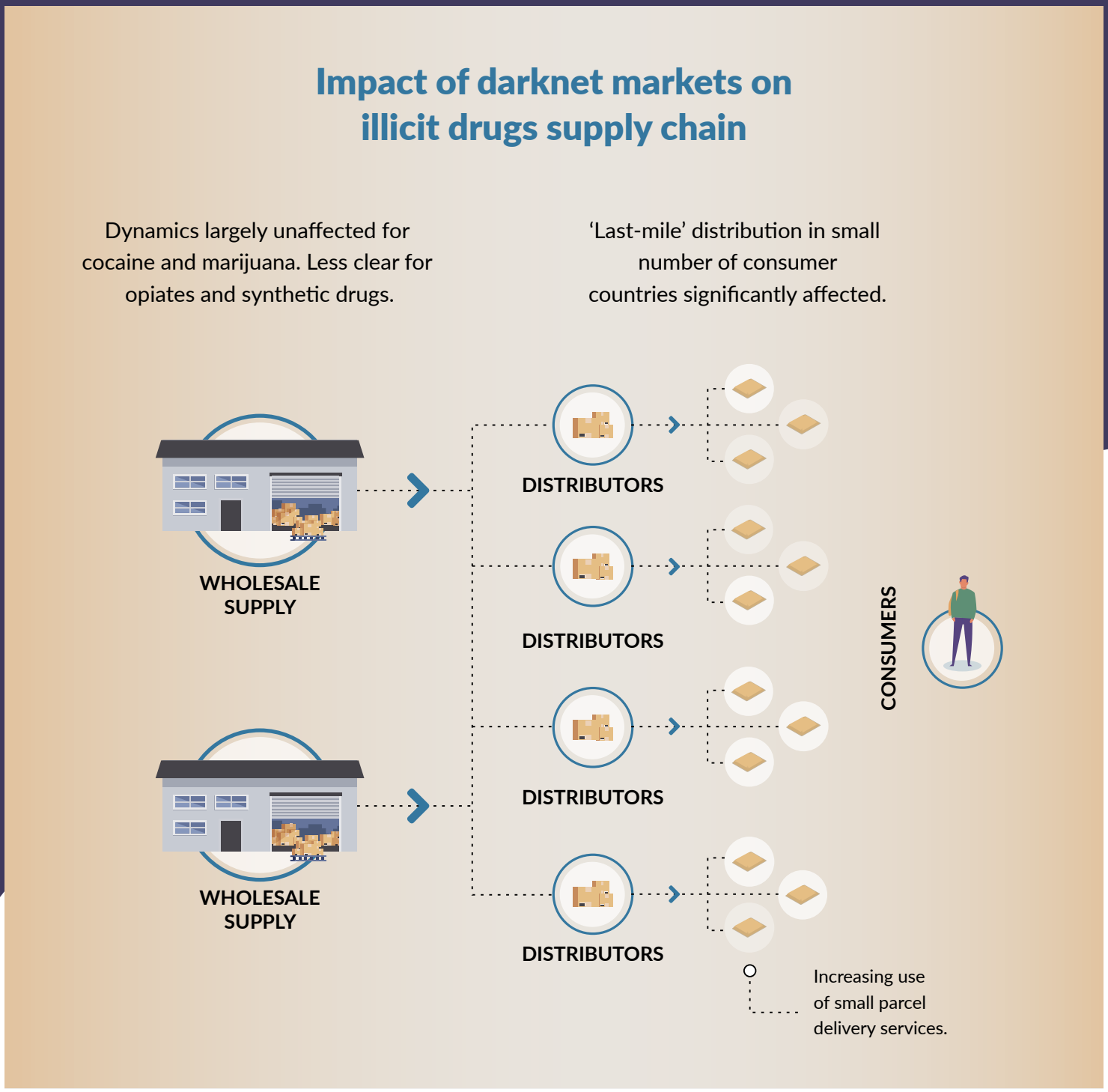


FIGURE 1 Impact of darknet on global illicit drugs supply chains.

In line with this, supply routes from producer countries do not appear to be affected significantly by the growth in darknet markets, and producers continue to move their goods across well-established offline networks. Although other technologies, in particular encrypted communications, are widely used by large drug-trafficking networks to coordinate activities, darknet markets remain 'of limited importance' to top-tier trafficking organizations, which focus on the bulk 'wholesale' movement of goods.[26]

Research conducted by RAND in 2016 found that the majority of illicit-drug transactions on darknet markets were under US$100, further supporting their characterization as consumer markets. Wholesale purchases are rare (1.8% of sales), but generate significant revenue (25% of the total).[27] The same study found that the most prominent products were cannabis (37% of total revenue), stimulants (such as cocaine and amphetamines) (29%) and ecstasy-type drugs (19%).[28]

Darknet markets play a significant role in the global distribution of certain synthetic drugs, including fentanyl. For example, synthetic opioids produced in China are regularly shipped to users in the US following transactions over the darknet.[29] Similarly, small and medium-sized organized-crime groups based outside the EU are believed to use the darknet to purchase synthetic drugs produced in Europe with the intention of distributing them elsewhere.[30] The harm caused by the use of synthetic opioids, particularly in the US, has increased law-enforcement focus on disrupting darknet markets, leading some, including Berlusconi (one of the largest markets as of 2019) to publicly announce it would ban the sale of fentanyl in order to make itself a lower-priority target for law-enforcement operations.[31]

How the growth of digital technologies has changed market dynamics

While the emergence of online markets on both the surface and the dark web, together with the growing availability of a range of digital and information communication technologies, has not transformed the underlying infrastructure of the international drug-trafficking trade, it has catalyzed a number of shifts in market dynamics.

Many drug-trafficking groups exploit technology and apps to communicate – El Mencho, of the Sinaloa cartel, communicates with his senior traffickers by WhatsApp group.[32] With end-to-end encryption, and easily installed, this is a simple and direct way in which to command horizontally structured organizations. WhatsApp is used by dealers and users in many countries as a means through which the various risks related to drug transactions (including arrest and hijacking) are diminished.

Trafficking networks are increasingly likely to rely on online financial transactions, including with the use of payment apps on smartphones, like EcoCash, which is common in Zimbabwe.[33] This allows consumers and dealers to avoid carrying cash, reducing the risk of cash being used as evidence in the event of arrest, and of being hijacked.

Turning to darknet markets, these have the greatest effect on the final links in the supply chain, and on consumer markets.

Online markets have transformed the drug market from a network economy, in which limited advertising and clandestine operations mean transactions typically occur through existing networks and thereby favour incumbents, to a conventional market where dealers compete on price, quality and service. This has eroded the incumbent advantage and lowered barriers to entry.[34]

Social-media platforms are being used to recruit new sellers. Research in the UK found that social media has reportedly been used to advertise the luxurious lifestyles of drug dealers and to groom child dealers as a way of cutting out the middleman, thereby penetrating local markets directly.[35] In two separate trafficking arrests in the US, the person arrested claimed to have responded to an advertisement on Facebook for 'people looking for work' or 'an opportunity to make money', and ended up trafficking illicit drugs for cartels in Mexico.[36] Social media is thus able to create new opportunities for transactional relationships between criminal groups and new ad-hoc employees.

Recreational users buy illicit drugs on darknet markets for a combination of reasons related to safety, quality and ease of purchase. The online market allows for anonymity in both sales and

The advantages for sellers on darknet markets are that they can avoid detection and minimize risks.

purchases, reduces direct contact between players in the market (thus possibly reducing risks associated with open-air drug markets), and in some cases has allowed for enhanced accountability in rating a seller's product or products – an interesting potential benefit from a public-health perspective. However, the ease with which vendors are able to post fake reviews and information online is poorly understood by users, and this can easily increase a user's chance of being misinformed.[37] Purchases tend to be based on 'price, details of product, vendor reputation, feedback from other buyers, and available "trip reports" (descriptions of personal experiences with the effects of specific substances)'.[38] Some listings are even described as 'fair trade' or 'conflict free'. The prevalence of illicit-drug supply on social-media platforms, which are heavily used by those between the ages of 16 and 24, could result in growing markets among younger drug users.[39] Built-in design features on these platforms, including 'suggested friend' functions and hashtags to expand reach, can be used by dealers to expand their customer base.

The advantages for sellers on darknet markets are that they can avoid detection and minimize risks, such as 'arrest and violence, and threat to profits and reputation'.[40] As noted above, this may have lowered barriers to entry for small-scale players in the drug-trafficking markets; a hypothesis supported by the limited use of the darknet by larger criminal groups.

According to RAND, both buyers and vendors of illicit drugs on the darknet share a common profile. This has been identified as someone young, male, hailing from English-speaking or West European countries, well-educated, entrepreneurial and with strong IT skills.[41] This is, to a significant extent, shaped by the prevalence of darknet markets for final-leg distribution in consumer countries. Some research suggests that online vendors are either established dealers with access to the product, or newcomers who are expanding their base beyond selling to friends.[42] There is concern that a younger and more tech-savvy consumer base could access illicit substances more easily, but evidence has not yet revealed this to be a trend.

Buyers purchasing drugs on the darknet typically use bitcoin or other types of cryptocurrency to pay for the product. In some cases, including in the case of the original Silk Road, payments are held in escrow by darknet administrators until the product is received. Then, the purchased substance is mailed through either private or public mail systems. Products can be delivered to a number of anonymous locations, including anonymous post-office boxes, automated booths or 'packstations'.

By collapsing geographical distances, online criminal markets empower smaller dealers to supply local markets while trading on the global drug-trafficking market. They also rely on small-parcel post, which has a significantly low surveillance rate, thereby further reducing the risk of engagement.[43]

Reduced operating costs means drug prices are predicted to decrease.[44] Online dealers require fewer employees and benefit from lower overheads, as is also the case with licit online businesses.

Legal and enforcement challenges

When trying to tackle operations conducted on the surface web, law-enforcement entities often rely on the cooperation of private-sector e-commerce platforms and social-networking sites. However, such cooperation has always been ad hoc or at the discretion of the respective platform.

When platforms have cooperated in attempting to mitigate their use by drug-trafficking operators, the speed at which sellers adapt to these changes lessens the impact. For example, in 2017, Facebook disabled certain key search terms – for example, 'OxyContin', 'Xanax' and 'fentanyl' – on its search engine and replaced some search results with adverts for substance-abuse treatment. Sellers adapted quickly by putting the name of their product in their Facebook profile name, thereby enabling searches to function as before.[45]

The use of dynamic coded language and emojis by dealers operating online, including on social media, presents a further challenge to both law enforcement and social-networking platforms in identifying accounts supplying illicit drugs.[46]

Large-scale law-enforcement operations have successfully shut down a number of marketplaces on the dark web, but this has led to the fragmentation of the darknet market. This is evident in the growth of the number of 'vendor shops (shops run by a single vendor), and secondary markets, i.e. non-English-language markets catering to a particular nationality or language group'.[47]

There is significant concern among law-enforcement entities that sellers distributing illicit drugs on the darknet will react to such shutdowns by moving away from large marketplaces, and instead offer products to consumers directly over encrypted messaging apps, such as Telegram. The already widespread use of encrypted networking platforms, including WhatsApp and Snapchat, by the illicit-drugs market poses a barrier to the gathering of data by law enforcement, particularly as platform owners have typically refused to share user data in the context of police investigations. These messaging apps are therefore extremely difficult for police to monitor.

Successful shutdowns do appear to have a temporary impact on the volume of transactions conducted on darknet markets. For instance, in July 2017 international operations shut down three darknet markets (selling illicit drugs and other commodities) that accounted for 87% of total market activity: AlphaBay, the Russian Anonymous Marketplace (RAMP) and Hansa.[48] It was observed that in the aftermath of the closures, the 'value of Bitcoin transactions to darknet markets fell by two-thirds'.[49] This could in part be because users are accustomed to a particular site, which means the closure of the site is likely to change the behaviour of the user. One survey found that after the closure of Hansa and AlphaBay, '15 per cent of users used darknet markets less frequently after the shutdown and 9 per cent stopped using the darknet for drug purchases'.[50]

The sheer number of substances available on ready-to-order platforms reflects the daunting nature of trying to shut down such platforms. On one site, over 2 000 kinds of opioids (real and synthetic) can be found, purchased and shipped to consumers around the world.[51] Although half a dozen darknet markets have been shut down in the past six years, there are still an estimated 30 illegal online markets in operation.[52]

The widespread use of cryptocurrencies on darknet markets complicates investigation techniques that are based on tracking financial flows, while the development of high-privacy cryptocurrencies poses even greater barriers to law enforcement. Darknet markets continue to accept a growing range of cryptocurrencies, as their founders take steps to mitigate the risk of law-enforcement disruption by encouraging transactions to be conducted using increasingly private currencies.

There have been some short-term successes in countering this niche area of the illicit-drugs trade, but the proliferation of this trade also reflects a

microcosm of the greater challenges faced by law enforcement in trying to counteract the use of illicit drugs. The 'balloon effect' – whereby greater enforcement in one country or region displaces illicit activity to another, and which has repeatedly been tracked as a result of traditional law-enforcement techniques on drug-trafficking operations – appears to be replicated in online markets.

The way forward

Online platforms should be held more accountable for their continued use in the trade of illicit substances and the illegal trade in prescription drugs. Law-enforcement and regulatory focus should be on those platforms most frequently used by youth, including social-media platforms, video service sites and streaming platforms.

Attention should also be paid to reducing access to substances that cause the most harm. There is evidence showing that some sites will self-regulate and refuse to sell substances such as fentanyl; both on account of the known harm it can cause, and the understanding that law enforcement will target sites that sell this product. Crafting law-enforcement strategies through a harm-reduction lens, and publicizing this approach, may prompt further self-regulation across darknet markets, making more harmful drugs increasingly difficult to access.

The implementation of awareness campaigns targeting 'social supply' – encouraging individuals to buy in bulk with the purpose of sharing with friends – could be helpful in stopping the distribution of drugs through informal social networks, the use of which seems to be growing with the increased availability of illicit drugs in the online marketplace and the perceived lower risk of purchase. Strategies could include educating people on the potential health risks involved in obtaining substances of unknown origin from an unknown seller, and predominantly in the context of plant-based synthetic drugs, of the harm created by the illicit-drug trade in producer and transit countries.[53]

Collaboration needs to be enhanced between law enforcement, online platforms and postal services, as the latter is increasingly being used to distribute illicit drugs and is currently being subjected to limited surveillance. Additionally, research should continue to explore how open web and darknet markets operate, including how they shift in response to law-enforcement interventions, in order to create a more holistic response to the problem.

Finally, as cryptocurrencies move further into the mainstream financial sector, working with cryptocurrency exchanges in attempting to identify funding from illicit sales – and isolating such funding could have a positive effect on limiting darknet sales.

HUMAN TRAFFICKING

Human trafficking[54] is a growing crime with a global foothold and a huge area of 'business'. It affects roughly 40.3 million people around the world, 71% of them women and girls and 25% of them children, and its perpetrators are estimated to bring in US$150 billion annually.[55] Two-thirds of human-trafficking victims are exploited through forced labour and two-thirds of profits generated by human trafficking come from commercial sexual exploitation.[56] These forms of modern slavery are most prevalent in Africa,[57] followed by Asia and the Pacific,[58] and then Europe and Central Asia.[59]

Digital and network technologies have led to the emergence and expansion of cyber-enabled human-trafficking offences. One fast-growing trafficking crime that has been predicted to increase as a result of the growth of digital and network technologies is online child sexual exploitation (CSE). CSE is one of the crimes adapting most quickly to the opportunities offered by technology, rapidly shifting from the use of group file-sharing services, to sextortion, online grooming, and the live streaming of sex acts to a closed audience. The latter is extremely difficult for law enforcement to track, as it leaves no record of the images streamed on the devices used.

The risks and costs to perpetrators are reduced in these crimes, as those committing the acts of exploitation do not have to be physically present with the victims. In 2018, over 45 million online images and videos were reported and flagged by technology companies as being in the category of child sexual abuse: the highest number ever recorded and more than double that recorded in 2017.[60] The COVID-19 pandemic has been driving more trafficking activities online. The virus is swelling both supply of, and demand for CSAM. This is partly attributable to the widespread closure of schools leading to an increase in unsupervised children online, an increase in working from home dynamics, and

Technological developments have changed every aspect of the human-trafficking process.

restricted offline movement. In early April 2020, as the COVID-19 pandemic spread globally, Europol reported a spike in the volume of online child sexual abuse materials (CSAM) being posted on online forums, and on the number of downloads in peer-to-peer sharing networks.[61] Europol has also tracked an increase in attempts to initiate online contact with children for the purpose of online exploitation.[62] In line with this, the FBI has issued specific warnings about the increased risk to children of online grooming during the COVID pandemic.[63] Newly produced CSAM will multiply online and remain available until taken down, while new perpetrators are likely to remain involved post-pandemic. This points to a long-term expansion of the online human trafficking market.

Current dynamics of online human-trafficking operations

How is technology changing the human-trafficking landscape? We will examine how it is being used to facilitate exploitation by traffickers, the ways in which it has altered market characteristics, and its effects on demand. This section also explores the legal and law-enforcement challenges arising from these changes. It concludes with promising examples of how technology has been used, and can continue to be used, to prevent, disrupt and mitigate human-trafficking activity.

As enhanced internet penetration enables the population at large to connect on an increasingly global scale, it also facilitates international connectivity among perpetrators and between traffickers and their victims. Technology, with its transformative impact on current trafficking dynamics, acts as a significant risk multiplier when combating this type of crime.[64] Technological developments have changed every aspect of the human-trafficking process: from planning, to the recruitment and exploitation of victims, to transactions and money laundering.

Traffickers use digital and network technologies, such as encrypted apps and invitation-only deep-web forums (for example, WhatsApp, Dark0de and ShadowCrew), to anonymously and securely plan and communicate with each other.

An increasing number of children and teenagers, especially girls, are being virtually groomed and controlled through chat rooms, messaging apps, and social-networking sites such Facebook, Snapchat and Kik.[65] Most recently, sex offenders have been found to be grooming children on Instagram more than on any other online platform.[66]

Traffickers are also using such platforms for labour-exploitation purposes through the advertisement of promising jobs. In the case of labour exploitation, it is in fact the lack of technology that is ultimately being used to deceive, isolate and exert control over victims. Traffickers often do not allow their victims access to any kind of media, telecommunications or internet connection, to prevent them from seeking help.[67]

Information and communications technology (ICT) – in the form of messaging apps, internet chat rooms, webcams, voice-chat systems (such as Skype), online games and virtual worlds (such as Second Life or VRChat) – is being used to coerce victims, especially children and teenagers, into being sexually exploited. This online sexual-abuse material is live-streamed, recorded and then distributed further.[68]

It is estimated that approximately 150 000 child-sex-trafficking advertisements are posted on the internet each day.[69] Live-streaming is growing particularly rapidly, as traffickers have realized that the content produced is extremely difficult for law enforcement to trace.

Societal attitudes in certain communities differ in the case of virtual and physical sexual exploitation, with the former perceived to be less harmful and somewhat destigmatized as a result. In certain cases in Asia, families were found to allow their children to perform on-demand sex acts for the camera because such acts are not physical and therefore not perceived to be harmful.[70]

Traffickers market their victims on various online platforms, both on the surface web and the dark web. Escort adverts involving trafficking victims have been reported on traditional websites such as Backpage and Craigslist,[71] while CSAM is prevalent on the darknet.[72] Buyers then use technologies to access, watch, record and disseminate materials of the victims. Perpetrators are often not only producers and distributors, but also consumers of these materials. Notably, membership of certain closed groups is predicated on members producing content and not merely consuming it. This membership is vast: Playpen, a members-only darknet website featuring CSAM, has roughly 160 000 members worldwide.[73]

Finally, the emergence of cryptocurrencies such as Bitcoin and Altcoin has enabled traffickers to receive their illegal proceeds anonymously and securely, as well distribute funds to other members of their criminal networks.

Live-streaming is growing particularly rapidly, as traffickers have realized that the content produced is extremely difficult for law enforcement to trace.

How the growth of digital technologies has changed human-trafficking markets

The increasing availability of a range of digital tools and technologies has been exploited by human-trafficking markets in numerous ways, but the effects this has had on market dynamics can be broadly categorized as follows:

- Traffickers have benefited from enhanced anonymity in their communication both with other criminal operators and with victims. Stakeholders in trafficking markets (trafficking networks, buyers/service users, victims and potential victims) are able to communicate anonymously and securely via encrypted messaging apps, closed chat rooms and other invitation-only deep-web forums.
- The growth and increased accessibility of encrypted ICT have flattened trafficking networking structures, rendering them less hierarchical and more horizontal and loosely interconnected.[74]
- In terms of the structure of criminal operators, individual criminal actors or 'entrepreneurs' have emerged in human-trafficking markets, and their numbers have increased, particularly regarding the production and distribution of CSAM online. This is largely owing to lowered risks and reduced overhead costs (for example, in recruiting potential victims, laundering money and transactions).[75]
- Widespread internet penetration, and the range of digital tools made easily available to the mass market, have made victims highly vulnerable to trafficking online. The rise of ICT and big data, and the proliferation of the internet of things (IoT),[76] have created new opportunities for traffickers to access and gather information, and to identify, profile and recruit an increasing number of potential victims, particularly among vulnerable groups such as children and teenagers.
- The widespread availability of labour- and sexual-exploitation materials online, to both regional and global audiences, has resulted in an increase in market reach and demand.[77] This is illustrated in a 2017 Europol report, which found that more than half of reporting European countries cited online CSE to be 'a growing phenomenon'.[78]
- Payment transactions are increasingly made using cryptocurrencies, enabled by blockchain technology.[79]

Legal and enforcement challenges

ICT enables traffickers to communicate and exploit victims without the need for face-to-face interaction, thereby obfuscating law-enforcement efforts to identify perpetrators. Research undertaken in 2018 into the role of technology in child sex trafficking found that under 50% of victims met their traffickers face-to-face, with the majority using texts, websites or messaging apps to communicate.[80] The widespread use of encrypted communication services and platforms by those involved in trafficking, both to communicate within networks and to contact victims and buyers, makes these communications more difficult to track.

Widespread data-protection legislation, and in particular the EU General Data Protection Regulation (GDPR), which contains the most stringent data-protection standards globally, can pose further obstacles to trafficking investigations. Although this is applicable to investigations of all crime types, it is particularly relevant to trafficking investigations, as they often require access to sexually explicit material, which falls within the definition of 'special category data' under the GDPR and is therefore under greater privacy protection.

In contexts where the GDPR applies,[81] and due to its extra-territorial effect it applies far beyond the EU, law enforcement now needs to navigate a complex legal process, in some cases requiring authorization from a judge to obtain information on users/registrants of domain names and IP addresses, including those registered on the so-called 'Whois' domain name database, which was previously

more easily accessible to the public.[82] This has placed a substantial administrative burden on law enforcement, specifically when investigating users, forums and websites containing online CSAM and other illicit materials generated from sexual exploitation.

Meanwhile, cyber-security legislation remains patchy, affecting the regulation of all categories of cyber-crime. The particular vacuum of IoT legislation – which translates into an extremely unregulated marketplace in which IoT devices are manufactured – is of particular relevance to human-trafficking markets (and to other criminal markets based on data theft or fraud, which are not covered in this paper). Traffickers can hack IoT devices to identify, profile and recruit potential victims, and record the material clandestinely. Ten years have passed since IoT was 'born' in 2008/9,[83] and yet only the UK and the US have introduced, or are starting to introduce, some kind of IoT security law.

An under-regulated or unregulated IoT marketplace encourages manufacturers of smart devices to focus exclusively on profit generation, and overlook security aspects, thus leading to security gaps that traffickers can exploit. One reported incident involved the hacking of a Wi-Fi-connected baby video monitor, which the hacker used to threaten the parents with the kidnapping of their baby.[84] Furthermore, the proliferation of IoT devices, coupled with law-enforcement agencies' limited resources and capacity, has made it difficult for agencies to cope with the large number of risks posed by the lack of cyber-security frameworks, enforcement and related measures.

Human trafficking online, particularly the sharing of CSAM, is transnational and borderless. The lack of a legal framework for systemic cross-border cooperation, including intelligence sharing and cross-border communication, significantly hampers cross-jurisdictional investigations and prosecutions.

The way forward

Given the fast-changing nature of human trafficking in the digital space, responses should similarly leverage technology developments in combating trafficking markets.

Awareness campaigns should focus on those groups most vulnerable to online grooming and exploitation by trafficking networks, in order to make them aware of the ways in which traffickers exploit certain social-networking platforms and other online communication methods.

A legal framework facilitating effective partnerships and collaboration with the private sector should be introduced, as should ways of regulating legal and transparency issues surrounding this cooperation. Given the key role of the private sector in combating trafficking,[85] a successful counter-trafficking approach must include this sector.[86]

Anti-online-trafficking approaches and strategies should include multiple stakeholders – such as governments, the private sector, NGOs, academia and the general public. Examples of multi-stakeholder initiatives countering online human trafficking include the Society for the Policing of Cyberspace (an international network of practitioners from the public and private sectors),[87] the High Tech Crime Consortium (an international organization connecting cyber cops and investigators, sharing information on cybercrime matters),[88] the Virtual Global Taskforce (an international collaboration of law-enforcement agencies, NGOs and industry partners to protect children from online and offline sexual exploitation),[89] and Tech Against Trafficking (a coalition of technology companies collaborating with global experts to help eradicate human trafficking using technology).[90]

The capacity building of stakeholders involved in law-enforcement efforts against cyber-enabled trafficking should be enhanced, specifically with respect to the use of the encrypted communications applications and cryptocurrencies commonly used by traffickers. Such stakeholders should include front-line police officers, judges and prosecutors.

There is a need for the harmonization of criminal-justice legislation across countries, within regions – or globally, if possible.

There is a need for the harmonization of criminal-justice legislation across countries, within regions – or globally, if possible. Significant convergence is already taking place at the level of the EU, but greater coherence is needed.[91]

Regulation of IoT devices and cyber security should be introduced and enforced in order to restrict criminal hacking of these devices. Although progress on this has been extremely slow, there are some nascent examples of promising practices. California became the first US state to introduce an IoT cyber-security law in September 2018, and in May 2019 the UK announced plans to introduce an IoT law, envisaged to come into force in 2020.[92]

Technological innovations and tools countering trafficking at each stage of the crime cycle continue to be explored, developed and put into use. Digital and network technologies have not only led to the emergence and expansion of cyber-enabled human-trafficking offences, but have also opened up new opportunities for anti-trafficking stakeholders and communities to effectively and innovatively combat these crimes. Law enforcement, the private sector and civil-society organizations have developed innovative solutions, ranging from low-tech applications, such as simple educational apps informing potential trafficking victims of the risks of sexual and labour exploitation (for example, (Un)trafficked, ACT! and BAN Human Trafficking!), to more advanced technologies, such as geospatial and space-based technology used to track down fishing vessels engaged in illegal activity (for example, Maxar and Global Fishing Watch).

Technologies are also increasingly being used in every phase of the trafficking cycle or the victim journey: as a tool for prevention (for example, educational tools to raise awareness), as a way to investigate and disrupt crimes (for example, digital forensic and reporting tools), as well as a means to prosecute trafficking, and to assist, support and empower survivors (for example, tools that help victims access legal assistance and knowledge of the various regional and national referral mechanisms available to them).[93] Such technological innovations and interventions have been, and will continue to be, the driving force of current and future anti-human-trafficking efforts.

The opportunities presented by the expanding mandate of data-protection authorities should be leveraged to combat online-trafficking markets. The appropriate way in which to regulate the internet is the subject of ongoing debate (as discussed later on in the section on the role of the private sector in regulating these markets). Some European jurisdictions, notably Spain, are seeking to enhance proactive monitoring of CSE and other unlawful, sexually explicit images on the internet, and putting pressure on internet platforms internationally to remove such content.[94] The high priority granted to countering CSAM by regulators and governments, together with the fact that most CSAM constitutes 'special category data' and falls within the category of stringent protection under the GDPR, make counter-CSAM activities fit more easily under the mandate of data-protection authorities than do other criminal operations.

MIGRANT SMUGGLING

Although human smuggling is not a new phenomenon, the pivotal role it has come to play at the centre of modern migration dynamics is a recent one. The newly found prominence of human smugglers has been driven by an enhanced desire or need for mobility, on the one hand, and a shrinking space for legal migration, on the other. The former is attributable, in part, to record-high and ever-growing displacement levels, driven by conflict, gang violence and climate change, among other factors, and an increase in both real and perceived global inequality.

Unprecedented levels of connectivity feed aspirations of a better life, and when combined with increasingly securitized borders and restrictive visa regimes, this bloats the client base of smugglers. As a result, the human-smuggling market is one of the fastest-growing criminal markets globally,[95] estimated to be worth, at a minimum, US$7 billion as of 2016.[96]

Increasing internet penetration, and in particular the growing popularity of social-networking sites, used widely and ever-increasingly by smugglers, has given the human-smuggling industry a new marketplace for advertising and communication. The policing of this marketplace has therefore become a priority for governments concerned with irregular migration.

The EU, in particular, has expended vast resources on countering human smuggling (and irregular migration), establishing new anti-smuggling operations with enhanced ICT capabilities,[97] and broadening the mandate of the Internet Referral Unit. The unit was originally established to monitor and combat terrorist propaganda and violent extremist activity online, but its mandate was expanded to include online content related to migrant smuggling.

The COVID pandemic is likely to drive, at least in the short term, more communications online as state-imposed movement restrictions within countries, together with emerging social taboo on movement, limits offline interactions. COVID-19 is driving increasingly hostile attitudes among communities and policymakers to migration. Pathways for legal migration are set to shrink further. These trends, together with the unprecedent movement restrictions imposed at borders and domestically, are diminishing migration and the smuggling business in many regions in the short term. Yet these developments promise to swell the profits of the smuggling industry in the medium term. The increased importance of online communications to the smuggling market is likely to linger.

The following section explores the current dynamics of the human-smuggling market, highlighting how it has changed the way in which the market functions. Next, we will be identifying key challenges to law enforcement and outlining initiatives that could yield some success in countering the enhanced reach of organized-crime groups working in human smuggling.

Current dynamics of the online human-smuggling market

The modus operandi of the smuggling industry is, as with all criminal markets, extremely flexible and dynamic, constantly evolving to mitigate the risk to smugglers themselves – particularly those higher up the power chain – and to evade law-enforcement action.[98] In line with this, smuggling networks have leveraged the opportunities presented to them by encrypted communication apps and social-networking sites to coordinate activities, and despite a recent upsurge in focused efforts, law enforcement is still in the early stages of tracking these developments.

In most source communities, including those across Africa and South East Asia, the predominant form of communication between smugglers and would-be migrants continues to be word of mouth or face-to-face interaction. Online interaction through social-networking sites, such as Facebook, has been reported as a prelude to a face-to-face meeting, used to establish initial contact and ascertain basic elements of the contract, including the cost of travel and country of destination. During the COVID crisis, more of this interaction will have occurred online, and this may continue once movement restrictions are lifted.

Social media is used for advertising, grooming potential clients and organizing logistics by smugglers globally, with Facebook, Viber, WhatsApp and Telegram being the most popular platforms. Significant detail is provided on surface-web communications, with Facebook feeds being used by smugglers to advertise modalities and prices for specific routes, including group discounts for families, in particular on routes from North Africa to Europe. Smuggling networks utilize the blended surface and deep-web functionality of social-networking sites to shift between advertising and providing greater detail to specific clients. Smugglers have also used social-networking platforms to send videos of migrants being tortured to families to extract ransom payments from them.

As smugglers typically share ethnic and cultural links with their clients, platforms preferred by smugglers tend to reflect those used most typically by the source community. This helps smugglers to facilitate communication with their clients. For example, Line is popular in Thailand and other countries in South East Asia, but less so elsewhere, and WhatsApp and Facebook are heavily used in the vast majority of countries internationally.[99] There are only

25 countries in the world where WhatsApp is not the most commonly used messaging app.[100]

In a number of regions analyzed, including most of Africa and South East Asia, online human-smuggling markets do not appear to make use of the dark web. However, some international law-enforcement professionals posit that smuggling networks operating to move high-net-worth individuals may be using the dark web, particularly in Eastern Europe.[101]

The online functionality of the smuggling market does not appear to have significantly affected the structure of networks, which range from hierarchical arrangements reminiscent of company structures (with a kingpin or 'CEO' coordinating transnational operations), to loosely affiliated individuals who cooperate to maximize earnings, but share limited intelligence or little allegiance. The latter is more common, particularly in the 'pay-as-you-go' smuggling industry, which moves a far larger volume of people than the more exclusive 'full-package' market.[102]

Technological innovation has modernized payment transactions between smugglers and their clients, particularly triggering innovation in the *hawala* market, which is heavily relied upon by human-smuggling services. However, the use of cryptocurrencies has not been widely reported. This is good news for the 'follow-the-money' investigative techniques, which are repeatedly emphasized as a promising route for human-smuggling investigations.

Technological innovation has modernized payment transactions between smugglers and their clients, triggering innovation in the hawala market.

How the growth of digital technologies has changed market dynamics

Advances in information and communications technology and the growing popularity of social-media platforms have affected both the decision-making process for migration and the systems by which people migrate, shaping how clients find smugglers and how smugglers advertise their services.

Enhanced connectivity has driven demand for human-smuggling services. Human smuggling can be characterized as an illicit market where local aspirations are achieved through illicit access – that is, local criminal human-smuggling markets meet local demand.[103] The growth of connectivity across the developing world acts as a driver for enhanced aspirations and for chain migration, as source communities are more exposed to the success of those diaspora émigrés who are able to retain close links to home.[104] Of the roughly 6 billion cellular phones in circulation globally, 5 billion are used by people in developing countries. Mobile-phone penetration in developing countries reached almost 90% in 2013, and smartphone usage is predicted to continue increasing exponentially, with smartphone connections estimated to reach over 700 million people in Africa and 480 million in South East Asia by 2020. This demand driver appears set to increase.[105]

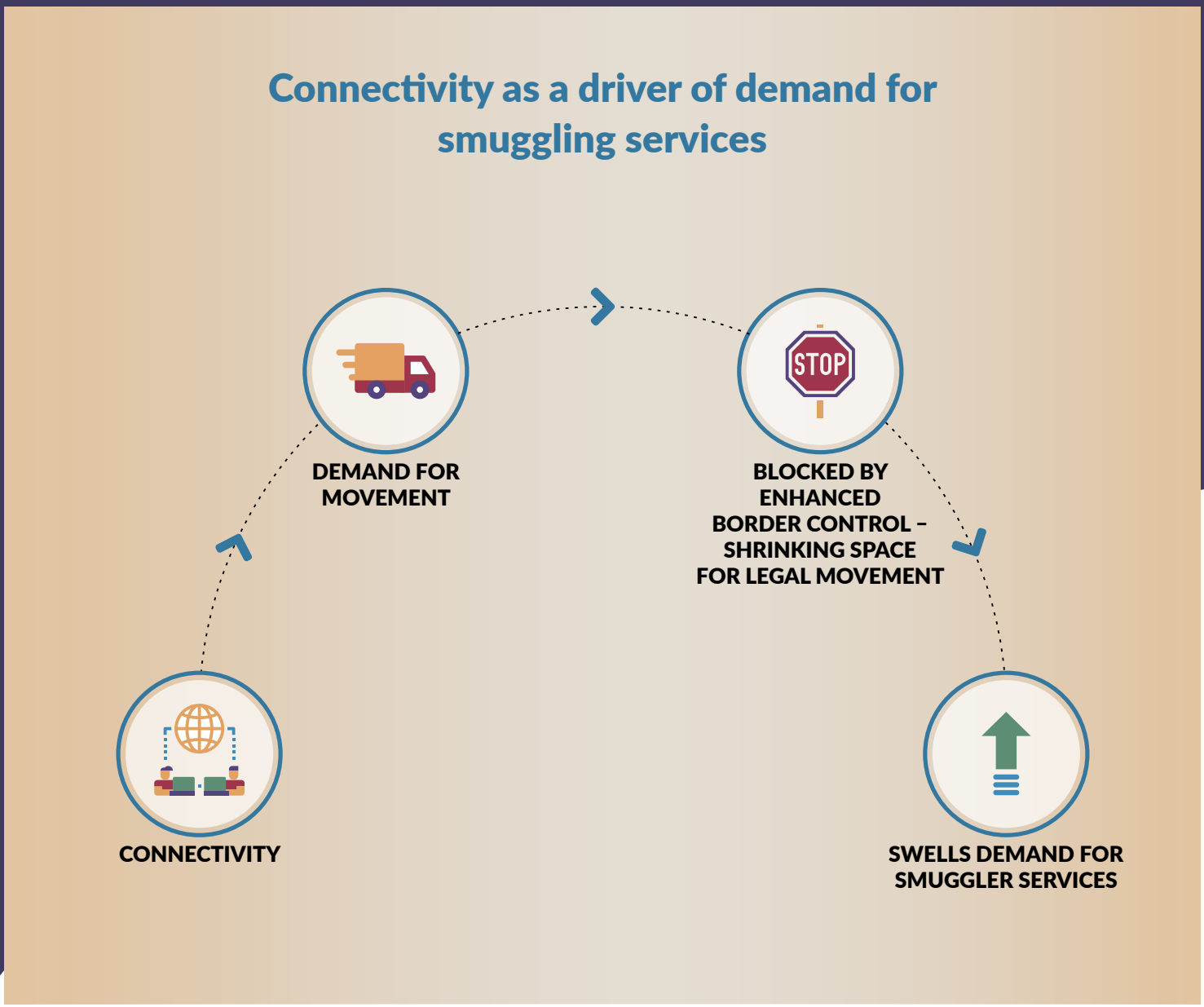


FIGURE 2 How connectivity fuels the demand for movement and creates chain migration dynamics.

Significant communication between smugglers and clients on social-networking sites has enhanced the ability of smugglers to shift their modus operandi in response to changing law-enforcement dynamics, and to facilitate the congregation of migrants at given meeting points.[106] Internet service providers are, in most jurisdictions, not yet legally required to monitor and remove content relating to migrant smuggling. Facebook has publicly stated that offering services relating to human smuggling is illegal and violates its terms of use, and seeks to remove related content from its platform. While content relating to the coordination of smuggling services (such as prices or locations) is removed, lags in timing mean that the information is sometimes already out of date by the time it has been taken down. Coordination and information sharing between migrants about their journeys is, however, likely to remain and thus Facebook will continue to be a platform for smugglers to use in engaging with prospective clients.

Heightened connectivity increases the information migrants are able to access regarding routes and risks, much of which is shared across social-networking sites. Enhanced information flows, for example, confirm that migrants are making rational and carefully calibrated decisions based on a significant amount of information and on careful assessments of risk and reward. This challenges previous claims that clients use smuggling services because they are ignorant of the risks faced. It also means that migration cannot be curbed by information campaigns, and that smugglers, while in many cases shaping routes, are not creating movement. This makes smuggling more difficult for governments of destination countries to tackle, as the desire for movement is far harder to address when it cannot simply be blamed on criminal coercive smuggling networks.

Connectivity also enables real-time feedback during the journey (which can be particularly valuable in contexts where the reputation of the smuggler is still key in the source community), and instant evidence of safe arrival. The voice-over-internet protocol (VoIP)[107] Viber and other instant-messaging apps are commonly used by migrants to report the safe arrival of boats in Europe.[108] Many apps have capitalized on this and have been designed to provide real-time information for people on the move.[109]

Widespread smartphone usage leaves the smuggled vulnerable to misinformation scams. A number of international organizations, including the UN High Commissioner for Refugees (UNHCR), have detected false branding of their logos on such scams. These entities have sought to combat misinformation by using social-media platforms and WhatsApp to communicate directly with community leaders so that they can relay accurate information to their communities, thereby decreasing vulnerability to scams.

Legal and enforcement challenges

A lack of capacity and resources needed to investigate online crimes is a significant challenge facing law enforcement, particularly as the multilingual nature of investigations, together with the vast quantities of data needing analysis, can drive up investigative costs and create a significant drain on already overstretched resources. In addition to this, human smuggling is not considered a high priority in most jurisdictions, arguably barring the US and Europe. The limited tech awareness of some law-enforcement entities means that social media's potential as a resource for tracing human smugglers is not being exploited fully. Some transit- and source-country governments (for example, Egypt) have identified cyber-enabled human smuggling and the significant gap in law-enforcement capabilities as a key cause for concern, and have therefore requested tailored training from Europe in an attempt to ameliorate the situation.[110]

Mandates relevant to tackling cyber-enabled elements of human smuggling are split between different government ministries. Their coordination is often not clearly delineated, causing delays in investigations. In Indonesia for example, while law enforcement/police are tasked with addressing human-smuggling crimes, the mandate to take down suspicious websites or social-media accounts falls under the Ministry of Communication and Technology. The lack of coordination between the two groups poses an obstacle to effective law enforcement.

Poor coordination between private technology companies and governments poses a continuing challenge to data gathering and investigation across all online criminal markets. This is exacerbated in the context of human smuggling, where a significant proportion of the relevant material may

There should be an enhanced use of social-networking sites to monitor and investigate human-smuggling activity.

not immediately appear illegal, and therefore is liable to fall outside of the scope of an online platform's terms of service. Across a number of jurisdictions, there are no set mechanisms for official cooperation or collaboration between government entities and private online service providers when it comes to human smuggling. Law enforcement often relies on informal communication channels, but these, in turn, rely on personal relationships and vary between agencies.

Data-protection laws can further hinder data gathering. Although some advertising is made public, most communication occurs on site-users' private forums and concerns specific individuals, meaning that law enforcement must navigate applicable data-protection laws in order to access content.

The way forward

There should be an enhanced use of social-networking sites to monitor and investigate human-smuggling activity. Nascent monitoring practices, particularly of Europe's national and cross-border law-enforcement bodies, have yielded some success,[111] and may enable forces to assess smuggling-network patterns. Such enforcement efforts should focus on the prosecution of sophisticated smuggling groups, rather than merely on high numbers of low-level prosecutions, as has been seen with previous trends.

Improving coordination and data sharing between private technology companies and governments is essential to countering human-smuggling operations. Although this is typically more advanced in Europe than it is in Asia or Africa, even there it remains patchy. A 2016 survey of EU member states found that only seven out of 16 member states (including Norway) reported having established cooperation with service providers with regards to online content and how it relates to migrant smuggling.[112]

Social-networking sites should review their terms of service and community guidelines to ensure they are sensitive to human-smuggling-related content and activity, and to facilitate data sharing. Furthermore, harmonization of cross-border e-data sharing regimes and other regulatory frameworks which govern the collection and use of electronic evidence, together with judicial capacity-building, would facilitate investigations and increase the power of e-evidence in court.

Social-networking sites should also be used to facilitate communication between irregular migrants exploited by smuggling services and law-enforcement, regulatory or third-sector bodies. An example of this is where instant-messaging apps, such as WhatsApp, have been used by smuggled persons to report human-rights violations to the Malaysian Human Rights Commissioner.

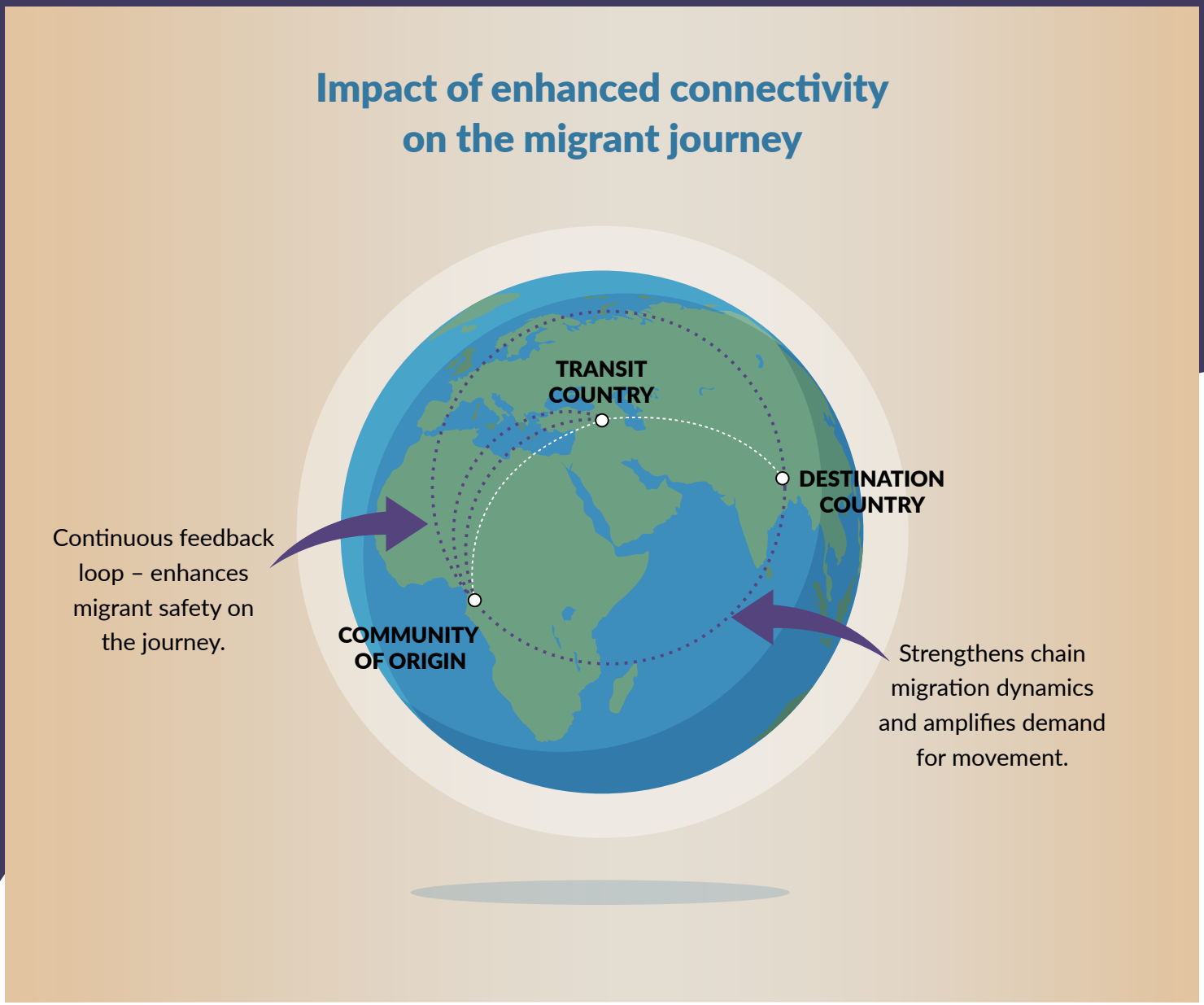


FIGURE 3 Connectivity along the journey drives aspirations in communities of origin, but also enhances migrant safety along the migrant trail.

Any action taken to address the use of social media and other digital tools by smuggling networks should be sensitive to the positive role that such platforms and modes of communication can play in enhancing the safety of the migrants on their journeys. The 'fight' against online human-smuggling markets will, as in the case of their offline counterparts, have a significant impact on the safety of migrants. Clamping down on the use of social-media platforms and messaging sites in the context of smuggling activities will limit the positive role they play in making information available to migrants, and their ability to communicate with family, fellow migrants and other people who can contribute to keeping them safer on their journeys.

THE ILLEGAL WILDLIFE TRADE

The illegal trade in endangered species and wildlife products (controlled under the Convention on International Trade in Endangered Species or CITES) is a major threat to global biodiversity and to the natural resources of many developing countries. Digitally enabled trade is a major and growing part of the international market, and is widely documented to implicate the world's major social-networking and e-commerce platforms as key sites for unimpeded illegal activity. Evidence suggests that the availability of online connections and trading platforms has driven demand across a widening base of consumers, changed the ways in which wildlife-trading networks operate, and frustrated the efforts of traditional law-enforcement approaches. Looking to the future, rapidly expanding internet access in key source countries for illegally traded species (countries such as Indonesia, which is one of the world's great biodiversity hotspots and a hub for trade in endangered reptile and parrot species) and demand countries (such as China, a major destination market for ivory and rhino horn, among other things) indicates that the role of technology will only continue to increase in importance.[113] Although growing attention is being paid to the issue – signalled, most notably, by the Global Coalition to End Wildlife Trafficking Online[114] – there appears to have been no real progress in limiting these markets.

This section draws primarily on research conducted under the Global Initiative Against Transnational Organized Crime's (GI-TOC) year-long Digital Dangers project, the aim of which was to acquire a better understanding of the unsustainable online illegal wildlife trade (IWT) and develop a foundation for its disruption.[115]

Current dynamics of the online illegal wildlife trade

Although online markets in illegal wildlife products vary greatly – encompassing everything from animal parts, such as rhino horn and pangolin scales, to live great apes destined for the pet trade[116] – a striking feature that has been observed across the board is that digitally enabled wildlife trade is conducted almost exclusively on the surface web.[117] While this may include the use of private channels and groups, it appears that the risk of law-enforcement involvement in these markets is not high enough to force illegal wildlife traders to sacrifice the marketing opportunities offered to them by the open web and to mask their activities more effectively on the dark web.[118] Illicit wildlife goods are therefore widely advertised on publicly available forums.

Trade in endangered species is routinely carried out on major social-networking platforms – including Facebook, Instagram and WhatsApp – and e-commerce platforms, such as eBay. These platforms feature prominently in reporting on the illegal wildlife trade in places as diverse as Indonesia, the UAE, Pakistan, Brazil and Madagascar (among others),[119] demonstrating the central role these countries play in the global illegal trade. This goes against the stated policies of these platforms, which prohibit users from engaging in illegal trade, and the pledges made by these companies to counter illegal trade through their sites, all of which suggests that their policies are not being enforced effectively.

At the same time, however, the focus placed on Big Tech platforms obscures the regional and local diversity in the type of platforms being used.

Our own research in Indonesia highlighted national platforms, such as Kaskus, Ceriwis and Carousell, as key sites for trade in endangered parrot species.[120] Local classified sites are also being used in other illegal-trade contexts.[121] Illegal online trade is therefore a product of broader demand and not limited solely to major social-media and e-commerce platforms.

Online illicit wildlife markets are heterogenous, ranging from small collector networks to substantial supply-chain arrangements for certain products.[122] The relationship with offline markets varies between cases: while in some instances online marketing may still be tied to transactions taking place in physical venues, in other cases trends suggest that online trade is replacing real-world markets. In many wildlife markets[123] – for example, in the case of the orchid market – players engage in both licit and illicit trade, thereby blurring the lines of legality and attempting to pass off illegally acquired specimens as legitimate.

The wide array of publicly available online material that documents illegal trade has been used by environmental NGOs to record snapshots of specific subsets of the global illegal wildlife market, including the volume and value of online advertisements present in particular jurisdictions and on certain platforms.[124] Although an estimate of the total scale of this online trade remains elusive, these studies indicate that the role played by online platforms in illegal trade is significant and fast-growing.

How the growth of digital technologies has changed market dynamics

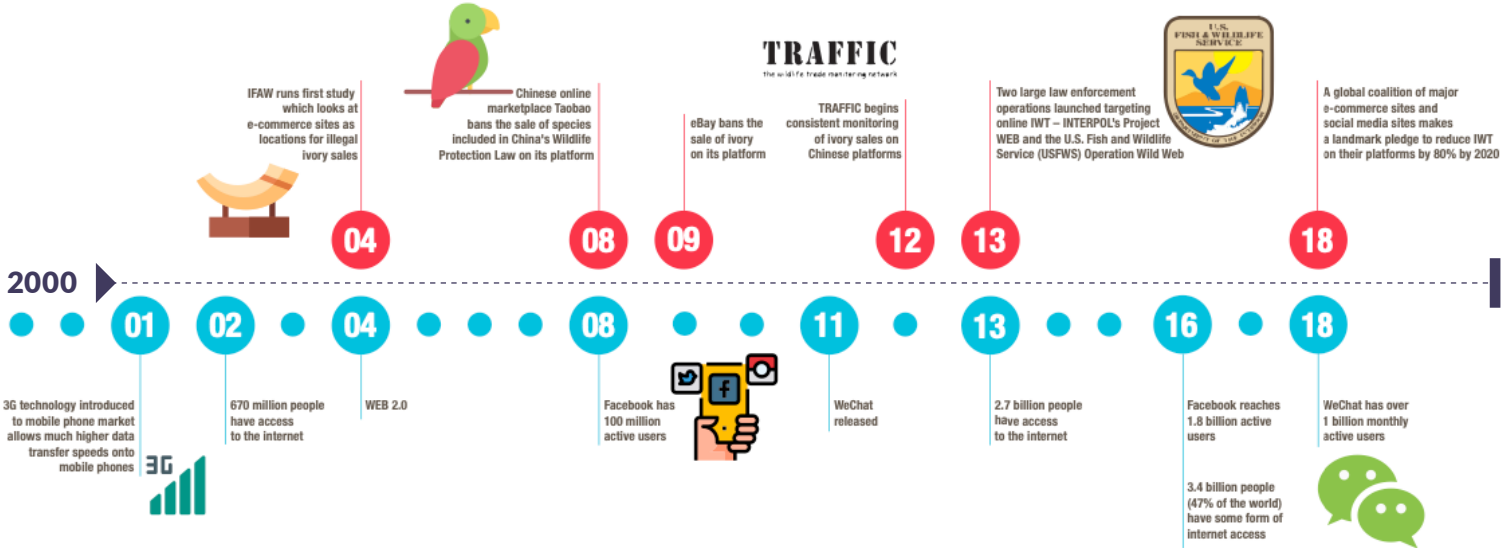
The growing importance of online transactions and marketing has had profound implications for the modus operandi of criminal players within IWT and across its consumer base. The different trading dynamics offered by online trading have given rise to new ways of conducting illegal trade practices.

The prevalence of sole traders rather than cohesive organized-crime groups is the most prominent shift in modus operandi that has been observed.[125] The ability to easily reach both suppliers and consumers allows this more individualized, flexible modus operandi to exist. Our case studies emphasized the rising role of 'agents' in social-media-based trade; people who are able to monetize the advertising of wildlife products using their own social networks and act as intermediaries in the sales process. This role either does not exist offline or else exists in a different form.[126]

The barriers to entry into the illegal wildlife trade have been lowered through the introduction of digital technology, and online marketplaces have enabled both new traders and consumers to enter the illegal wildlife trade with greater ease. Social networks facilitate transnational connections between would-be wildlife dealers and international suppliers, allowing individuals without previous links to the wildlife trade to establish themselves quickly within the market.[127] For consumers, the open advertising of wildlife products online enables the participation of the casual buyer, who otherwise would not actively seek out a specialist offline market; the open nature of trade destigmatizes the activity and reduces the extent to which it is perceived as a 'real crime'.

The supply chains for IWT have also become shorter. Connections made over social media enable criminal players and poachers within species' source regions to communicate and advertise with ease to consumers internationally. Some investigations have even documented instances of social media being used to

FIGURE 4 Digital dangers through the decades: a timeline of the online wildlife trade.



essentially commission the poaching of a particular species, bringing the demand into direct contact with the source. This phenomenon is thankfully rare.[128]

The movement online of IWT marketplaces has driven demand. For many wildlife species, legal and illegal demand is propelled by enthusiastic collectors, for whom owning rare species and unique specimens is a source of pride and prestige. Social-media platforms and marketplaces offer opportunities for collectors and dealers to network and discuss purchases (as well as to execute transactions). By feeding the enthusiasm and competitiveness of these collectors, online networks intensify the demand for rare or unusual species, and so the drive for illicit trade is increased.[129]

Legal and enforcement challenges

Although the capacity to combat online IWT is being strengthened in some countries, law-enforcement actors tackling this type of criminal activity are still forced to deal with a number of key challenges, some of which are greater with respect to IWT than they are with other illegal markets.

First, online trade has the capacity to reach across legal jurisdictions, and when met with changing local regulations concerning species that may be legally traded in one country and not in another, this means that determining the geographical location of the individuals involved, the species involved and the online platforms where the trade is being offered becomes crucial to investigations. These questions may, however, be difficult and time-consuming to answer, and this exacerbates the challenges already inherent in determining whether or not a sale is illegal, and identifying any suspects involved.[130]

Second, due to the growing volume of internet-facilitated trade, the capacity for proactive, manual monitoring of environmental markets is stretched even in well-resourced law-enforcement agencies. As online trade continues to grow, proactive monitoring will soon become unfeasible unless costly technological monitoring systems can be developed and systematically incorporated into enforcement efforts.

Law-enforcement agencies around the world are faced with a huge strain on resources, and as a result, few law-enforcement agencies can justify applying scarce resources to problems that do not affect humans (as, for example, in the way that child sexual exploitation does) and whose effects are primarily felt elsewhere (that is, in the countries where animals are poached, rather than where they are sold). Although source countries have a greater incentive to combat online IWT, they also generally have far fewer resources with which to do so. In addition to this, one needs to take into account the jurisdictional challenges raised above.[131]

In the case of sophisticated networks and high-value animal products, private communications are most widely used for conducting trade, without the products ever being advertised on open forums. Even in the case of animal trades that are less 'sensitive', products may be marketed (with varying degrees of covertness) on open forums and initial interactions between prospective buyers and sellers can appear relatively benign, but the conversations that cement the illegal transactions will always move to private channels. This limits the public evidence available to law enforcement. Criminal use of private channels poses challenges in the case of the protection of personal privacy for future innovations in the regulation of social media.[132]

The way forward

Given the complex social and economic factors driving the IWT, the limited resources available and the heterogeneity of markets trading in different species, it may be necessary to adopt several different approaches or strategies.

There is a need for improved platform compliance with regulatory frameworks. Despite the broader ongoing debate about the responsibility of major tech companies for illegal trade taking place on their platforms, many of these platforms are failing to achieve their existing commitments in the case of IWT. Future regulation placing increased responsibility on social-media platforms in the case of proactive monitoring of user-generated content could be influential in combating illicit wildlife markets.[133]

Collaboration between civil society and law enforcement needs to be enhanced. The openly available evidence of online illegal trade has already been used by environmental NGOs to research and highlight criminality. Future monitoring work by civil society could support ongoing investigations by law-enforcement units concerned with preventing wildlife-related crimes.

Law-enforcement efforts should target identified illegal practices. Considering that one of the challenges to combating IWT lies in being able to determine which products are being traded illegally, and because there are a limited number of resources available for investigations, it is essential that law enforcement target the platforms most likely to be engaged in illegal trade and focus on the species most commonly traded. This will allow scarce resources to be used most effectively. This could be done either by making use of species-specific knowledge (for example, knowing the likelihood that a particular specimen has been bred in captivity) or by employing automated systems capable of sifting for key indicators of illegal activity.[134]

Finally, awareness needs to be raised at both public and political levels with regards to IWT, and the norms surrounding it need to change. Efforts to raise awareness of the harm created by the illegal wildlife trade could encourage greater political buy-in to law-enforcement and reduction efforts, while also educating consumers about the criminality and harm of participating in IWT markets. This would hopefully lead to a change in the norms and conditions that allow the illegal trade to proliferate online.[135] Online communities could themselves play a prominent role in altering these perceptions and behaviours.

ILLICIT TRADE: A CASE STUDY IN CULTURAL PROPERTY

Illicit trade – that is, the illegal production, movement or sale of goods for which there are also legal markets – is a vast and amorphous problem. As an umbrella term, trade here can signify a range of criminal activities, ranging from piracy, counterfeiting and tax evasion, to the smuggling of genuine goods and the insertion of illegally acquired commodities into global supply chains. Illicit trade covers everything from illicit cigarette markets to the trade in counterfeit pharmaceuticals and luxury goods.

Although estimates of the value of illicit trades vary, all point to them dwarfing the scale of other criminal markets (such as those outlined in this primer), most commonly those associated with organized crime and those for which the harm created is immediately evident (such as in the case of human and drug trafficking).[136] Illicit trade contributes to eroding trust in institutions, the presence of violence and exploitation in illicit supply chains, and in some instances (such as in the case of counterfeit medicines) direct harm to consumers.

As illicit trade is a nebulous group encompassing many different commodities, it may be useful to understand it in terms of those goods that have proven the most susceptible to criminal exploitation. These include:

- aspirational goods, which are those that may convey status or would otherwise be unavailable to consumers due to their high costs (for example, counterfeit luxury goods);
- addictive substances (such as tobacco, alcohol and prescription drugs);
- illicit inputs into global supply chains for high-value commodities (such as metals and minerals) from illicit sources; and
- counterfeit forms of essential goods, such as substandard medicines.[137]

The illicit trade in goods for which there are otherwise legal markets presents a different set of policy challenges compared to the trade in illegal goods. The presence of parallel legal markets opens up a grey area where consumers are unable to differentiate between legally and illegally sourced goods, and criminal players are able to exploit this ambiguity. The emergence of online markets and the facilitation of trade by technology compounds this issue by enabling unregulated transnational trade and by connecting criminal suppliers with a ready market, providing encryption and privacy, and facilitating easy distribution of counterfeit and otherwise-illicit goods.

The dynamics involved in different forms of illicit trade vary widely, as they are shaped by the legal and regulatory structures of the relevant legal markets at national level, while also being affected by global trends in demand. For example, recent analysis of counterfeit-pharmaceutical markets has suggested that India and China (although to a lesser extent) are major source countries of counterfeit medicines consumed in Africa.[138] This dynamic is connected to legal pharmaceutical production: African nations have notably few pharmaceutical-production facilities compared to their Asian counterparts, and as a result, have become net importers of medicines both genuine and counterfeit.[139] At the same time, reports have emerged that counterfeit medicines are being packaged to emulate brands coming from the EU, as the standards enforced in the EU are internationally respected and so the counterfeit brand can ride on this reputation.[140] The enforcement of pharmaceutical standards then becomes dependent on national regulatory bodies and police forces.

Because of the intricacies involved in each individual illicit trade, it is not possible to do justice to the topic in the space of just one brief. Instead, this section focuses on one particular example – the trade in antiquities and cultural objects – to illustrate the complexities of this particular illicit market and the changing role of technology within it. In terms of the overall typology outlined above, antiquities fall under the category of 'aspirational' goods, in the sense of being art objects and collectors' items desired for their aesthetic value and ability to convey status. As a result, a comparison can be made with the collector markets that trade in exotic and high-value wildlife species, such as the illegal trade in orchids and high-value Madagascan reptiles (such as tortoises). In both instances, the desire to collect rare, high-value goods considered to be symbols of status is what shapes and drives the market.

While this market may be more highly specialized and less prevalent than, for example, that of counterfeit pharmaceuticals, cultural property is a topical and politically contentious example of illicit trade and it speaks to many of the issues relevant to other forms of illicit trade: supply-chain integrity, overlap between criminal and licit players, regulation and state enforcement capacity. However, this particular form of illicit trade brings with it a unique concern – that is, the loss of valuable cultural heritage and collective identity, primarily from developing countries and conflict zones, to wealthy consumer markets.

As a criminal market, the illegal trade in cultural property is widely acknowledged as being under-researched and therefore in need of more investigation. At the same time, a number of recent law-enforcement investigations and research projects coming out of civil society and academia

have begun to cast light on the scale and complexity of this illicit trade. The case of cultural property illustrates how illicit markets of all kinds – no matter how specialized, niche or even antiquated they may seem – are being transformed with the advent of technology and online trade.

Current dynamics of the online illegal antiquities trade

Cultural objects and archaeological sites around the world are extensively targeted for looting and illegal trade. Archaeological looting, in particular, is associated with conflict zones and forms part of the illicit trade that takes place in subsistence economies. In some instances, this trade has also been exploited by armed forces and extremist groups.[141]

The international art market has been widely described as a 'grey' market and shown to be subject to illicit trade through practices such as falsified documentation, the sale of 'unprovenanced' objects lacking the documentation to prove their (potentially illicit) origins, and underground person-to-person trade.[142]

The trafficking of antiquities is taking place widely on the surface web, involving criminal networks that interact on major social-media platforms and e-commerce sites. There is currently little concrete evidence that illegal trade in antiquities is taking place on the dark web.[143] Recently, one major study found 95 Arabic-language Facebook groups (comprising over 1 million members) trading in antiquities. These groups are managed by middlemen (who receive a fee from sales made within the group), including individuals in conflict zones, who are offering artefacts to consumers in market countries such as the US.[144] This demonstrates how online markets are used to connect buyers in destination markets with suppliers in countries that are difficult to travel to, such as conflict zones (e.g. Syria, Libya or Yemen). If COVID continues to make it more difficult to access certain regions, the practice of using online markets to circumvent travel restrictions is set to grow further.

Other studies have highlighted sales of looted objects (including objects from Egypt, Syria and India) taking place via eBay.[145] It is understood that e-commerce growth has increased sales of illegally acquired cultural objects, as many of them are sold unprovenanced. As a result, there is no control over the entry of looted objects into the market.[146]

While these public and semi-public forums offer traders the opportunity to advertise widely, closed communication channels, such as WhatsApp and Snapchat, have been described as key tools for illegal-antiquities traders in other contexts. These platforms allow for secure communication between illicit traders and established connections, including dealers within the legitimate antiquities trade.[147]

The online trade in antiquities (of dubious origin) represents a higher-volume, lower-value area of the overall market than is traditionally traded in by specialist art dealers and through established auction houses.[148] As a result of this, there is a widespread perception that the online marketplace offers traders greater anonymity and less scrutiny, as lower-value objects traded outside of the public view attract fewer questions of provenance, meaning vendors can sell trafficked antiquities with seemingly little risk.[149] There is a widespread lack of awareness and understanding of the legal restrictions around buying and selling antiquities online, not only by consumers, but also by dealers themselves.[150] The online market is also able to facilitate the widespread dissemination of fakes, as consumers include non-specialist buyers who may not be able to differentiate between a genuine and a fake article, documentation can be falsified, and physical examination of the objects is impossible. Estimates suggest that the vast majority of antiquities offered online may, in fact, be fake.[151]

In instances where the illegal antiquities trade has been highlighted, the reaction of social-media platforms has thus far been reactive rather than proactive, involving the shutting down of groups and blocking of key vendors, rather than any changes being made to platform policies.[152]

International law-enforcement cooperation dismantling antiquities-trafficking networks online

International law-enforcement investigations into antiquities-trafficking networks are rare. However, three recent major operations conducted under the auspices of Europol and INTERPOL illustrate the growing importance of online trade in this market:[153]

- Operation Pandora: led by Europol in October and November 2016, resulted in 3 561 objects being seized in an operation spanning 18 European countries. Over 400 ancient coins were recovered following investigations into suspicious online adverts.
- Operation Athena/Pandora II: coordinated by INTERPOL across 81 countries in December 2017. The recovery of over 7 000 of these objects (nearly 20% of the total seized) resulted from law-enforcement officers monitoring online marketplaces and sales sites.
- Operation Pandora III: coordinated by INTERPOL in October 2018, this focused on the online market-place as a key challenge for law enforcement with regards to this form of illicit trade. It resulted in the seizure of over 18 000 objects.

How online trade has changed the illegal antiquities trade

The online marketplace has brought about changes at each step of the supply chain, shaping demand for illegal antiquities, and affecting both the range of products available and how these goods are purchased.

Online trading has opened up the trade in dubiously sourced antiquities and cultural objects to a wide online customer base. This includes non-specialist buyers, who would, without online availability, not be engaging in this market and this generates additional demand.[154]

Lowering the barriers to entry has, in turn, shaped the kinds of items that are trafficked and looted, and the ease of online marketing and small-scale shipping has facilitated trade in lower-value looted items. This is a problem for cultural-heritage protection, as lesser-resourced archaeological sites, which might otherwise have escaped looting, become commercially viable.

Supply chains are shortened by online marketplaces, which enables connections to be formed quickly between widely dispersed players, thus allowing direct connections between vendors in source countries and consumers. In some cases, this includes vendors in conflict zones.[155] The online marketplace allows vendors to break down the barriers to trade that conflict and the disruption of legitimate means of trade and transport may otherwise pose.

While the online trade offers opportunities for public marketing, private communication channels also provide secure, discreet connections between buyers and illicit suppliers. This reduces the need for open contact between illicit and licit markets and supports the facade that traders are dealing in legitimate objects.

Legal and enforcement challenges

While there has been an increase in the number of international operations targeting antiquities-trafficking networks in recent years, cultural-property crime is still rarely considered a priority for policing. The online trade in illegally acquired antiquities poses further challenges to law enforcement, some of which are unique.[156]

The international legal frameworks and norms governing the antiquities trade (and hence shaping its illegal counterpart) are complex and evolving, comprising an interlinked set of international conventions, bilateral agreements and national laws that set out protections for specific categories of objects.[157] This complexity creates ambiguity about which objects may be legally traded, and where.

The additional complexities of establishing jurisdiction and locating and securing evidence in cases of online trade make the task of law enforcement all the more difficult. The complexities of definitively establishing which objects are genuine and which have been looted pose challenges for law enforcement. As a result, it is difficult to implement automated systems of identification and selection of such objects.

The way forward

INTERPOL, the UN Educational, Scientific and Cultural Organization (UNESCO) and the International Council of Museums developed a list of 'basic actions to counter the illicit sale of cultural objects through the internet' as early as 2006.[158] Despite this having been outlined before the proliferation of social-media platforms and their revolutionary role in facilitating informal and illicit trade, many of its recommendations are still surprisingly apposite. They include encouraging online platforms to cooperate with law enforcement and post information about cultural-object sales and legality in a prominent manner, and urging states in each case to mandate a national cultural body with the task of monitoring and verifying online sales.

Several observers of the online illicit trade have called for more responsibility to be placed on social-media platforms whose policies often do not address the sale of cultural goods.[159] This falls under the larger debate over the harm of online illicit trade and the prospective future regulation of social-media platforms. Future regulation encouraging platforms to undertake more proactive monitoring of sales through their sites could include sales of illicit cultural property. Several states have already taken steps to collaborate with internet platforms to improve regulation in this field.[160] In Germany, for example, antiquities sales via eBay must be accompanied by valid export documentation and sales are monitored by regional cultural-heritage-management bodies, thereby combining internal platform policies with external oversight.[161]

The harms associated with the online illegal trade in cultural property are fairly unique and differ significantly from those of the other illegal trades discussed in this primer. However, being able to curtail this market's vulnerability to criminal exploitation involves addressing the same key issues: the social norms governing consumer behaviour, and the need for regulation that spurs responsible action in the private sector, among those directly involved in trade and the platforms through which the trade is enacted.

Although these recommendations for a way forward are specific to cultural property as a form of illicit trade, they highlight the need for responses to illegal online markets to be commodity-specific, in order to effectively address the differing drivers, supply networks and regulatory constraints that shape each market.

THE PRIVATE SECTOR'S ROLE IN REGULATING ONLINE ILLICIT MARKETS

Social-networking sites and e-commerce platforms play a significant role in each of the illicit markets analyzed in this study. The heavy usage of social-networking and messaging sites by illicit markets has fuelled a debate regarding the role of private technology companies in regulating online illicit markets and, more broadly, the internet. We have currently reached a critical point in this debate, with the prevailing traditional free-market perspective, bolstered by private tech lobby groups, coming under fire.

Who regulates the internet?

Europe, and in particular the UK (as publicized in its Online Harms White Paper), is driving towards a 'new regulatory framework' that doesn't merely build upon existing legislative regimes, but recasts the parameters of enforcement.[162] This considers placing a new statutory duty of care on private service providers, essentially compelling the private sector to play a larger role in regulating the internet. Service providers would need to comply with a statutory code of practice, regulated by a public-sector entity, and be liable to sanctions in the case of breaching this code.[163]

In contrast to this, other jurisdictions (certainly in the developing world and arguably in the US following the Cambridge Analytica scandal, though to a lesser extent) continue to advocate for a free-market-economy model, in which it is not considered the role of private companies to regulate the internet. In other countries, most notably in China, the enhanced regulation of private-sector tech firms and data use stands in contrast to increasing government surveillance and use of citizens' data to govern society, reward compliance and punish perceived uncitizenlike behaviour.[164]

The importance of the 'tech giants' in regulating the internet and in combating the growth of cyber-crime is increasingly being recognized. In 2017, Denmark established the world's first embassy in Silicon Valley, signalling its intent to approach negotiations with these corporations as if they constituted a global superpower.[165] Casper Klynge, the Danish ambassador appointed in this case, recognizes that these corporations are no longer companies with narrow commercial roles, but rather 'de facto foreign policy actors'.[166]

Although the power of these monoliths is widely recognized, their role in combating criminal activities conducted on the platforms they operate has, to date, been voluntary rather than compelled. Having said that, increasing legal obligations on tech companies can have unintended consequences. One unfortunate side effect of increased regulation, which has already been seen in response to enhanced governance, is the consolidation of control in the hands of a small number of large operators, who can afford the enhanced compliance burden of regulations such as those outlined in the GDPR.

Regulatory capture

The power of tech giants, which constitute some of the richest companies in the world, to be able to lobby governments and achieve significant dilution of relevant regulatory frameworks is significant, and has been key in ensuring a persistently weak regulatory context for the operations of technology companies, and the online marketplace more broadly.

Although a recent upsurge in scandals involving online service providers has started to enhance public and political scrutiny of the operations of these companies in the Western context, their power to influence the shaping of the regulations governing their operations remains formidable.[167]

This can, to some extent, be tracked in the February 2020 interim UK government consultation response to the Online Harms White Paper, in which the government rowed back from a number of proposals after an overwhelming reaction from the technology sector, which submitted over 2 400 responses. However, the response remained focused on ensuring that platforms remove illegal content and continued to signal a particular focus on terrorist content and online CSE.[168]

It has also manifested in the ongoing lobbying of US regulators who are considering enacting new data-protection legislation,[169] with a number of commentators noting the significant dilution of government bills following sectoral pressure.

Monitoring and removing content on online platforms

To date, most jurisdictions do not require internet service providers to check for content relating to illicit markets. Instead, large social-networking sites, including Facebook and Google, implement internal policies regarding content that is permitted and respond to government requests for data, or for removal of content, on the basis of national laws.

A recent ruling by the European Court of Justice (ECJ) has clarified that online platforms can be compelled to remove content through orders issued by national courts (although until now this has only been tested in the context of the EU). Until recently, such domestic court orders were understood by platforms to relate only to content available within the relevant country; however, the October 2019 ECJ judgment[170] ruled that Facebook can be compelled by any one of the national courts of the EU member states to remove posts globally if they are deemed to consist of defamatory or unlawful content. This seeks to match the borderless nature of the internet and demonstrates the increasing desire of the judiciary to improve online regulation.[171]

The ECJ has gone even further in stating that EU member states can require platforms to 'apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities'.[172] Although the imposition of 'general monitoring' obligations on online service providers is prohibited by EU law,[173] the scope of this duty of care and of permitted 'specific monitoring' obligations is yet to be determined.

In September 2019, the Spanish Data Protection Authority launched an initiative tasking the public with identifying and requesting the removal of sexually explicit or violent imagery, including CSE materials, on internet platforms.[174] Where a request made to the relevant platform to remove the material is unsuccessful, or the harm of continued dissemination is deemed high, the public can contact the data-protection authority directly. They will review the request within 24 hours of receipt and, if they find the content to be harmful, will demand that the platform promptly remove this content. Failure to comply is sanctionable and platforms may face penalties for the dissemination of harmful material. Where the material indicates a crime, the authority then liaises with law enforcement in investigating. The authority has already compelled content removal by Chilean and other platforms outside of the European Economic Area, making clear that the authority's mandate extends, at least in practice, globally. Platforms have reportedly been collaborative in this initiative, possibly driven, in part, by the threat of reputational harm stemming from public awareness of non-compliance. This also demonstrates increasing collaboration between data-protection authorities, whose revenues and powers are growing, and law enforcement in regulating the internet.

Large internet service providers, including Facebook and Google, have sizable and ever-growing teams focused on removing content. These teams triage the nature of threats, with terrorist content and CSAM (albeit to a lesser extent) included in their scope of focus. However, prevalent online criminal markets, such as those pertaining to counterfeit goods or human smuggling, are not considered a priority. For example, Facebook's community standards, which aim to 'disrupt real-world harm', cite 'terrorist activity' as the first item on its list of targets, while 'organized violence or criminal activity' comes last and is only outlined in general terms.[175] While the description of criminal activities listed includes sexual exploitation and trafficking in drugs and arms, it does not include human smuggling, counterfeit operations or IWT. Although the list is

indicative rather than exhaustive, it provides some insight into the platform's priorities.

A range of image-recognition techniques, which screen images posted on sites and run them against a vast bank of images identified as being linked to illicit markets, process posts and remove suspicious content. Although ever improving, such technologies remain imperfect and have, for example, been reported to fail in distinguishing between marijuana plants and certain green vegetables,[176] resulting in the surprise removal of certain health-blogger posts.

Furthermore, while advanced in the context of screening imagery, technology used to identify and remove suspicious language material is less advanced, and as a result, social-media providers continue to employ large teams of people whose job it is to moderate such content.[177]

Data sharing by service providers with government

Enhanced coordination between government and private internet providers and social-networking platforms is required to enhance law enforcement of online markets. Governments are increasingly turning to sites with data requests – between July and December 2019, Facebook received over 140 000 data requests from governments globally, which is double the number received in the same period in 2016. The number of data requests received by Google also increased exponentially between 2016 and 2019, reaching almost 82 000 requests concerning over 175 000 user accounts (more than doubling since 2016).[178] The two companies provide data to a similar and slowly increasing proportion of government requests, 73% in the case of Facebook and 74% in the case of Google.[179]

Both organizations operate two distinct disclosure pathways. The first involves legal-process requests, which must be accompanied by legal process (such as a search warrant), provided in line with the companies' terms of service and applicable law. The second are emergency requests, answered voluntarily, which are made in cases where there is reason to believe imminent injury or death may be likely. However, compelling international tech companies to disclose information poses a significant challenge for domestic law-enforcement agencies.[180]

When considering voluntary cooperation, this is stymied in contexts where the relationship between governments and private-sector online-platform providers is poor. This is particularly acute where government practices have repeatedly utilized internet shutdowns, extreme content control and censorship, engendering significant distrust between tech companies and governments.

In the context of legal-process requests, where companies require a request to follow Mutual Legal Assistance Treaty procedures[181] and which vary depending on the incorporation jurisdiction of the relevant service provider, responses can take between three and five months, in many cases resulting in missed prosecution deadlines. The majority of requests acceded to by these two entities follow legal process. Emergency procedures only result in disclosure if they fall within the narrow criteria of the companies' terms of service, which are relatively restrictive and are more developed in relation to child-pornography and trafficking offences than to the smuggling of migrants or illegal wildlife crime (the latter, in fact, rarely qualifies as it does not relate directly to danger faced by people).

The way forward

Multi-lateral development organizations[182] and governments have both requested that private-sector internet service providers play a larger role in the regulation of online illicit markets. Judicial decision-making in the EU, the global leader with respect to privacy rights and the intertwined regulation practices of the internet, appears to be driving towards recognizing the more widespread powers of national courts and regulatory authorities to compel content removal globally.

Perhaps of greater concern to private-sector operators is a similar trend in jurisprudence, suggesting that online service providers should recognize a duty of care towards service users, which could include specific monitoring for illicit content. The private sector would far prefer public-sector authorities to continue to shoulder the burden of monitoring for content, as in the model adopted by the Spanish Data Protection Agency, than to be forced to undertake monitoring and investigation themselves, which would mean fundamentally changing regulatory structures and would require far greater resources.

As a formal government publication indicating what the future of internet regulation could look like, the UK's Online Harms White Paper is the first of its kind – and in it, the private sector is required to shoulder far greater responsibility than they have to date. This will primarily be of concern to the tech giants that increasingly dominate internet trade, as smaller rivals would be unable to conduct the kinds of monitoring activities required. This is likely to be a positive step for countering the growth of online illicit markets as traditional law-enforcement bodies, lacking resources and capacity, fall increasingly further behind criminal innovation.

OVERALL FINDINGS AND COMPARATIVE CROSS-MARKET ANALYSIS

Although each illicit market is unique and carries distinctive challenges for law enforcement and opportunities for intervention, comparative analysis of the different markets yields some key overarching similarities regarding the impact of technological innovation on market dynamics, the challenges it poses to law enforcement, and possible interventions and ways forward. It also highlights striking differences in how the various illicit markets have exploited the new opportunities offered to them by the digital world.

Some of these impacts, law-enforcement challenges and recommendations are common to each of the markets. Where this is the case, they are set out below rather than explored in the previous individual sections.

Key findings

Barriers to entry appear to have been lowered by online illicit markets for the provision of illicit goods; however, in the context of the provision of services, the impact is less clear. Where illicit services are then transformed into goods, as in the case of images resulting from child sexual exploitation, the effect is comparable. The transformation of illicit markets from network economies (where limited advertising and clandestine operations mean transactions typically occur through existing networks), which favour incumbents, to conventional markets (where dealers compete on price, quality and service) erodes the incumbent advantage and lowers barriers to entry.[183] Furthermore,

Cryptocurrencies are being used increasingly in the trafficking of drugs and persons, while remaining unreported in human smuggling and the illicit trade in cultural property.

overheads are decreased in the digital world, enabling smaller entrants to shoulder set-up costs. The differing effects on separate markets can be premised on the offline dynamics of each market. For example, each market has significantly different requirements in the case of storage and delivery dynamics. These are far simpler when the commodity involved is a type of drug, and more complex when the 'commodity' involved is a person.

The use of the dark web by online markets for trafficking illicit drugs and persons and trading in counterfeit goods is a growing phenomenon,[184] but this has not been reported to be the case with markets concerning human smuggling, IWT or the illicit trade in cultural property. In these cases, activity remains predominantly on the surface web. This reflects the nature of the commodity being traded, with inherently illicit goods being exchanged predominantly on the darknet, and those where the question of legality is less clear being exchanged predominantly on the surface web. Displacement from the surface web onto the darknet due to greater law-enforcement efforts has occurred more among 'high-priority' illicit markets. Trafficking in persons and drugs has historically featured more prominently on law-enforcement agendas than have human smuggling, IWT and the illicit trade in cultural property.

Cryptocurrencies are being used increasingly in the trafficking of drugs and persons, while remaining unreported in human smuggling and the illicit trade in cultural property,[185] and rarely reported in the case of IWT. These differences can for the most part be traced to the twin phenomena explored above – namely, differing law-enforcement patterns to date, and the inherently illicit nature of some markets. They also reflect the profile of the purchaser, with tech-savvy young consumers in Western markets (prevalent profiles in the illicit-drugs trade) likely to be more comfortable with cryptocurrencies such as Bitcoin than the majority of those consumers procuring human-smuggling services in source countries. Where cryptocurrencies are not commonly used, other internet-enabled payment systems and telephone banking are often prevalent.

Online markets enable new harm-reduction strategies to be used by some illicit markets under scrutiny, while in the case of other markets, the harm is in fact increased by the expansion of the market online. IWT and human trafficking are examples of the latter, while human smuggling (where an enhanced information flow can empower migrants to address their vulnerabilities) and illicit-drugs trafficking (where the darknet enables greater volumes of candid feedback, which arguably empower users to select safer products) fall into the former category. Misinformation is rife in both of these latter markets, complicating the analysis.

Overarching challenges to enforcement

Poor communication and coordination between state enforcement bodies and private-sector technology companies pose a challenge to law enforcement across illicit online markets. This is particularly acute in jurisdictions where the digital freedom of individuals is not protected, and governments have used 'cyber-crime' as a pretext for curtailing the rights of individuals and limiting freedom of speech and expression. This hampers the cooperation of private-sector online service providers

with state law-enforcement bodies, and creates significant harm in the name of enhanced cyber security. Furthermore, cooperation in the case of certain illicit markets, including human trafficking, is more established and falls within the terms of service of service providers more comfortably than in the cases of other illicit markets, such as IWT or migrant smuggling.

Existing legal frameworks are insufficient to ensure illicit online activity is appropriately regulated,[186] and more stringent legislation governing cyber-security is required, including regulation of the IoT market. However, beyond creating more laws, it is important to consider which entities should be responsible for monitoring compliance of these laws and enforcing them. Traditionally this has been the role of the state, carried out by law-enforcement actors. But, as the complexity of online markets increases, some argue that technology companies, as the only entities empowered with the appropriate tools and resources, should be the ones required by legislation to police the online environment.

Legal frameworks are fragmented, including those governing the use of electronic evidence in court, complicating cross-border investigations. While cross-border data flows continue to increase, judicial and law-enforcement authorities struggle to access electronic evidence relating to criminal investigations. This is particularly true as such evidence is increasingly available exclusively on private infrastructures. Where these are either located outside the territory of the investigating country, or owned by service providers established outside this territory, obtaining such evidence can be difficult or even impossible. Delays in seizing the relevant evidence mean it is often destroyed or moved before cross-border sharing processes are completed. Even where electronic evidence is gathered and used in prosecutions, poor understanding among many members of the judiciary undermines its usefulness.

Law-enforcement agencies lack the capacity and resources to utilize technology to counter online illicit markets, and are struggling globally to develop the specialized legislation and law-enforcement skills that cybercrime requires. Even the wealthiest countries in the world do not have enough police staff trained in online forensics to deal with the wide variety of crimes being committed online, from credit-card fraud and sextortion, to drug trafficking on the dark web and the trade in rare and endangered species.

Blockchain technology enables criminal operators to conduct online transactions anonymously and securely at low costs. In the past, credit-card and web-browser histories have made financial transactions harder to conceal online, but cryptocurrencies, the dark web and Tor browsers (which bounce web traffic between a multitude of servers, creating layers of encryption) are changing that. The cryptographic keys and digital wallets of cryptocurrencies enhance the anonymity of users and exist entirely electronically and independently of a central bank, thus making it exceptionally difficult for law enforcement and investigators to trace.[187] Most governments do not appear to be considering banning cryptocurrencies (now recognized as a formal form of currency in many jurisdictions) or Tor browsers, as these can be used for licit as well as illicit means (the latter was famously used during the Arab Spring). Although some countries have tried to prohibit the use of these technologies – for example, China, which tried to ban the use of Tor browsers – they have been unsuccessful.

The 2017 closure of a number of large dark-web markets triggered the fragmentation of platforms into smaller and more local ones (including some that make exclusive use of local languages rather than English), demonstrating the flexibility of the darknet market.[188] This trend towards an increasingly unconsolidated market composed of large numbers of small platforms is predicted to continue.[189] The proliferation of a multitude of smaller markets places a greater investigative burden on law-enforcement bodies, as the impact of any one shutdown is less significant.

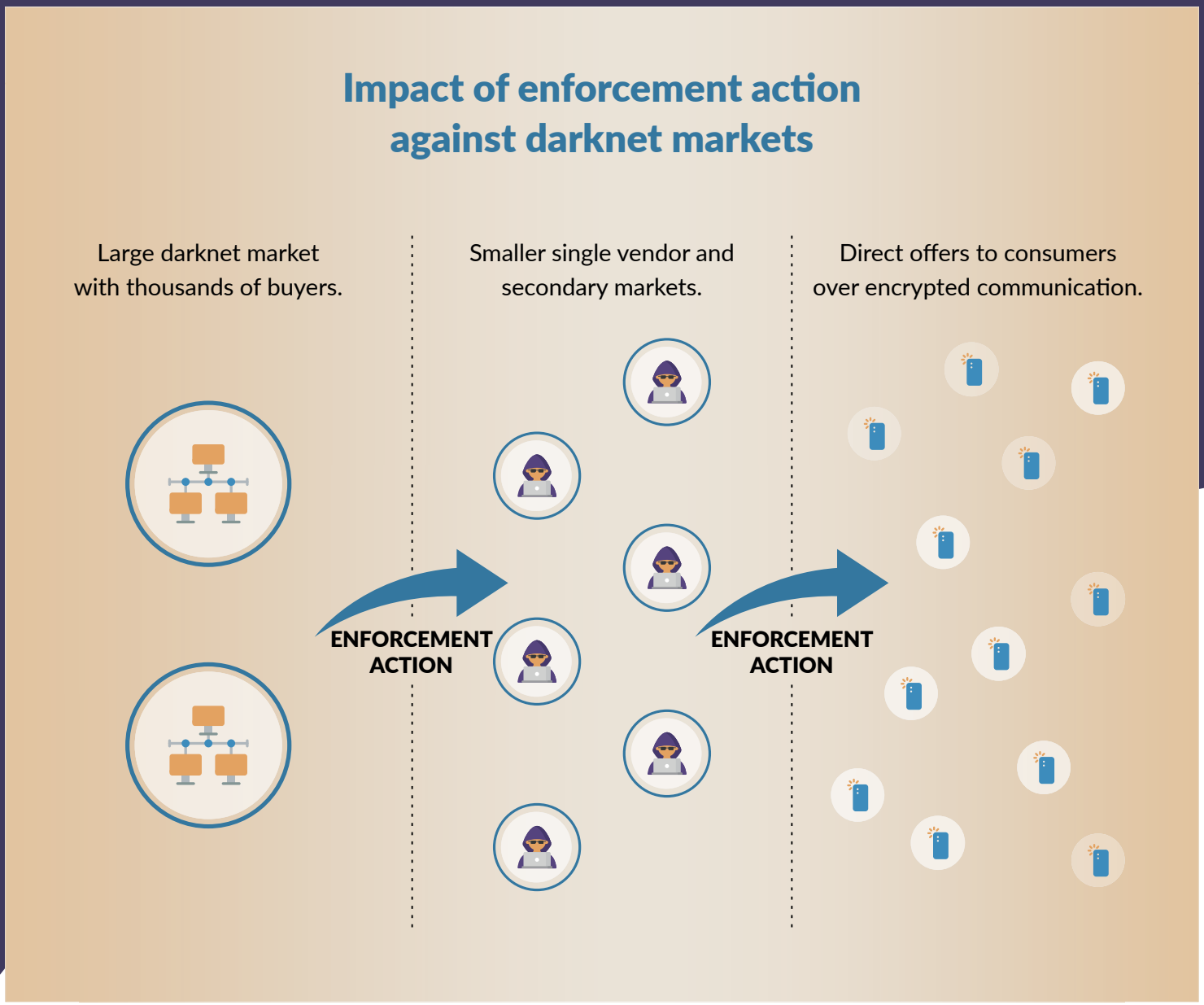


FIGURE 5 Impact of enforcement on darknet markets.

Global data-protection regimes enshrine the privacy of individuals, but pose a significant challenge to data collection and analysis in online markets, particularly where the data exists on a user's private account (which it typically does) or is considered to be 'personal data'[190] (which it typically is). Global data-protection regimes include wide carve-outs for law-enforcement activities, but forces must navigate a formal legal process to access the data they require. Not only has this placed an additional substantial administrative burden on law-enforcement agencies, but it has also created significant delays in investigations. By the time the legal process has been concluded, the data requiring investigation may no longer exist.[191] Data-protection concerns also hinder the sharing of personal data by social-media companies with law enforcement, particularly in jurisdictions where governments practise forms of online censorship and are in the habit of requesting the data of site users who have been deemed 'offenders' by the state in question.

The growing use of encryption technologies, in part driven by increasing privacy concerns, poses a significant investigation challenge. Facebook's 2019 announcement that it was considering introducing end-to-end encryption for Facebook Messenger and Instagram, is a move in this direction.[192] Encryption has already been shown to be a major obstacle in criminal investigations – for example, in the case of an investigation into a drug-trafficking network in Brazil, where courts fined Facebook (as WhatsApp's parent company) for refusing to share data (protected by the app's end-to-end encryption) that was considered relevant to the investigation.[193]

The introduction and growth of 5G communication technology further complicates investigations. Envisaged to launch worldwide in 2020, 5G is expected to match the growth in IoT devices and meet the increasing demand for faster and more reliable connections for all devices, propelled by users' communication needs.[194] However, 5G's ability to simultaneously download data from multiple sources will complicate law-enforcement investigations by making identification of the device and source more difficult. This will apply particularly in the case of tracing advertisements for illicit products, or tracking CSAM shared in member-only forums, both on the surface web and on the dark web.[195]

The way forward

Continuing investment is needed in artificial intelligence (AI), blockchain and other digital technologies to combat the growth in cyber-enabled, and indeed cyber-dependent, organized crime. Developments such as the EU-funded programme TENSOR, an AI tool for identifying and collecting electronic evidence, are promising and could significantly speed up investigative efforts.[196] However, this needs to be accompanied by an acceleration in the regulation of digital technologies and marketplaces, in part to mitigate the opportunities that these developments present to criminal organizations. Similarly, digital innovation needs to be crime sensitive and developers need to consider how new devices and applications could be exploited by criminals, prior to their market launch. This would promote 'crime-sensitive innovation', and easily mitigated vulnerabilities could be addressed quickly in the development phase. This could mimic the approach taken by the GDPR in the context of data protection, which requires privacy to be built into programmes, devices and new technologies at the design phase, with significant penalties for developers who fail to do so.

Awareness campaigns can help shape online social norms governing consumer behaviour. The increased sense of anonymity and enhanced impunity encourages users who would not normally participate in offline illicit markets to participate in those online. Awareness campaigns aimed at reversing this trend may therefore yield some positive results. In the context of online child sexual exploitation, some law-enforcement agencies have set up fake adverts for CSE so that when a buyer contacts the number posted in these adverts, a chatbot automatically replies with a message saying that buying online child-sexual-exploitation services is a crime, and refers them to specific hotlines in case they are in need of counselling services. These messages are sent with a time-delay so that buyers cannot identify which adverts

generate this reply. Similar techniques could be used in other markets – for example, with regards to IWT, would-be purchasers could be informed of the devastation their purchases are bringing on the particular species or environment concerned.

Law-enforcement bodies need to bolster their capacity to work efficiently within data-protection regulatory frameworks, and the role of privacy regimes in countering the spread of compromised personal data (which is crucial to a range of cyber-enabled crimes, such as fraud, phishing and identity theft) should be recognized and communicated to the public through awareness campaigns. The global trend in privacy regimes – with Europe positioning itself as a pioneer in data-protection regulation with the enactment of the GDPR in 2016, and jurisdictions worldwide following suite – suggests that they will become increasingly pivotal in online regulation.

Electronic communication services, the cloud and internet-infrastructure service providers are also essential in countering the growing online presence of illicit markets. Social-networking platforms perform key roles in online organized-crime markets, straddling surface-web channels in their public-facing interface with those of the deep web, through private-messaging functions. The combination of direct commercial-transaction capabilities and the marketing functionality performed by the platforms means that in some cases, these platforms act as a one-stop shop for criminal operations. Enhanced detection of illicit activity and improved coordination with law enforcement could transform such platforms into entry points for online investigations. The 'duty of care' of such platforms towards users needs to be explicitly recognized in regulations governing their operations, and states should consider analyzing the cost benefits of imposing requirements on consumer-facing platforms to monitor for and remove illicit content.

Furthermore, there needs to be continued exploration into legislative measures and judicial-cooperation structures to streamline cross-border sharing of e-evidence in criminal investigations. This has already been identified as a priority at the EU level.[197] At an international level, negotiations regarding a Second Additional Protocol to the Convention on Cybercrime of the Council of Europe (CETS No. 185, also known as the Budapest Convention) were concluded in December 2019, the focus of these also being on enhancing the sharing of cross-border e-evidence in criminal investigations.

Finally, given the significant resource constraints faced by law enforcement in tackling the growth of cyber-enabled crime, available resources should be focused on interventions that can maximize impact through a harm-reduction lens. This may exclude interventions that have been shown to merely fragment the marketplace.

NOTES

1 Dr Mike McGuire, Samantha Dowling, Cyber crime: A review of the evidence, Chapter 2: Cyber-enabled crimes – fraud and theft, Home Office Research Report 75, October 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf.

2 Simon Kemp, Digital 2019: Global internet use accelerates, We Are Social, 30 January 2019, https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

3 Europol, The relentless growth of cybercrime, 27 September 2016, https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime.

4 Ibid.

5 International Telecommunication Union, Statistics: Individuals using the Internet, 2005–2019, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

6 GSMA, The state of mobile internet connectivity 2019, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/GSMA-State-of-Mobile-Internet-Connectivity-Report-2019.pdf.

7 Online discussion with law enforcement specializing in gangs, Honduras, 1 April 2020.

8 RAND Europe, The role of the 'dark web' in the trade of illicit drugs, Research brief, 2016, https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9900/RB9925/RAND_RB9925.pdf.

9 Ibid., p 3.

10 Channing Mavrellis, Transnational crime and the developing world, Global Financial Integrity (GFI), 27 March 2017, https://gfintegrity.org/report/transnational-crime-and-the-developing-world.

11 UN Office on Drugs and Crime (UNODC), Executive Summary, World Drug Report 2019, p 55.

12 Martin Dittus, Joss Wright and Mark Graham, Platform criminalism: The 'last-mile' geography of the Darknet market supply chain, WWW '18: Proceedings of the 2018 World Wide Web Conference, April 2018, pp 277–286, https://arxiv.org/pdf/1712.10068.pdf.

13 UNODC, World Drug Report 2018.

14 Jane Mounteney, Alessandra Bo and Alberto Oteo, The internet and drug markets, European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf.

15 Liz McCulloch and Scarlett Furlong, DM for Details: Selling drugs in the age of social media, Volteface, September 2019, https://volteface.me/publications/dm-details-selling-drugs-age-social-media.

16 This is according to a January 2019 poll of over 2 000 people between the ages of 16 and 24 conducted by Survation, commissioned by Volteface; see Liz McCulloch and Scarlett Furlong, DM for Details: Selling drugs in the age of social media, Volteface, September 2019, https://volteface.me/publications/dm-details-selling-drugs-age-social-media.

17 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

18 RAND Europe, The role of the 'dark web' in the trade of illicit drugs, Research brief, 2016, https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9900/RB9925/RAND_RB9925.pdf.

19 As cited in, and supported by, Martin Dittus, Joss Wright and Mark Graham, Platform criminalism: The 'last-mile' geography of the Darknet Market Supply Chain, WWW '18: Proceedings of the 2018 World Wide Web Conference, April 2018, pp 277–286.

20 Ibid.

21 Ibid.

22 Lukas Norbutas, Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network, *International Journal of Drug Policy*, 56, 2018, pp 92–100.

23 Martin Dittus, Joss Wright and Mark Graham, Platform criminalism: The 'last-mile' geography of the Darknet Market Supply Chain, WWW '18: Proceedings of the 2018 World Wide Web Conference, April 2018, pp 277–286.

24 Diana S Dolliver, Steven P Ericson, and Katherine L Love, a geographic analysis of drug trafficking patterns on the TOR Network, *Geographical Review*, 108, 1, 2018, pp 45–68.

25 Martin Dittus, Joss Wright and Mark Graham, Platform Criminalism: The 'last-mile' geography of the Darknet Market Supply Chain, WWW '18: Proceedings of the 2018 World Wide Web Conference, April 2018, pp 277–286.

26 UNODC, Executive Summary, World Drug Report 2019, pp 51–52.

27 RAND Europe, The role of the 'dark web' in the trade of illicit drugs, Research brief, 2016, https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9900/RB9925/RAND_RB9925.pdf.

28 Ibid.

29 Nathaniel Popper, Dark web drug sellers dodge police crackdowns, *The New York Times*, 11 June 2019, https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html.

30 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
31 Ibid.
32 Email correspondence with expert in drugs trafficking, 9 April 2020.
33 Ibid.
34 Tom Wainwright, *Narconomics: How to Run a Drug Cartel*. London: Penguin, 2017, p 198.
35 Liz McCulloch and Scarlett Furlong, DM for Details: Selling drugs in the age of social media, Volteface, September 2019, https://volteface.me/publications/dm-details-selling-drugs-age-social-media.
36 Justin Rohrlich and Hanna Kozlowska, Drug traffickers are recruiting smugglers on Facebook, Quartz, 1 August 2019, https://qz.com/1680134/facebook-ads-are-being-used-to-recruit-drug-smugglers.
37 Liz McCulloch and Scarlett Furlong, DM for details: Selling drugs in the age of social media, Volteface, September 2019, https://volteface.me/publications/dm-details-selling-drugs-age-social-media.
38 RAND Europe, The role of the 'dark web' in the trade of illicit drugs, Research brief, 2016, https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9900/RB9925/RAND_RB9925.pdf, p 6.
39 Liz McCulloch and Scarlett Furlong, DM for details: Selling drugs in the age of social media, Volteface, September 2019, https://volteface.me/publications/dm-details-selling-drugs-age-social-media.
40 EMCDDA and Europol, Drugs and the darknet: Perspectives for enforcement, research and policy, EMCDDA–Europol Joint publications, Luxembourg, 2017, p 28.
41 Assessment based on collection and analysis of data and information extracted from eight of the largest darknet markets during January 2016. RAND Europe, The role of the 'dark web' in the trade of illicit drugs, Research brief, 2016, p 5.
42 Ibid.
43 The increasing use of small parcel delivery services has also been tracked in the context of counterfeits and other forms of illicit trade. See OECD, Misuse of small parcels for trade in counterfeit goods: Facts and trends, 12 December 2018, https://www.oecd.org/governance/misuse-of-small-parcels-for-trade-in-counterfeit-goods-9789264307858-en.htm.
44 Tom Wainwright, *Narconomics: How to Run a Drug Cartel*. London: Penguin, 2017, p 202.
45 Josh Constine, Facebook cracks down on opioid dealers after years of neglect, TechCrunch, 16 August 2018, https://techcrunch.com/2018/08/16/facebook-opioid-searches.
46 Liz McCulloch and Scarlett Furlong, DM for details: Selling drugs in the age of social media, Volteface, September 2019, https://volteface.me/publications/dm-details-selling-drugs-age-social-media.
47 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
48 UNODC, World Drug Report 2019, p 53.
49 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
50 UNODC, World Drug Report 2019, p 54.
51 Nathaniel Popper, Dark web drug sellers dodge police crackdowns, *The New York Times*, 11 June 2019, https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html.
52 Ibid.
53 Tom Wainwright, *Narconomics: How to Run a Drug Cartel*. London: Penguin, 2017, p 214.
54 As defined by the UN Convention against Transnational Organized Crime's Protocol to Prevent, Suppress and Punish Trafficking in Persons, human trafficking is 'the recruitment, transport, transfer, harbouring or receipt of a person by such means as threat or use of force or other forms of coercion, abduction, fraud or deception for the purpose of exploitation.' Several different crimes therefore fall under this banner, including trafficking for sexual and labour exploitation, forced criminal activity, forced begging, forced marriages, forced removal of organs, and the trafficking of children for use as child soldiers. See UNODC, What is human trafficking?, https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html.
55 ILO, Profits and poverty: The economics of forced labour, Geneva, 2014. https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_243391.pdf.
56 Ibid.
57 The figure is 7.6 per 1 000 people. See International Labour Office (ILO), Global estimates of modern slavery: Forced labour and forced marriage, 2017, https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_575479.pdf.
58 The figure is 6.1 per 1 000 people. However, Asia and the Pacific account for the largest number of forced labourers at 15.4 million (62% of the global total). See ILO, Global estimates of modern slavery: Forced labour and forced marriage, Geneva, 2017, https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_575479.pdf.
59 The figure is 3.9 per 1 000 people. See ILO, Global estimates of modern slavery: Forced labour and forced marriage, Geneva, 2017, https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_575479.pdf.
60 Michael H Keller and Gabriel JX Dance, The internet is overrun with images of child sexual abuse. What went wrong? *The New York Times*, 28 September 2019, https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.
61 Europol, Linkedin, child sexual exploitation, https://www.linkedin.com/feed/update/urn:li:activity:6651798977517764608/.
62 Ibid.
63 FBI officials quoted in the *San Diego Union Tribune*, FBI warns of increased child-exploitation risks during COVID-19 crisis, 1 April 2020, https://www.sandiegouniontribune.com/news/public-safety/story/2020-04-01/fbi-warns-of-increased-child-exploitation-risks-during-covid-19-crisis.
64 UN Global Initiative to fight human trafficking, 017 Workshop: Technology and Human Trafficking, background paper, Vienna Forum to Fight Human Trafficking, 2008, https://www.unodc.org/documents/human-trafficking/2008/BP017TechnologyandHumanTrafficking.pdf.

65 BBC News, Kik messenger app to shut down, 24 September 2019, https://www.bbc.com/news/technology-49809449.
66 BBC News, Instagram biggest for child grooming online – NSPCC finds, 1 March 2019, https://www.bbc.com/news/uk-47410520.
67 International Trade Union Confederation, Mini action guide: Forced labour, 2008, https://www.ituc-csi.org/IMG/pdf/guide_forced_labour_EN.pdf.
68 Stop It Now, How people use the internet to sexually exploit children and teens, https://www.stopitnow.org/ohc-content/how-people-use-the-internet-to-sexually-exploit-children-and-teens.
69 Kaiser Larsen, Thorn collaborates with Amazon Rekognition to help fight child sexual abuse and trafficking, Amazon Web Services Machine Learning Blog, https://aws.amazon.com/blogs/machine-learning/thorn-partners-with-amazon-rekognition-to-help-fight-child-sexual-abuse-and-trafficking.
70 Andy Brown, Safe from harm: Tackling online child sexual abuse in the Philippines, UNICEF, 19 October 2016, https://www.unicef.org/protection/philippines_91214.html.
71 Jessica Formoso, Human trafficking on the dark web and beyond, FOX 5 New York, 27 September 2017, https://www.fox5ny.com/news/human-trafficking-on-the-dark-web-and-beyond.
72 TOR is a free and open-source software programme for enabling anonymous communication. The name is an acronym of the original project name, The Onion Router. See Bingdong Li et.al., An Analysis of Anonymity Technology Usage, International Workshop on Traffic Monitoring and Analysis 2011, Lecture Notes in Computer Science, 6613, edited by J Domingo-Pascual, Y Shavitt and S Uhlig, pp 113–116.
73 Nikita Malik, When it comes to child sexual exploitation, we cannot ignore the darknet, *Forbes*, 4 September 2018. https://www.forbes.com/sites/nikitamalik/2018/09/04/when-it-comes-to-child-sexual-exploitation-we-cannot-ignore-the-darknet/#62708606de6a.
74 Europol, IOCTA 2014, 29 September 2014, p 11, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014.
75 Europol, Exploring tomorrow's organised crime, 2 March 2015, https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime.
76 The Internet of Things (IoT) is 'a system of interrelated computing devices' provided with unique identifiers and 'the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction'; see Margaret Rouse, Internet of things (IoT), IoT Agenda, https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.
77 UNODC, Study on the effects of new information technologies on the abuse and exploitation of children, May 2015, https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.
78 Europol, IOCTA 2017, 27 September 2017. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017.
79 Blockchain is an incorruptible digital ledger of economic transactions. See Ameer Rosic, What is Blockchain technology? A step-by-step guide for beginners, Blockgeeks, 2016, https://blockgeeks.com/guides/what-is-blockchain-technology.
80 Thorn, Survivor insights: The role of technology in domestic minor sex trafficking, January 2018, http://gracehaven.me/uploads/default/Thorn_Survivor_Insights_061118.pdf.
81 The EU General Data Protection Regulation (GDPR) went into effect on 25 May 2018, requiring companies that gather, process or hold European residents' personal data, to be subject to certain data privacy and protection requirements.
82 WHOIS is a query and response protocol used for querying databases that store the registered users of an internet resource, including domain names and IP addresses. See L Daigle, WHOIS Protocol Specification, September 2004, https://tools.ietf.org/html/rfc3912; and European Commission, Impact Assessment, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN.
83 Dave Evans, The Internet of Things: How the next evolution of the internet is changing everything, CISCO White Paper, April 2011, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
84 Rebecca Joseph, Wi-Fi baby monitor hacked: Parents wake up to voice threatening to kidnap their child, *Global News*, 21 December 2018, https://globalnews.ca/news/4785542/wifi-baby-monitor-hacked-kidnap.
85 Businesses, knowingly or unwittingly, can become either the 'facilitators' or 'targets' of human trafficking. See Robin Cartwright and Frances Cleland-Bones, Transnational organized crime and the impact on the private sector: The hidden battalions, GI-TOC, December 2017, https://globalinitiative.net/transnational-organized-crime-and-the-impact-on-the-private-sector-the-hidden-battalions.
86 A recent study found that 71% of companies believe that modern slavery is likely to be occurring in their supply chains. See Quintin Lake, Nadine Page, Matthew Gitsham and Jamie MacAlister, Corporate approaches to addressing modern slavery in supply chains: A snapshot of current practice. 360° *The Ashridge Journal*, Spring 2016, pp 14–21.
87 See http://www.polcyb.org.
88 See https://www.hightechcrimecops.org.
89 See http://virtualglobaltaskforce.com.
90 See https://www.bsr.org/en/collaboration/groups/tech-against-trafficking.
91 Europol, Exploring tomorrow's organised crime, 2 March 2015, https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime.
92 Nicole Lindsey, New IoT security laws seek to protect consumers from hacks of internet-connected devices, *CPO Magazine*, 10 May 2019, https://www.cpomagazine.com/data-protection/new-iot-security-laws-seek-to-protect-consumers-from-hacks-of-internet-connected-devices; and UK Government, Plans announced to introduce new laws for internet connected devices, 1 May 2019, https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices.

93 Hannah Darnton and Thi Hoang, Accelerating the use of tech to combat human trafficking, GI-TOC, 30 April 2019, https://globalinitiative.net/accelerating-the-use-of-tech-to-combat-human-trafficking.
94 Agencia Española de Proteccion de Datos, Canal Prioritario, https://www.aepd.es/canalprioritario.
94 Facebook conference, London, March 2019.
95 Europol, Migrant smuggling in the EU, 22 February 2016, https://www.europol.europa.eu/publications-documents/migrant-smuggling-in-eu.
96 UNODC, Global study on smuggling of migrants, June 2018, https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2018_web_small.pdf.
97 For example, the European Migrant Smuggling Centre (EMSC), in partnership with Europol's EU Internet Referral Unit, assessed over 800 pieces of internet content containing migrant-smuggling-related information in 2018, referring 764 to service providers for removal, with a success rate of 99%. See Europol, EMSC 3rd Annual Activity Report – 2018, 25 March 2019, https://www.europol.europa.eu/publications-documents/emsc-3rd-annual-activity-report-––2018.
98 Lucia Bird, The future of human smuggling in Africa: Creating a new criminal economy?, ENACT, forthcoming.
99 DataReportal, Hootsuite and We Are Social, Digital 2019: Q3 Global Digital Statshot, https://datareportal.com/reports/digital-2019-q3-global-digital-statshot.
100 Ibid.
101 Interview with key informant (international law-enforcement professional), by telephone, August 2019.
102 Tuesday Reitano and Lucia Bird, Understanding contemporary human smuggling as a vector in migration, GI-TOC, May 2018, https://globalinitiative.net/understanding_human_smuggling.
103 Mark Shaw, Africa's changing place in the global criminal economy, ENACT, September 2017, https://enactafrica.org/research/continental-reports/africas-changing-place-in-the-global-criminal-economy.
104 Christopher Horwood and Tuesday Reitano, A perfect storm? Forces shaping modern migration and displacement, GI-TOC, May 2016, https://globalinitiative.net/a-perfect-storm-forces-shaping-modern-migration-displacement.
105 Frank Laczko and Marzia Rango, Can big data help us achieve a 'migration data revolution'? *Migration Policy Practice*, 4, 2 (2014), pp 20–29.
106 European Migrant Network (EMN), The use of social media in the fight against migrant smuggling, EMN Inform, European Commission, 2016, https://www.emn.at/wp-content/uploads/2018/05/EMN-Inform-2016_Social-Media-in-the-Fight-Against-Migrant-Smuggling.pdf.
107 VoIP permits voice communications over the internet.
108 Patrick Kingsley, People smugglers using Facebook to lure migrants into 'Italy trips', *The Guardian*, 9 May 2015, https://www.theguardian.com/world/2015/may/08/people-smugglers-using-facebook-to-lure-migrants-into-italy-trips.
109 Some technology companies are trying to play a role in enhancing information flow for migrants. Google, for example, has collaborated with the International Rescue Committee and Mercy Corp to create Crisis Info Hub, an open-source app that provides location-specific information for refugees about services, providers, shelters and transportation.
110 Interview with key informant, Egypt, September 2019.
111 Europol, EMSC 3rd Annual Activity Report – 2018, 25 March 2019, https://www.europol.europa.eu/publications-documents/emsc-3rd-annual-activity-report-––2018.
112 EMN, The use of social media in the fight against migrant smuggling, EMN Inform, European Commission, 2016, p 6.
113 Internet access via smartphone in Indonesia is currently experiencing double-digit growth and is set to increase to almost 40% by 2021. (Data taken from Statista; more information on internet and social-media access in Indonesia can be found at https://www.statista.com.) As of December 2017, mainland China had 772 million internet users, but an internet penetration rate of only 54.6%, making it both the largest online market in the world and one with immense room for growth; see Internet World Stats, Usage and Population Statistics, https://www.internetworldstats.com/stats.htm.
114 According to the World Wildlife Fund (WWF), as part of this coalition 'WWF and partners are collaborating with companies across continents, such as eBay, Google, Microsoft and Tencent, to unite the industry and maximize impact for reducing wildlife trafficking online.' See WWF, Coalition to End Wildlife Trafficking Online, https://www.worldwildlife.org/pages/coalition-to-end-wildlife-trafficking-online.
115 Simone Haysom, In search of cyber-enabled disruption: Insights from the Digital Dangers project, GI-TOC, February 2019, https://globalinitiative.net/in-search-of-cyber-enabled-disruption.
116 Christine Clough and Channing May, Illicit financial flows and the illegal trade in great apes, GFI, 1 October 2018, https://gfintegrity.org/report/illicit-financial-flows-and-the-illegal-trade-in-great-apes.
117 Currently there is little to no trading taking place on the dark web, although research by INTERPOL suggests that it still requires monitoring. See Tania McCrea-Steele, INTERPOL research says illegal wildlife trade exists on Darknet, International Fund for Animal Welfare (IFAW), 14 June 2017, https://www.ifaw.org/united-kingdom/news/interpol-research-says-illegal-wildlife-trade-exists-darknet.
118 Felipe Thomaz, Illicit wildlife markets and the dark web: A scenario of the changing dynamics, GI-TOC, November 2018, https://globalinitiative.net/illicit-wildlife-markets-and-the-dark-web.
119 Aldem Bourscheit, *300 grupos de WhatsApp estão ligados ao tráfico de animais me todo o país*, The Intercept Brasil, 10 October 2018, https://theintercept.com/2018/10/10/grupos-whatsapp-trafico-de-animais (translated using Google Translate); Haniya Javed, The untamed market for wild animals in Pakistan, Herald, 30 November 2018, https://herald.dawn.com/news/1398726.
120 Indah Budiani and Febri Raharningrum, Illegal online trade in Indonesian parrots, GI-TOC, September 2018, https://globalinitiative.net/indonesian_parrots.
121 For example, this study on the role of online intermediaries in illegal ivory markets in Nigeria: Taiwo Alimi, Yahoo Boys: Nigeria's newest players in the illegal ivory trade, *The Nation*, 25 November 2018, http://thenationonlineng.net/yahoo-boys-nigerias-newest-players-illegal-ivory-trade.
122 Felipe Thomaz, Illicit wildlife markets and the dark web: A scenario of the changing dynamics, GI-TOC, November 2018, https://globalinitiative.net/illicit-wildlife-markets-and-the-dark-web.

123 Amy Hinsley, The role of online platforms in the illegal orchid trade from South East Asia, GI-TOC, September 2018, https://globalinitiative.net/illegal_orchid_trade.
124 For example, this recent report: Jo Hastie, Disrupt: Wildlife cybercrime – Uncovering the scale of online wildlife trade, IFAW, 2018, https://www.ifaw.org/united-kingdom/online-wildlife-trade-2018.
125 This has been observed in both investigations of specific markets – see Siv Rebekka Runhovde, Illegal online trade in reptiles from Madagascar, GI-TOC, September 2018, https://globalinitiative.net/illegal-online-trade-in-reptiles-from-madagascar; and Amy Hinsley, The role of online platforms in the illegal orchid trade from South East Asia, GI-TOC, September 2018, https://globalinitiative.net/illegal_orchid_trade – and in research looking at online wildlife trafficking in its entirety – see Anita Lavorgna, The social organization of pet trafficking in cyberspace, *European Journal on Criminal Policy and Research*, 21, 3, 2015, pp 353–370.
126 Indah Budiani and Febri Raharningrum, Illegal online trade in Indonesian parrots, GI-TOC, September 2018, https://globalinitiative.net/indonesian_parrots.
127 See a journalistic investigation supported by the Digital Dangers project that documented the sourcing of lion cubs from South Africa by new entrants into the wildlife market in Pakistan: Haniya Javed, The untamed market for wild animals in Pakistan, *Herald*, 30 November 2018, https://herald.dawn.com/news/1398726.
128 See the Digital Dangers investigation of WhatsApp groups dedicated to the wildlife trade in Brazil: Aldem Bourscheit, *300 grupos de WhatsApp estão ligados ao tráfico de animais me todo o país*, The Intercept Brasil, 10 October 2018, https://theintercept.com/2018/10/10/grupos-whatsapp-trafico-de-animais.
129 See Siv Rebekka Runhovde, Illegal online trade in reptiles from Madagascar, GI-TOC, September 2018, https://globalinitiative.net/illegal-online-trade-in-reptiles-from-madagascar; and Amy Hinsley, The role of online platforms in the illegal orchid trade from South East Asia, GI-TOC, September 2018, https://globalinitiative.net/illegal_orchid_trade.
130 For a comprehensive overview of the legal challenges faced by law enforcement in cases involving transnational online wildlife crime see: James Wingard and Maria Pascual, Catch me if you can: Legal challenges to illicit wildlife trafficking over the internet, GI-TOC, July 2018, https://globalinitiative.net/legal-challenges-to-preventing-iwt-online.
131 Personal correspondence with numerous people working either in law enforcement or in international bodies concerned with cybercrime; Simone Haysom, In search of cyber-enabled disruption: Insights from the Digital Dangers project, GI-TOC, February 2019, https://globalinitiative.net/in-search-of-cyber-enabled-disruption.
132 Ibid.
133 See proposals from the UK Government's Online Harms White Paper, 8 April 2019, https://www.gov.uk/government/consultations/online-harms-white-paper.
134 For examples, see Enrico Di Minin et al, A framework for investigating illegal wildlife trade on social media with machine learning, Conservation Biology, 33, 1 (2019), pp 210–213; and Alexander Loos and Andreas Ernst, An automated chimpanzee identification system using face detection and recognition, *EURASIP Journal on Image and Video Processing*, 49, 2013.
135 For greater detail on this complex discussion see: Reducing demand for illegal wildlife products, the guide produced in September 2018 by TRAFFIC, WWF, Imperial College Business School and the Oxford Martin Programme on Illegal Wildlife Trade; Daniel WS Challender et al, Towards informed and multi-faceted wildlife trade interventions, *Global Ecology and Conservation*, 3, 2015, pp 129–148; and Felipe Thomaz, Illicit wildlife markets and the dark web: A scenario of the changing dynamics, GI-TOC, November 2018, https://globalinitiative.net/illicit-wildlife-markets-and-the-dark-web.
136 For example, a 2019 report by the OECD and the European Union Intellectual Property Office (EUIPO), based on 2016 data, estimated the worth of counterfeit and pirated goods alone at US$509 billion – or 3.3% of total world trade; see OECD/EUIPO, *Trends in Trade in Counterfeit and Pirated Goods*. Paris: OECD Publishing, 2019. GFI's 2017 study estimated that the annual value of counterfeiting could range between US$923 billion and US$1.13 trillion; see Channing Mavrellis, Transnational crime and the developing world, GFI, 27 March 2017, https://gfintegrity.org/report/transnational-crime-and-the-developing-world.
137 Typology drawn from Tuesday Reitano, States on the cusp: Addressing illicit trade in developing economies, GI-TOC, forthcoming.
138 Namita Kohli, India, China are leading sources of counterfeit medicines: report, *The Week*, 4 May 2019, https://www.theweek.in/news/biz-tech/2019/05/04/India-China-are-leading-sources-of-counterfeit-medicines-report.html.
139 Michael Conway et al, Should sub-Saharan Africa make its own drugs?, McKinsey & Company, January 2019, https://www.mckinsey.com/industries/public-sector/our-insights/should-sub-saharan-africa-make-its-own-drugs.
140 GI-TOC, Risk Bulletin of Illicit Economies in Eastern and Southern Africa, 4, January–February 2020, https://globalinitiative.net/esaobs-risk-bulletin-4.
141 Neil Brodie and Isber Sabrine, The illegal excavation and trade of Syrian cultural objects: A view from the ground, *Journal of Field Archaeology*, 43, 1 (2018), pp 74–84; Ben Taub, The real value of the ISIS antiquities trade, *The New Yorker*, 4 December 2015, https://www.newyorker.com/news/news-desk/the-real-value-of-the-isis-antiquities-trade.
142 Simon Mackenzie and Donna Yates, What is grey about the 'grey market' in antiquities, in *The Architecture of Illegal Markets: Towards an Economic Sociology of Illegality in the Economy*, edited by Jens Beckert and Matias Dewey. Oxford: Oxford University Press, 2016.
143 Katie A Paul, Ancient artifacts vs. digital artifacts: New tools for unmasking the sale of illicit antiquities on the dark web, *Arts*, 7, 12, 2018.
144 Amr al-Azm and Katie A Paul, Facebook's black market in antiquities: Trafficking, terrorism, and war crimes, Antiquities Trafficking and Heritage Anthropology Research (ATHAR) Project, June 2019, http://atharproject.org/wp-content/uploads/2019/06/ATHAR-FB-Report-June-2019-final.pdf.
145 Neil Brodie, eBaywatch (1), Market of mass destruction, 19 February 2016, http://www.marketmassdestruction.com/ebaywatch-1; Samuel A Hardy, Does the 'e' in eBay stand for 'easy'? Antiquities from India, Egypt or Ukraine, via the US, Turkey or Cyprus…, Conflict Antiquities, https://conflictantiquities.wordpress.com/2014/09/08/ebay-india-egypt-ukraine-usa-turkey-cyprus.

146 Zeynep Boz, Fighting the illicit trafficking of cultural property: A toolkit for European judiciary and law enforcement, UNESCO, 2018, http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CLT/movable/pdf/Toolkit.pdf.

147 For a discussion of private communication channels being used by antiquities traffickers in Syria, see Ben Taub, The real value of the ISIS antiquities trade, *The New Yorker*, 4 December 2015, https://www.newyorker.com/news/news-desk/the-real-value-of-the-isis-antiquities-trade; and Mike Giglio and Munzer al-Awad, This is how Syrian antiquities are being smuggled and sold, Buzzfeed News, 30 July 2015, https://www.buzzfeednews.com/article/mikegiglio/the-trade-in-stolen-syrian-artifacts. A forthcoming GI-TOC study on illegal antiquities trading from Mali also found that the use of private-messaging channels was a key means by which antiquities dealers in Mali could maintain links with international dealers who, due to insecurity, would no longer be able to travel to purchase objects directly.

148 Neil Brodie, The internet market in pre-Columbian antiquities, in *Cultural Property Crime: An Overview and Analysis on Contemporary Perspectives and Trends*, edited by Joris Kila and Marc Balcells. Leiden: Brill, 2014, pp 237–262.

149 Neil Brodie, How to control the internet market in antiquities? The need for regulation and monitoring, Policy Brief No. 3, Antiquities Coalition, July 2017, https://live-ac-thinktank.pantheonsite.io/wp-content/uploads/2017/07/Policy-Brief-3-2017-07-20.pdf.

150 Lauren Dundler, 'Still covered in sand, looked very old.' – Legal obligations in the internet market for antiquities, *Heritage*, 2, 3 (2019), pp 2311–2326.

151 Neil Brodie, How to control the internet market in antiquities? The need for regulation and monitoring, Policy Brief No. 3, Antiquities Coalition, July 2017.

152 Amr al-Azm and Katie A Paul, Facebook's black market in antiquities: Trafficking, terrorism, and war crimes, ATHAR Project, June 2019, http://atharproject.org/wp-content/uploads/2019/06/ATHAR-FB-Report-June-2019-final.pdf.

153 For details of the operations, see: Europol, 3561 artefacts seized in Operation Pandora, 23 January 2017, https://www.europol.europa.eu/newsroom/news/3561-artefacts-seized-in-operation-pandora; INTERPOL, Over 41,000 artefacts seized in global operation targeting trafficking of cultural goods, 21 February 2018, https://www.interpol.int/en/News-and-Events/News/2018/Over-41-000-artefacts-seized-in-global-operation-targeting-trafficking-of-cultural-goods; and INTERPOL, More than 18,000 objects seized and 59 arrested in operation targeting cultural goods, 29 July 2019, https://www.interpol.int/en/News-and-Events/News/2019/More-than-18-000-objects-seized-and-59-arrested-in-operation-targeting-cultural-goods.

154 Neil Brodie, How to control the internet market in antiquities? The need for regulation and monitoring, Policy Brief No. 3, Antiquities Coalition, July 2017.

155 Amr al-Azm and Katie A Paul, Facebook's black market in antiquities: Trafficking, terrorism, and war crimes, ATHAR Project, http://atharproject.org/wp-content/uploads/2019/06/ATHAR-FB-Report-June-2019-final.pdf.

156 UNESCO, INTERPOL and ICOM, Basic actions concerning cultural objects being offered for sale over the internet, 2006, discusses the challenges to law enforcement (which remain relevant over a decade later).

157 For a comprehensive overview in greater detail than there is space for here, see: Maxwell Anderson, *Antiquities, What Everyone Needs to Know*. Oxford: Oxford University Press, 2017; Mariya Polner, Preventing illicit trafficking of cultural objects: A supply chain perspective, in *The Palgrave Handbook on Art Crime*, edited by Saskia Hufnagel and Duncan Chappell. London: Palgrave MacMillan, 2019, pp 769–793; and Sophie Delepierre and Marina Schneider, Ratification and implementation of international conventions to fight illicit trafficking in cultural property, in *Countering Illicit Traffic in Cultural Goods The Global Challenge of Protecting the World's Heritage*, edited by France Desmarais. Paris: ICOM, 2015, pp 129–138.

158 UNESCO, INTERPOL and ICOM, Basic actions concerning cultural objects being offered for sale over the internet, 2006.

159 Amr al-Azm and Katie A Paul, Facebook's black market in antiquities: Trafficking, terrorism, and war crimes, ATHAR Project, June 2019, http://atharproject.org/wp-content/uploads/2019/06/ATHAR-FB-Report-June-2019-final.pdf.

160 See the discussion in Zeynep Boz, Fighting the illicit trafficking of cultural property: A toolkit for European judiciary and law enforcement, UNESCO, 2018.

161 Neil Brodie, How to control the internet market in antiquities? The need for regulation and monitoring, Policy Brief No. 3, Antiquities Coalition, July 2017.

162 UK Government, Online Harms White Paper, April 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

163 The 'new' framework remains within existing conceptions of 'responsibility' of internet providers by limiting liability to contexts were providers are aware of the existence of illicit content, and fail to remove it, in line with, for example, the EU's e-Commerce Directive.

164 China's social-credit system, currently still in pilot phase, predicates citizens' rights to a range of benefits, from applying to good schools to being featured prominently on dating apps, on their social-citizenship rating. This is composed drawing on a vast amount of personal data of citizens, and analyzing positive and negative behaviour.

165 Adam Satariano, The world's first ambassador to the tech industry, *The New York Times*, 3 September 2019, https://www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html.

166 Ibid.

167 Cambridge Analytica being a key example.

168 UK Government, Online Harms White Paper – Initial consultation response, updated 12 February 2020, https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response.

169 Kartikay Mehrotra, Laura Mahoney and Daniel Stoller, Google and other tech firms seek to weaken landmark California data-privacy law, *Los Angeles Times*, 4 September 2019, https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law.

170 C-18/*18 Eva Glawischnig-Piesczek v Facebook Ireland Limited*.
171 By contrast, in October 2019 the ECJ found that the EU's right to be forgotten, which compels internet service providers to remove all material regarding a particular individual, did not, in most cases, have a global reach. This demonstrates the careful tightrope judiciary must walk in making decisions regarding the extra-territorial reach of laws governing the internet.
172 C-18/*18 Eva Glawischnig-Piesczek v Facebook Ireland Limited*.
173 Article 15(1), EU Directive 2000/31.
174 Agencia Española de Proteccion de Datos, Canal Prioritario, https://www.aepd.es/canalprioritario.
175 Facebook, Community Standards, https://www.facebook.com/communitystandards/dangerous_individuals_organizations.
176 Facebook conference, London, March 2019.
177 Jason Koebler and Joseph Cox, The impossible job: Inside Facebook's struggle to moderate two billion people, Vice, 23 August 2018, https://www.vice.com/en_us/article/xwk9zd/how-facebook-content-moderation-works.
178 Google, Transparency Report, https://transparencyreport.google.com/user-data/overview?hl=en_GB.
179 Facebook Transparency, government requests for user data, https://transparency.facebook.com/government-data-requests.
180 This is a point of pride for certain technology companies, including Apple, whose privacy policy reads: 'Apple has never created a backdoor or master key to any of our products or services. We have also never allowed any government direct access to Apple servers. And we never will.' See https://www.apple.com/lae/privacy/government-information-requests.
181 Agreements between states to facilitate the sharing of information in investigations pursuant to public or criminal laws.
182 Chantal Da Silva, Facebook must do more to crack down on people smugglers luring migrants on site, UN migration agency says, *The Independent*, 11 December 2017, https://www.independent.co.uk/news/world/europe/un-migration-agency-calls-on-facebook-to-crack-down-on-people-smuggling-a8103621.html.
183 Tom Wainwright, *Narconomics: How to Run a Drug Cartel*. London: Penguin, 2017, p 198.
184 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
185 Ibid.
186 Daniel Malan, The law can't keep up with new tech. Here's how to close the gap, World Economic Forum, 21 June 2018, https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up.
187 Nikhilesh De, Human-trafficking expert urges US Congress to regulate crypto miners, CoinDesk, 3 September 2019, https://www.coindesk.com/human-trafficking-expert-urges-us-congress-to-regulate-crypto-miners.
188 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
189 Ibid.
190 Information that either directly or indirectly renders a living individual identifiable.
191 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
192 Mike Isaac, Zuckerberg plans to integrate WhatsApp, Instagram and Facebook Messenger, *The New York Times*, 25 January 2019, https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html.
193 Gabriela Mello, Brazil court slashes fine for Facebook's refusal to share WhatsApp data, Reuters, 25 June 2019, https://www.reuters.com/article/us-facebook-fine-brazil/brazil-court-slashes-fine-for-facebooks-refusal-to-share-whatsapp-data-idUSKCN1TQ2RI.
194 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
195 Especially given the mechanism of participating in such forums, sharing or uploading new CSAM is a prerequisite for downloading existing or new materials. See Kim-Kwang Raymond Choo, Organised crime groups in cyberspace: a typology, *Trends in Organized Crime*, 11, 2008, pp 270–295.
196 Europol, IOCTA 2018, 18 September 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
197 European Commission, Impact Assessment, Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 500 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www. globalinitiative.net