

This analytical report was compiled in the framework of the European Union (EU) funded Project ENACT (Enhancing Africa's response to transnational organized crime). The contents of this INTERPOL report can in no way be taken to reflect the views of the EU or the ENACT partnership.

ENACT is implemented by the Institute for Security Studies and INTERPOL,
in association with the Global Initiative Against Transnational Organized Crime



DISCLAIMER: This publication must not be reproduced in whole or in part or in any form without special permission from the copyright holder. When the right to reproduce this publication is granted, INTERPOL would appreciate receiving a copy of any publication that uses it as a source.

All reasonable precautions have been taken by INTERPOL to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall INTERPOL be liable for damages arising from its use. INTERPOL takes no responsibility for the continued accuracy of the information contained herein or for the content of any external website referenced.

This report has not been formally edited. The content of this publication does not necessarily reflect the views or policies of INTERPOL, its Member Countries, its governing bodies or contributory organizations, nor does it imply any endorsement. The boundaries and names shown and the designations used on any maps do not imply official endorsement or acceptance by INTERPOL. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of INTERPOL concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

© INTERPOL 2020

Table of Contents

Table of Contents.....	2
List of Acronyms.....	4
Executive Summary.....	6
Introduction	8
1. STRUCTURE OF THE REPORT.....	8
1.1. Scope and Objective	8
1.2. Methodology.....	9
2. WHAT ARE THE SURFACE WEB, DEEP WEB AND THE DARK WEB?.....	9
3. INTERNET, CYBER AND CYBER ENABLED CRIME IN AFRICA.....	10
3.1. Internet and social media penetration	10
3.2. Cybercrime and cyber-enabled crime.....	12
3.3. Organized crime groups.....	12
4. SURFACE WEB AND DEEP WEB.....	17
4.1. Financial crimes online.....	17
4.2. Trafficking in human beings and people smuggling.....	22
4.2.1. <i>Human trafficking facilitated online</i>	23
4.2.2. <i>Smuggling of migrants facilitated online</i>	25
4.3. Crimes against children online.....	26
4.4. Trafficking in works of art online	29
4.5. Environmental crimes online	33
4.6. Illicit trade in diamonds online	35
4.7. Trafficking in small arms and light weapons online.....	35
4.8. Drug trafficking online	36
4.9. Trafficking in counterfeit goods online.....	38
4.10. Trafficking in stolen motor vehicles online.....	39
5. DARK WEB.....	40
5.1. Background	40
5.2. How to access the dark web?	41
5.3. Africa and the dark web.....	43
5.4. Use of cryptocurrency.....	44
5.5. What can the user find on the dark web?	47
5.5.1. <i>Hidden services</i>	47
5.5.2. <i>Crime areas on the dark web - Africa</i>	49

5.5.3.	<i>Locations mentioned</i>	52
5.5.4.	<i>User profiles</i>	58
5.5.5.	<i>Payment methods</i>	61
5.5.6.	<i>Use of language</i>	62
5.6.	VPN and TOR usage in Africa	63
5.6.1.	<i>Usage of VPN in Africa</i>	63
5.6.2.	<i>Usage of TOR in Africa</i>	64
6.	DRIVING FACTORS.....	67
	Conclusion.....	68
	References	69

List of Acronyms

ACPF	African Child Policy Forum
ANTIC	Agence Nationale des Technologies de l'Information et de la Communication
ATM	Automated Teller Machine
BDC	Bureau de change
BEC	Business Email Compromise
CAPCCO	Central African Police Chiefs Coordination Organization
CEO	Chief executive officer
DDoS	Distributed Denial-of-Service
EAPCCO	East African Police Chiefs Coordination Organization
ECPAT	End Child Prostitution, Child Pornography and Trafficking
EFCC	Economic and Financial Crimes Commission
ENS	Environmental Security
EU	European Union
FBI	Federal Bureau of Investigation
GIATOC	The Global Initiative against Transnational Organized Crime
ICOM	International Council of Museums
ICT	Information and Communications Technology
IFAW	International Fund for Animal Welfare
IOM	International Organization for Migration
IP	Internet Protocol
ITU	International Telecommunication Union
IWT	Illegal Wildlife Trade
MENA	Middle East and North Africa
MO	Modus Operandi
NCF	Nigerian Conservation Foundation
NGO	Non-Governmental Organization
OCG	Organised Crime Group
OCLCTIC	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication
OPSEC	Operations Security

OSINT	Open Source Intelligence
POC	Point of Contact
POS	Point of Sale
RAT	Remote Access Tool
RSO	Regional Specialized Officers
SALW	Small Arms and Light Weapons
SABRIC	South African Banking Risk Information Centre
SARPCCO	Southern African Regional Police Chiefs Coordination Organization
SMV	Stolen Motor Vehicles
SOCMINT	Social Media Intelligence
THB	Trafficking in Human Beings
TOR	The Onion Router
UAE	United Arab Emirates
UCLA	University of California, Los Angeles
UK	United Kingdom
UNESCO	The United Nations Educational, Scientific and Cultural Organization
UNODC	United Nations Office on Drugs and Crime
URL	Uniform Resource Locator
USA	Unites States of America
VIN	Vehicle Identification Number
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAPCCO	Western African Police Chiefs Coordination Organization
WHO	World Health Organization
WWF	World Wide Fund for Nature

Executive Summary

In recent years, cyber-enabled crimes have increased on the African continent. This has been a result of a combination of factors, including, the improvement of Internet coverage, the wide availability of cyber-tools and the growing flexibility of cybercriminals. As a consequence, online crime nowadays represents a bigger security issue for law enforcement in African member countries than ever before. In this framework, INTERPOL, under the European Union funded ENACT Project, examines through this assessment the issue of cyber and cyber-enabled crimes in Africa in order to help drive a more strategic law enforcement response.

Cybercriminals and Organized Crime Groups (OCG) active in Africa are most probably using the Internet to commit a range of online criminal activities. They use the Internet to find, coerce and control victims online or offline. They also use it to sell products, in most cases procured illegally, as well as to deceive online users and steal their money. They take advantage of online anonymity, use code languages and temporary tools and, in some cases, leave no online trace.

The assessment highlights those cybercriminals that are likely changing the face of the Internet to further their illegal activities on the international scene. They are becoming more sophisticated, with a growing capacity to carry out a range of new types of crimes. In addition, the lack of investment and public awareness, exacerbated by limited capacities to prevent, detect, and investigate these incidents in some African countries, are further driving this criminality on the continent.

Certain crime areas have most likely witnessed in recent years a shift from the surface web to the dark web, where enforcement on a national level is more complex. Despite difficulties at the moment to quantify criminal

use on the dark web as much as on the surface web due to the anonymity factor, the report seeks to show the growing criminal activity on the dark web in connection to Africa.

As cyber-enabled crimes in Africa increase and change, greater awareness of the overall issue and identification of best practice responses from law enforcement will most probably be required. INTERPOL is in a position to support member countries through coordinated, intelligence-led support to law enforcement using a range of operational databases and support techniques.

The following are the key findings deriving from an analysis of a range of data sources available on cyber-enabled crime in Africa:

- ❖ African countries are likely increasingly vulnerable to cyber-enabled crimes as source as well as target countries.
- ❖ Cyber-enabled financial crimes most probably take various forms and affect individuals, companies, and public administration in all African regions.
- ❖ Trafficking in Human Beings (THB) in Africa is likely facilitated by the Internet as it allows the recruitment, control, and deception of victims through social media, instant messaging applications and online platforms.
- ❖ Migrant smuggling in Africa is likely facilitated by social media and encrypted messaging applications: OCGs advertise their services and African migrants refer to information to reduce risks.
- ❖ African and non-African offenders most probably use the Internet to abuse African children online and offline.
- ❖ OCGs active in Africa probably use the Internet to sell drugs and contact local as well as international customers/providers.

- ❖ African OCGs, mainly North African, are likely using social networking sites to facilitate the looting and trafficking of stolen works of art on continental but also transnational levels.
- ❖ African OCGs, almost certainly in connection with their transnational counterparts, are increasingly using social media-based trade for Illegal Wildlife Trade (IWT) and trafficking in precious minerals through the help of middlemen/women.
- ❖ OCGs active in Small Arms and Light Weapons (SALW) trafficking in Africa are increasingly using social networking sites to conduct trade. They are likely engaged in other online criminal activities as well.
- ❖ With the increase in Internet coverage, online trade of illicit goods is likely increasing on the African continent.
- ❖ OCGs active in Africa are likely increasingly using the Internet to complete various stages of the process of trafficking in Stolen Motor Vehicles (SMV).
- ❖ African cybercriminals are most likely limiting contact by using code languages and temporary tools, making disruption by law enforcement even harder.
- ❖ Cybercriminals trafficking online in Africa include private individuals, enthusiasts, collectors and traditional Internet users.
- ❖ Some cyber OCGs involved in online trafficking on the continent are most likely part of hierarchical networks where the leader recruits members to complete specific tasks that would facilitate online crimes. Other OCGs are likely non-traditional loosely connected groups that connect for the purpose of committing a crime.
- ❖ Cybercriminals on surface web and dark web are increasingly flexible and knowledgeable Internet users. They are most probably investing in improving their technological skills, business know-how and advertisement strategies.
- ❖ Some OCGs active online in Africa are most probably employing middlemen/women at different stages of the crime activity to ensure the smooth running of criminal business.
- ❖ The analysis of various elements on dark web domains suggests that cybercriminals located in Africa are likely active on the dark web with growing transnational links.
- ❖ It is likely that crime elements from Kenya, Nigeria and South Africa are engaged in dark web activities.

Introduction

In recent decades, African and international OCGs have increased their activities on the African continent, further encouraged by growing economies. Over the years, these OCGs have developed an understanding of the Internet and the multiple possibilities of exploiting its capabilities for their criminal activities. In particular, the Internet enables OCGs to widen the scope of their operations, by expanding their networks and enhancing their abilities to stay undetected.

Internet penetration on the continent has increased steadily in recent years as a result of multiple factors, including improved Internet coverage and the increased use of the Internet for basic individual needs. This increased online exposure of Africans, many of whom lack basic technical knowledge on accessing and using the Internet, makes them easy targets for transnational cybercriminals. At the same time, younger Africans mostly, are demonstrating good abilities in using and depending on cyber tools. This has led to an increase in cyberattacks targeting individuals and groups on the African continent, as well as in attacks originating from the continent.

Many African member countries still lack proper policies and strategies to combat cybercrime. On the continental level, in 2014, the African Union adopted the Convention on Cybersecurity and Personal Data Protection. However, only 14 of the 55 African Union member countries had signed the convention, and only seven¹ ratified it, by January 2020. The convention needs to be ratified by at least 15 member countries to enter into force, meaning it is not in force yet. This shows that cybersecurity is still not perceived as a necessity by many African countries which further exacerbates the problem.

In 2017, the economic loss in Africa due to cyber and cyber-enabled crime reached USD

3.5 billion. In Nigeria, this number reached USD 649 million and USD 210 million in Kenya. South Africa also reported major economic losses due to cyberattacks, reaching around USD 157 million.²

Emerging economies and the impact of globalization associated with non-restrictive cybersecurity practices in many African member countries have greatly contributed to Africa becoming a safe haven for cybercriminals. This threat assessment will explore cyber-enabled crime on the African continent in light of several strategic indicators.

**** Two versions of this report exist. This report is the public version of the completed analysis, which included police information; where specific police information was used, this information has subsequently been sanitized for public distribution ****

1. STRUCTURE OF THE REPORT

1.1. Scope and Objective

The objective of this report is to examine the major aspects of organized crime in Africa on the surface web, deep web and dark web.

This assessment will draw upon data from available open and closed sources and present a comprehensive overview on how the different OCGs active in Africa (or linked to Africa) exploit the different levels of the Internet to foster their illegal activities.

This report should assist and guide law enforcement in designing strategies to combat this form of emerging crime throughout the continent. This assessment also intends to be a tool for eliciting law-enforcement cooperation among countries of the five African regions, not only among the countries impacted the most by this crime, but also among those which are at risk of being affected in the near future.

1.2. Methodology

This assessment follows an all-source intelligence analysis methodology. It is the result of integrating multiple data sources.

Open sources used in the framework of this report include news articles and reports from various private entities, international organizations and think tanks. Whenever identified, official statistics and data were used and given preference over other sources. Data related to social media and dark web sources were processed while keeping in line with INTERPOL's legal framework applicable to the processing of open source information, which did not allow to monitor and investigate information from some sources.

Information from the aforementioned sources was aggregated together in order to identify consistencies across all data, patterns and trends, and any identifiable convergences.

This report was drafted using a regional approach. Therefore, when national examples are quoted, it is done for illustrative purposes, in order to put forward regional dynamics.

INTERPOL African regions are defined on the basis of countries' participation in regional chiefs of police organizations. Some countries participate in more than one regional chiefs of police organization. In such cases, they are counted in each of the regional organization in which they participate. North African countries are members of the INTERPOL Middle East and North Africa (MENA) region. For the purpose of this report which only covers the African continent, they were regrouped in a category named North Africa. This category includes the following countries: Algeria, Egypt, Libya, Morocco and Tunisia. The other INTERPOL African regions and their member countries are as follows:

CAPCCO³: Cameroon, Central African Republic, Chad, Democratic Republic of Congo,

Equatorial Guinea, Gabon, Republic of Congo, Sao Tome and Principe.

EAPCCO⁴: Burundi, Comoros, Djibouti, Democratic Republic of Congo, Eritrea, Ethiopia, Kenya, Rwanda, Seychelles, Somalia, South Sudan, Sudan, Tanzania, Uganda.

SARPCCO⁵: Angola, Botswana, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia, Zimbabwe.

WAPCCO⁶: Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea Bissau, Liberia, Mali, Mauritania, Niger, Nigeria, Senegal, Sierra Leone, Togo and Guinea.

2. WHAT ARE THE SURFACE WEB, DEEP WEB AND THE DARK WEB?

Surface web

Also known as the 'visible web', it is the 'Internet', the web that is accessible by the general public. Information on the surface web is indexed, and therefore, searchable with standard web search engines. Access to its content does not require special configuration. Compared to the deep web, the surface web is relatively small in size, making up less than 10 per cent of the total World Wide Web content.⁷ Examples of surface web include, Google, Bing, Yahoo, YouTube, Wikipedia, news sites, shopping sites, blogs, etc.

Deep web

Known as the 'invisible web', it is the part of the Internet that is not visible to everyone. Its content is not accessible through standard search engines. Generally, deep web websites require a Uniform Resource Locator (URL) to find the website as well as further authorization and permission to access the website (i.e. a username and password). Examples of the deep web include email accounts, social networking websites, cloud

service accounts, online banking, internal networks of companies, education pages, government-related pages, services that require the user to pay for them (i.e. video on demand, magazines and newspapers), data shared on private social networks and Internet messaging, etc.

Dark web

Also known as the 'dark net', it is a small part of the deep web. In order to access the dark web, a specialized software is needed (i.e. TOR, I2P, Freenet), which anonymizes the Internet Protocol (IP) address of the user. Inside the

dark web, most websites are hidden and users can browse online almost anonymously. Within this web level, illegal markets known as 'dark net markets' operate, and many of them constitute a space for the illegal selling of products, including drugs, firearms, child sexual abuse material, hitman services, etc. Examples of dark net markets include Alphabay Market, Hansa Market, Dream Market, etc. The dark web could also be used for legal purposes, such as accessing and sharing information, communication and identity protection.^{8 9}

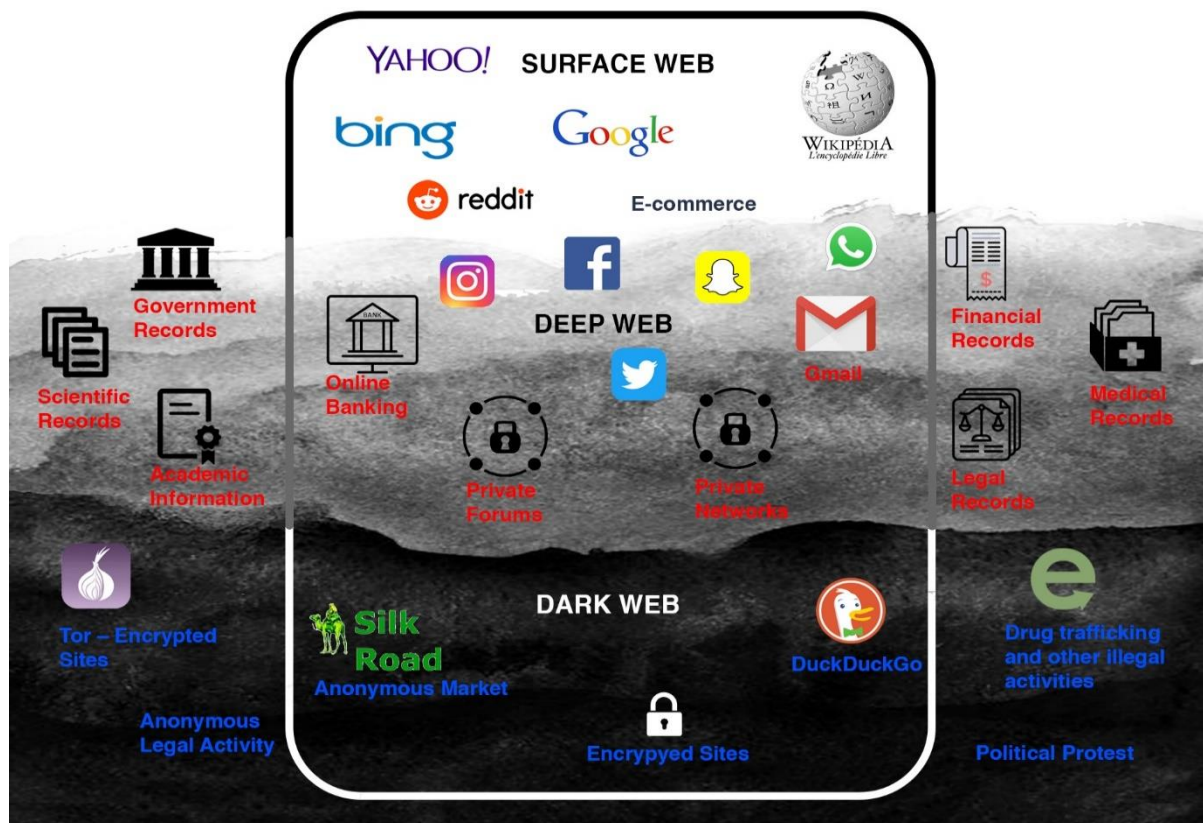


Figure 1. Representation of the surface web, deep web and dark web

3. INTERNET, CYBER AND CYBER ENABLED CRIME IN AFRICA

3.1. Internet and social media penetration

Internet penetration in Africa is continuously increasing despite increased restrictions. In

1989, the creation of the World Wide Web revolutionized communication, yet, by 1990, statistical reports indicated that “only half of a per cent of the world population were online”. The following decade witnessed a qualitative leap. However, by the year 2000, 99 per cent of population in Sub-Saharan Africa were still offline.

Sixteen years later, countries worldwide were joining the online world at a growing pace. Nonetheless, countries from some parts of the world, including Africa, had barely witnessed any change in online activity since the 1990's, with less than 5 per cent of population having online access in countries such as Central African Republic, Eritrea, Guinea Bissau, Madagascar, Niger and Somalia. Yet, the global trend shows that every year more people from all over the world are online, through a mobile phone, a computer, a digital TV, a game or a personal digital assistant.

According to the World Bank, despite some minimal irregular changes, Internet users have steadily increased in Africa between 2015 and 2017 from an average of 20 per cent of the share of African population using the Internet in 2015 to 26 per cent of the population in 2017. In some African countries, the number of Internet users has even doubled over the three years studied, such as in Côte d'Ivoire, Ghana and Malawi.¹⁰

In its recent report, the International Telecommunication Union (ITU) revealed that a reported 4.1 billion people used the Internet in 2019, indicating a 5.3 per cent increase from the previous year. Global penetration has also witnessed a massive increase from nearly 17 per cent in 2005 to 53 per cent in 2019.

In 2019, ITU estimated that in the least developing countries, only 19 per cent of individuals were using the Internet, compared to 87 per cent in developed countries. On this scale, Africa ranked lowest, with only 28 per cent of individuals using the Internet, compared to Europe, which ranked the highest, with 83 per cent of individuals using the Internet. This same year, the African continent had the highest percentage of offline population in the world, with the majority of offline countries being in Central, Eastern and Western Africa.¹¹ Differences across the five African regions in Internet usage patterns were also noted (see figure 2).¹²

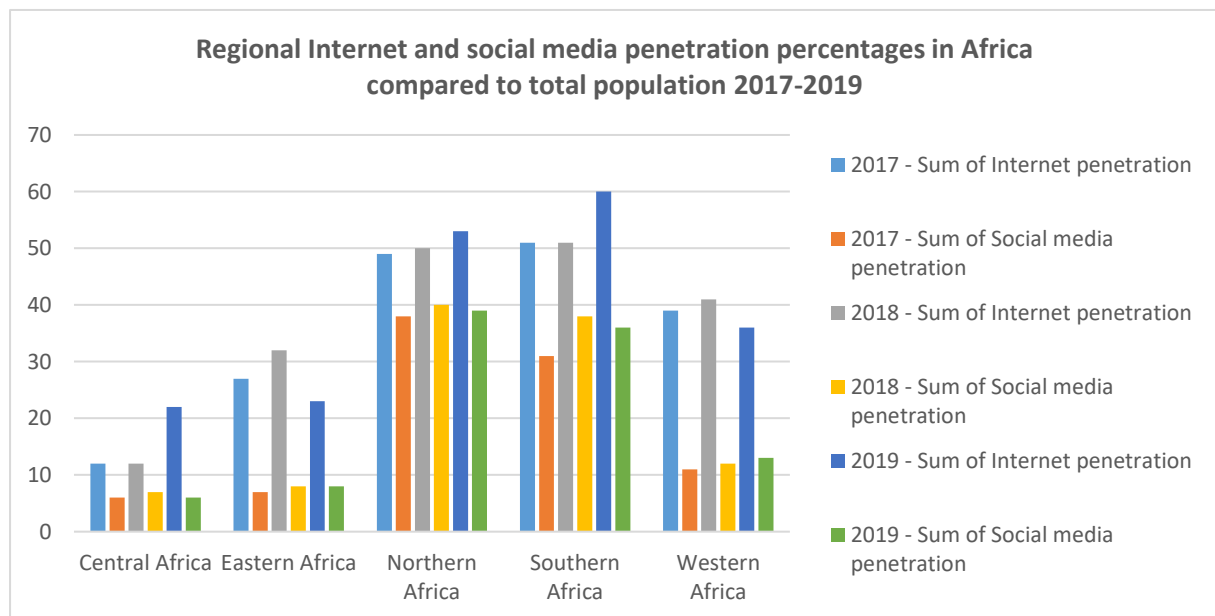


Figure 2. Regional Internet and social media penetration percentages in Africa compared to total population 2017-2019

The inter-regional differences are further highlighted in the graph above. The graph shows that Internet and social media penetration present different patterns across the five African regions between 2017 and

2019. A great difference is noted between the levels of Internet and social media penetration in Central, Eastern and Western Africa when compared to Northern and Southern Africa, where they are mostly higher. Despite the

variations, Internet and social media penetration is mostly increasing in Africa.

The relatively slow increase and variation in penetration levels on the continent between 2017 and 2019, in particular in Eastern and Western Africa, are likely due to various factors such as the growing ease of Internet access in parts of Africa more than in others as well as the multitude functions that Internet and social media are increasingly offering in some member countries paralleled with restrictive measures to control and/or limit Internet and social media access in some African countries.

3.2. Cybercrime and cyber-enabled crime

As cyberattacks evolve, the misconception about the difference between cyber and cyber-enabled crime has become common, including in Africa, with some sources combining data relative for both areas and referring to them as cybercrime. According to INTERPOL, cybercrime refers to “crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user.” As for the cyber-enabled crime, it occurs when a ‘traditional’ crime is facilitated by the Internet, such as fraud, theft and the sale of fake goods.¹³

In the last decade, both cyber and cyber-enabled crimes have become widespread in Africa. Despite the fact that 75 per cent of its population were still offline by 2016,¹⁴ many personal/private/public infrastructures in African countries are increasingly emerging as targets for these types of crime. Attacks are also increasingly originating from African countries. In 2013, Trend Micro predicted that “the number of cybercrime activities targeting or originating from Africa will increase—and probably dramatically—in the next few years.” The growing base of Facebook users,

inadequate or the absence of cybercrime laws¹⁵ and under-documentation of the crime were among the main reasons that made the continent vulnerable to malicious attacks, according to the report. Sources also mention that 18,607 cyber security incidents were counted in 2011 compared to 564 in 2000.¹⁶ In 2016, approximately 24 million malware incidents targeted Africa. By 2017, malware, spam emails, botnets and software piracy, among other crimes, were reported in many African countries across the continent.¹⁷

3.3. Organized crime groups

This section summarizes some of the inferences and conclusions included in the assessment concerning OCGs. Further detailed information will be provided throughout the report. In particular, this section examines the various dynamics of some of the OCGs found to be using the Internet to further their illegal activities in Africa. It highlights some of the main techniques OCGs active in Africa are using online. Where possible, it draws attention to specific OCGs identified in the framework of the report.

Some cyber OCGs are likely to have specific roles assigned for each member. For example, the leader might handle recruitment, whereas group members would be in charge of extracting e-mails, creating fake profiles and developing a fake website, among other tasks. Other OCGs are likely to form non-traditional organized groups that are loosely connected. Small groups would connect, share experience, commit the scam and then share the money.

According to open sources, OCGs use the Internet both for internal communication within the group, and for external communication with non-OCG associates. Internet allows OCGs to reach new customers, new victims, and to a lesser extent, possible new partners. It also allows them to advertise

their illicit goods and services. They are increasingly using code languages and temporary contact numbers, which makes it more difficult to leave traces and as a result, enforcement harder.

Cyber OCGs make wide use of social networking sites, instant messaging applications and Voice over Internet Protocol (VoIP) services. Facebook is the main tool used, followed by WhatsApp, and to a lesser extent, Instagram, Telegram, Twitter and Snapchat.¹⁸ OCGs also use e-mail services such as Yahoo, Gmail and Outlook. To promote their offers, OCGs use social media and classified ads and e-commerce websites.

Social networks allow OCGs to connect with customers and possible partners across Africa and worldwide. They use social networking sites to:

- Contact, lure, recruit, coerce and control victims;
- Advertise and sell illegal services or products;
- Share locations of victims;
- Organize logistics of the crime;
- Exchange best practices and modus operandi among cybercriminals;
- Launder revenue gained from illicit activities;
- Blackmail victims and/or their families.

OCGs also produce fake Internet sites similar to legitimate ones and manipulate search engines.

OCGs active in Africa have different levels of expertise. The more they are experienced in terms of social engineering and computer skills, the more money they gain illegally. Below are some of the methods adhered to by

OCGs to acquire more experience in illegal activities online. This includes:

- Apprenticeship, which involves an established criminal taking an apprentice under their wing to teach them the business;¹⁹
- 'Yahoo Boy's' academy, a real life workshop where students are taught how to perpetrate scams online;²⁰
- Trainings dedicated to cybercriminals in North Africa.²¹

Financial cyber-enabled crimes

Some OCGs involved in financial cyber-enabled crimes are likely of Western African origins, with some of them based in Africa and others in Asia, Europe and the USA, where they built connections with their counterparts.²²

Some OCGs active in online financial crimes are opportunists and link their scams to current events or regional instability in concerned countries.

Some OCGs are probably poly-criminal, involved in or linked with offenders engaged in, among others, money laundering, kidnapping, coercion, human trafficking, prostitution, political patronage, arms and narcotics trafficking.²³

Members of Nigerian cyber OCGs based outside Nigeria, such as in Eastern Africa, probably have links with cybercriminals based in Nigeria. OCGs from Benin, Cameroon, Congo, Côte d'Ivoire, Democratic Republic of Congo and Nigeria implicated in scams originating from their countries are most probably supported by members of their community based in target countries, mainly in Europe.²⁴

Nigerian OCGs, or confraternities, such as the Black Axe Confraternity, are active in cybercrime on the African continent as well as abroad, including in Canada, Italy and the USA.

Other Nigerian OCGs include Supreme Eiye Confraternity and the London Blue, which is based in the UK and operates mostly abroad.

The Supreme Eiye Confraternity

Also known as the Air Lords, was reportedly founded in 1963 or 1970 (date not agreed upon) at the University of Ibadan in Nigeria. This Nigerian OCG is composed of a “system of cells (called forums) operating locally, but connected to other cells established in different countries in West Africa, in North Africa, in the Middle East and in Western Europe.” This confraternity is poly-criminal and known to be involved in THB, drug trafficking, money laundering, etc. Leaders are referred to as ‘Capones’, with a ‘hierarchy of Capones’, and new members undergo brutal initial rituals, including criminal acts.

Source: ‘Nigeria: The Eiye confraternity, including origin, purpose, structure, membership, recruitment methods, activities and areas of operation; state response (2014-March 2016), *Immigration and Refugee Board of Canada*, 08 April 2016, <https://www.refworld.org/docid/5843fa644.html> (accessed 03 June 2020).

Black Axe Confraternity

The group is widely believed to be the same as the Neo Black Movement founded in 1977 at the Benin University in Nigeria. Black Axe is a transnational OCG with a pyramidal hierarchical structure with cult-like tendencies. Black Axe gangs are involved in prostitution, human trafficking, narcotics trafficking, grand theft, money laundering, and email fraud/cybercrime mainly in Nigeria, but also Europe and North America. Members are known as ‘Axemen’ and the commander or boss of a zone in a foreign location is known as an ‘Oga’.

Source: ‘Intelligence Report: Nigerian Confraternities Emerge as Business Email Compromise Threat’, *CrowdStrike Global Intelligence team*, 03 May 2018, <https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf> (accessed 15 January 2020).

London Blue

A Nigerian gang, that likely originated in Nigeria, with members in the UK and collaborators involved in moving funds in the USA and Western Europe. The group operates like a modern corporation. London Blue evolved from Craigslist scams, to phishing, to BEC and uses legitimate commercial data providers to identify targets, mainly in the USA and Western Europe.

Source: ‘London Blue UK-Based Multinational Gang Runs BEC Scams like a Modern Corporation’, *AGARI Data*, 09 November 2018, <https://www.agari.com/cyber-intelligence-research/whitepapers/london-blue-report.pdf> (accessed 18 March 2020).

Human trafficking and human smuggling

OCGs, with most likely Western African members, active in human trafficking in Europe are using online platforms to offer victims to potential customers, where they give the possibility to costumers to leave comments and evaluate services.

Western African OCGs active online in recruiting victims as domestic servants abroad are almost certainly connecting with destination-country recruitment agencies to complete the trafficking process.

Western African OCGs active in Western Africa and Europe use mostly social networks, including Facebook and WhatsApp, to recruit victims of human trafficking and migrant smuggling. Some of them were found to offer 'travel packages' including all necessary items for the journey. OCGs have most probably developed links with local gangs active in sexual exploitation as well as other crimes such as THB, migrant smuggling, fraud, corruption, document forgery and money laundering.

Western African OCGs, actively using social media for transnational human trafficking purposes have possible links to Europe and other parts of the African continent.

Central African OCGs active in recruiting people online for trafficking purposes are often composed of local community members, such as former religious leaders and victims who have turned into perpetrators. Some OCGs active online also involve family members.

Eastern African OCGs active in human trafficking are found to have links to the Gulf region.

Sexual abuse/exploitation of children

In Eastern Africa, 'diva clubs' attract young girls using social media platforms and convince them to expose themselves sexually.

Environmental crimes

OCGs active in Western Africa offer and sell their illegal wildlife products online.

In Western Africa, some former 'Yahoo Boys', previously active in online financial scams, have moved to selling pangolin scales and ivory artefacts online, with links in Western Africa, Europe and Asia.

Trafficking in works of art

Some OCGs active in trafficking in works of art online in connection to Africa are probably originating from the Middle East and North Africa with links to Europe and the USA.

Trafficking in stolen motor vehicles

OCGs active in trafficking in SMV in Africa use the Internet to forge documents and sell stolen cars as well as other vehicle components. OCGs active in Western Africa forge Vehicle Identification Numbers (VIN) and deceive their clients using illegitimate websites to sell non-existent vehicles.

Dark web

Based on the analysis of available information, it is likely that crime elements active in Kenya, Nigeria and South Africa are investing in dark web activities.

It is likely that OCGs are active in the MENA underground.

Predictions suggest that Western African cybercriminals are likely to form their own online criminal communities in the framework of a Western African underground market.

On the dark web, vendor sites can be managed by a single individual or an OCG. However, given that marketplaces are platforms that gather sellers and buyers interested in multiple types of products and services, sometimes in different languages, it is likely that OCGs investing on the dark web, are investing in

marketplaces. Forums also possibly provide a platform for future members of OCGs to initiate contact seemingly anonymously.

Main techniques

In some crime areas, online markets offering illicit products are extensions of physical black markets. The analysis reveals that in most cases, cyber criminals initiate contact with would-be victims or customers through online platforms, mainly Facebook groups. Once negotiations start, they move to more private platforms, such as encrypted messaging applications and phones. When and/or if needed, physical contact between the offender and/or associate and the future victim is established.

Payment methods used are mostly cash, mobile money, online transfer and cryptocurrency.

Use of Facebook

OCGs active online use mainly Facebook to support their illegal activities. They use it to share know-how and best practices as well as to offer and sell products and services in closed groups. They also use the platform to promote third party sites, on the surface and dark web.

Facebook has become the go-to web platform for OCGs active in Africa due to the features that it offers and which can support criminal activity easily. This includes the privacy settings that Facebook provides, including 'public', 'closed' and 'secret', which give the administrator the freedom to decide who joins the group, further complicating enforcement attempts. In some cases, future members must reply to screening questions, in others, they need to commit to paying a 20 per cent commission to the administrator after any sale. Traffickers also use video and pictures to advertise products, encrypted messages for communication and the 'Buy and Sell' feature. Such features allow traffickers to connect with

individuals engaged in similar criminal interests easier and expand as a result their networks effortlessly.

It should be noted that traffickers avoid using terminology that can be tracked by law enforcement on Facebook, and often move to WhatsApp for negotiations after initial contact on Facebook. The encryption features of WhatsApp has made it in recent years the method of choice for communication between traffickers and smugglers.²⁵

Information gathering and tailoring the message

In many cases, the sophistication and success of the cyber-enabled crime is highly dependent on the hard work that attackers have put into preparing the scam and tailoring the message. This requires OCGs to use legitimate online tools to study the profiles of future victims, including e-mail tools and business listings. In addition, they also monitor and study future victims' profiles on social media websites (i.e. location, interests, contacts, images, social situation, personal taste, etc.). Using these tactics, OCGs can identify expectations and exploit the emotional vulnerabilities of future victims. This is how OCGs maximize the chances that a user buys a product or chooses to benefit from a service.

Use of middlemen/women

Analysis of online crime in connection to Africa reveals that OCGs likely employ middlemen/women to support the criminal process. Some former members of OCGs are acting as middlemen/women by accompanying potential customers, with whom contact was initiated online, to check out physical products. When deals are made through online markets, middle agents are employed to arrange the transfer and sometimes move the pieces ordered themselves. Sometimes, they are employed to move the money gained.

Middlemen/women also use their online pages to advertise items and demonstrate to potential customers their access to buyers or particular products. In the case where one of their contacts is interested, middle agents would buy the product, and resell it to them at a higher price.

4. SURFACE WEB AND DEEP WEB

4.1. Financial crimes online

African OCGs are likely engaged with counterparts across the world to commit online financial crimes targeting African and non-African countries as well as generate large sums of illegal money. Financial crimes pose significant threat to member countries as victims include not only individuals, but private entities, governmental bodies and national institutions. The complex and transnational nature of this under-reported, and sometimes undetectable crime, further complicates enforcement measures.²⁶

Financial crimes occur on the three web levels:

- The surface web (i.e. scam classified ads, fake phishing websites, scam tutorials, etc.);
- The deep web (i.e. phishing e-mails, social media used for social engineering, etc.);
- The dark web (i.e. malware markets, stolen financial data, etc.).

Online financial crimes can be divided into two categories: cyber-dependent crimes, when targeting a system, network, or software and cyber-enabled crimes, as previously mentioned, when a 'traditional' crime is facilitated by the Internet. In some cases, online financial crimes are complex and hybrid, combining cyber-dependent and enabled techniques, such as in some Business Email Compromise (BEC) scams.

The examination of available information reveals that online financial crimes are the most prevalent and developing crimes on the African web. These crimes can take many forms. In the public version of the report, only cyber-enabled financial crimes will be examined in details.

African OCGs, mostly West Africans, are likely conducting various forms of cyber-enabled financial crimes that target African as well as non-African countries.

Main online platforms used: Facebook, e-mail, WhatsApp, etc.

Main payment methods used: Western Union, Orange Money, Express Union, wire transfers, gift cards, etc.

Online financial crimes are cyber-enabled when the Internet is used as a facilitator for the crime, such as a means to reach the victim's money. In this case, social engineering²⁷ is the key ingredient for bypassing the traditional defense perimeters and committing fraud. Cyber-enabled offenders can be entry-level criminals, mid-level criminals and the most advanced cybercriminals, depending on their technical abilities.

Business Email Compromise (BEC)

BEC scams originating in Africa, mainly Western Africa, targeting victims based in non-African and African countries are likely the most used online financial crimes by OCGs connected to Africa.

BEC is a global phenomenon increasingly targeting businesses, administrations and individuals worldwide, including in Africa.

As defined by INTERPOL, BEC occurs when "criminals hack into email systems or use social engineering tactics to gain information about corporate payment systems, then deceive

company employees into transferring money into their bank account".²⁸ BEC is a global phenomenon increasingly targeting businesses, administrations and individuals worldwide, including in Africa.²⁹ On the continent, BEC scams are increasing rapidly, with losses amounting to USD to USD 2 million in 2016.³⁰

According to open sources, BEC cases are reported in Central Africa³¹ and in Northern Africa.³² In Eastern Africa, cybercrime losses in Kenya reportedly amounted to an estimated USD 295 million in 2018, "with BEC being one of the main ways used to defraud local businesses."³³ It is also a common threat in Rwanda,³⁴ where the cost of cyber fraud more than doubled between 2017 and 2018, increasing from USD 432,019 (RWF 400,000) to USD 6,480,294 (RWF 6,000,000,000).³⁵

In a 2018 report, South African Banking Risk Information Centre (SABRIC) reported that BEC is among the most prominent schemes having an impact on the digital banking industry.³⁶ In 2019, SABRIC indicated that South Africa and in line with global trends, has witnessed an increase in BEC cases.³⁷

In addition, multiple open sources indicate that BEC scammers from Western African countries are targeting individuals as well as companies in Africa and abroad.³⁸ It is worth noting that some Western African offenders tend to settle outside their country of origin and operate in Western African countries, or in other African regions. For example, some Nigerians have reportedly settled in Ghana³⁹ and Senegal,⁴⁰ whereas some Ivoirians have settled in Mali,⁴¹ Benin and Togo, allegedly to evade law enforcement efforts.⁴²

In order to transfer the money illegally from abroad to accomplices based in Western Africa, some cyber OCGs use money mules. These individuals are usually based in the victim's country and route the money through

their bank accounts, holding a percentage of the money.⁴³ In this context, according to the Federal Bureau of Investigation (FBI), romance scams' victims have been also used as money mules to cash out or transfer money stolen from BEC scams.⁴⁴ Multiple sources reveal that Nigerian cybercriminals, after focusing on simpler scams such as romance scams and/or advanced-fee fraud, have moved in recent years to sophisticated BEC scams using Remote Access Tool (RAT) as well as malwares⁴⁵ from Russian and other illegal English-speaking forums in the deep and dark web.⁴⁶

In many cases, African OCGs operate outside Africa. A recent analysis uncovered the working method of London Blue, a Nigerian gang with members based in the United Kingdom, targeting companies and operating like a modern corporation with members carrying out specialized functions.⁴⁷ A potential victims list of more than 50,000 corporate officials in 82 different countries (mainly Europe and the USA), of which 71 per cent were CEOs, was identified.⁴⁸

According to a survey on BEC fraud, the most-targeted countries are the USA, closely followed by China, France, Germany, India, Saudi Arabia, South Korea, Turkey, the UAE and the UK. Industries most targeted by BEC campaigns in 2016 included manufacturing businesses, which accounted for nearly half of the victims (45.96 per cent), followed by food and beverages companies (5.05 per cent) and retail businesses (3.54 per cent).⁴⁹

CASE STUDY

On 10 September 2019, the U.S. Department of Justice announced that Operation REWIRED, a coordinated international enforcement operation, disrupted BEC schemes that were designed to deceive businesses and individuals. The four-month operation resulted in the seizure of approximately USD 3.7 million as well as the arrest of 281 individuals in the United States and overseas, including 167 in Nigeria, 18 in Turkey and 15 in Ghana. Arrests also included individuals in France, Italy, Japan, Kenya, Malaysia, and the UK.

Source: '281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes', U.S. Department of Justice, 10 September 2019, <https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds> (accessed 12 February 2020).

In the context of Operation REWIRED, the US Department of Justice stated that foreign citizens that commit BEC scams are often “members of transnational criminal organizations, which originated in Nigeria but have spread throughout the world.”⁵⁰

In addition, perpetrators on the continent use advance money laundering techniques including the use of Banks in China, particularly in Hong Kong. Nigerian OCGs, such as the Black Axe confraternity, have invested in cybercrime in Africa but also abroad (i.e. Canada, the USA

and Italy). To exchange information and organize themselves, these groups use closed Facebook groups.⁵¹ According to open sources, cybercriminals use closed Facebook groups to share know-how relative to social engineering schemes and to offer malware, stolen personal information and illegal financial services such as money mule services.⁵² Such groups sometimes advertise third party sites based on surface or dark web sites. In a recent article on these Facebook groups, a list of the studied groups was made available. The names of some of the groups included the ‘Yahoo boys’, which likely bring together hackers from Western Africa.⁵³ When deleted by Facebook, which relies on its members to report illicit activity, new groups with similar names and objectives are established again.⁵⁴

Cybercriminals use closed Facebook groups to share know-how relative to social engineering schemes and to offer malwares, stolen personal information and illegal financial services such as money mule services.

In this context, multiple sources indicate that Nigerian cybercriminals are likely to rely on Nigeria-based Bureau de change (BDC) operators as key facilitators when transferring and laundering financial fraud proceeds.^{55 56} BDC operators are financial service providers, registered with the Nigerian government who deal mostly in legitimate transactions. A 2016 report on money laundering rated the vulnerability of BDCs to money laundering as very high.⁵⁷ More recently, the Central Bank of Nigeria urged BDC operators in Nigeria to self-regulate to better combat money laundering.⁵⁸

In addition, iTunes or Google play gift cards are becoming increasingly popular methods of cashing out among cybercriminals as they

allow them to collect the money quickly and directly, without the help of a money mule who has to be paid and whose account could be monitored and shut down by law enforcement. However, the money gained through gift cards is less than what is gained through fraudulent wire transfers (between USD 1,000 and USD 2,000 compared to USD 35,000). This is why some cybercriminals use gift cards to buy cryptocurrencies. For example, some cybercriminals use a USA-based peer-to-peer market called Paxful to buy bitcoins using their gift cards. To convert the bitcoins into cash, cybercriminals use Reminatio, another peer-to-peer market place. The process is quick and can be completed in less than three hours. The use of cryptocurrencies seems well entrenched in Western African cybercriminal OCGs, and tends to develop in all other African regions, except in Central Africa.⁵⁹

Sextortion

It is likely that sextortion originating in Africa, mostly in Western and Northern Africa, targets males and females in African and non-African countries.

As defined by INTERPOL, sextortion occurs when “victims (often men) are tricked by an attractive stranger into participating in naked videos chats which are secretly recorded and subsequently used for blackmail”.⁶⁰ This type of offense is widespread in Africa.

In Western Africa, cases of sextortion are reportedly originating from Senegal⁶¹ and Nigeria.⁶² In Ghana, sextortion recently ranked second with about 10 cases recorded each week, most of which involve children and young people.⁶³

In an analysis carried out in 2018, *l’Office central de lutte contre la criminalité liée aux technologies de l’information et de la communication* (OCLCTIC) reveals that the vast majority of cases originate from French-

speaking African countries, where OCGs use anonymization means. Such means include Virtual Private Networks (VPN), used to create fake online accounts, which further complicate identification attempts by law enforcement. The source also indicates that 60 per cent of victims examined were deceived through an online dating site and 70 per cent had not made the payment claimed by the author. The follow-up of the files led to approximately 80 reports that were sent through the INTERPOL channel to the concerned member countries, mainly from Western Africa, Northern Africa, and Southern Africa. Out of 900 procedures identified, 96 per cent of the victims were male and 84 per cent were adults, most often young adults, around 19 years old.⁶⁴

Cybercriminals are also active in Morocco. They mainly use fake female profiles to deceive individuals, mostly from Morocco.⁶⁵ In Southern Africa, in South Africa the offense is reportedly on the rise via email and social media,⁶⁶ especially via WhatsApp and Facebook.⁶⁷ In Central Africa, cases of sextortion were reported in the Democratic Republic of the Congo,⁶⁸ Gabon and Cameroun, where Facebook and Western Union are used for money remittance.⁶⁹ Analysis of victim profiles indicate that, overall, they are predominantly male, when targeted outside Africa, but women appear to be more targeted on the African continent. In Ghana, women represent approximately 99 per cent of sextortion victims.⁷⁰ In Cameroon, cases of women being tricked by a would-be ‘European husband’, who uses a webcam to record compromising material involving the women and then blackmail them, were reported.

Analysis of victim profiles indicate that, overall, they are predominantly male, when targeted outside Africa, but women appear to be more targeted on the African continent.

Available data also show that sextortion scams may be used for human trafficking purposes.⁷¹

Romance scam

Romance scams originating in Africa, mostly Western Africa, have an inter-regional as well as an intercontinental nature.

This type of scam occurs when “criminals develop a ‘relationship’ with victims through social media with the ultimate goal of obtaining money”.⁷²

In Western Africa, offenders are active in Benin,⁷³ Côte d’Ivoire,⁷⁴ Guinea,⁷⁵ Nigeria⁷⁶ and Ghana.⁷⁷ To contact their victims, romance scammers use dating sites, Facebook, Instagram, WhatsApp and Hangouts.⁷⁸ Open sources report similar cases across the continent in Northern Africa,⁷⁹ ⁸⁰ Central Africa,⁸¹ and Southern Africa.⁸²

A 2018 analysis focusing on the geographic origins of romance scams, based on the analysis of a dataset of real online scamming profiles, reveals that their origins are mostly Western Africa, including Ghana, Togo, Senegal, and Côte d’Ivoire, with Nigeria as the largest single contributor. South Africa also appears to be an important African origin of this crime, followed by Kenya, to a lesser extent. Locations given in fake profiles indicate that the most targeted countries are the USA (63 per cent), followed by the UK (11 per cent), Germany (3 per cent) and Canada (2 per cent).⁸³

Phishing

Despite different levels of reporting between African countries, phishing scams are increasingly opportunist scams that are likely spread on the continent and constitute a lucrative illegal activity for OCGs in Africa.

As defined by INTERPOL, phishing refers to when offenders send “fake emails/text messages/telephone calls purporting to be

from a legitimate source such as a bank or e-commerce site that are used to induce individuals to reveal personal or financial information”.⁸⁴ In Africa, phishing is widespread.

In 2017, it was reported that Southern Africa witnessed an increase in the phishing websites hosted on its infrastructure.⁸⁵ In this context, a 2018 survey conducted in South Africa showed that 90 per cent of respondents have fallen victims to security incidents resulting from a deceptive e-mail.⁸⁶ According to a 2018 Serianu study, the cost of phishing targeting businesses in Nigeria, Kenya, Ghana, Uganda, and Tanzania is estimated at USD 108 million.⁸⁷ In addition, the results of a 2019 survey conducted across the African continent show that 28 per cent of respondents from Eastern Africa, Northern Africa, Southern Africa and Western Africa, have fallen victims to a phishing email and 50 per cent have had a malware infection.⁸⁸

CASE STUDY

In April 2018, six offenders were arrested in France. The victim, having established a virtual love affair via a dating site, was driven to send 9000 euros in exchange for three checks that turned out to be stolen. To transfer the funds to Côte d’Ivoire, where the fraud was originating, the offenders used the services of occult bankers, prepaid cards and cryptocurrencies. After investigation, it appeared that 700 prepaid cards were involved, representing almost 3 million euros.

‘Rapport - l’état de la menace liée au numérique en 2019’, French Interior Ministry, 19 July 2019, <https://www.interieur.gouv.fr/content/download/117535/942891/file/Rapport-Cybermenaces2019-HD-web-modif%C3%A9.pdf>, (accessed 05 February 2020).

Advance-fee fraud and variants

Advance-fee fraud and its variants, including ‘Stranded Traveler’ fraud and unexpected money scams, are reportedly occurring across the African continent.

This type of scam occurs when the victim pays money to someone in anticipation of receiving something of greater value that was promised, mostly through online means—such as a loan, contract, investment, or gift—and then receives little or nothing in return.⁸⁹ The development and growth of mobile money in Africa has also contributed to the increase in advance-fee scams on the African continent.

‘Stranded Traveler’ fraud and other appeal for compassion scams could be perceived as variants of the Advance-fee fraud. This type of scam occurs when the offender takes control of a social network account to impersonate the account owner and asks contacts for emergency financial help, usually while overseas.⁹⁰

The unexpected money scam, which occurs when scammers offer the victim a large sum of money/inheritance/gift and trick them into parting with their money or sharing bank or credit card details, is another variant of the Advance-fee fraud.⁹¹

In Western Africa, advance-fee fraud is widely spread⁹² and payment is increasingly made via mobile money.⁹³ In Central Africa, advance payment is usually requested against precious gems, animals and works of art offered for sale online.⁹⁴ In Eastern Africa, similar schemes are reported with goods sold and paid for via mobile money transfers, where victims never received the goods.⁹⁵ In Northern Africa, in 2019, authorities warned about online fake job advertisement, fake lottery prize and fake charity call, operating on social networks such as Facebook or Twitter.⁹⁶ Similar scams are reported in Southern Africa as well.⁹⁷

Scammers also tend to exploit crisis situations for financial gain. In Cameroon, some victims received threatening emails and messages through social media, asking them to demonstrate that they have “chosen a side” in the Anglophone Crisis⁹⁸ by sending mobile funds to the scammer.⁹⁹

4.2. Trafficking in human beings and people smuggling

African OCGs likely use social networking sites in the process of trafficking and smuggling of African victims inter-regionally and transnationally.

The main online platforms used: *Facebook, WhatsApp, e-mails, Instagram, Haraj, 4Sales, Twitter, Telegram, etc.*

Human trafficking is a lucrative form of transnational organized crime, constituting modern-day slavery. The victims, considered as commodities by criminals, are targeted due to their vulnerabilities and trafficked between countries and regions using deception or coercion. Deprived from their freedom of movement and choice, they can be exploited for forced labor, forced criminal activities, sexual exploitation and removal of organs. Human trafficking is linked to a number of crimes, including illicit money flows, the use of fraudulent travel documents and cybercrimes.¹⁰⁰

According to Article 3 of the Smuggling of Migrants Protocol of the United Nations Convention Against Transnational Organized Crime, smuggling of migrants is the “the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident.” Migrant smuggling is closely connected to human trafficking, as some smugglers may exploit the migrants

while being smuggled. Unlike victims of human trafficking, migrants who pay a smuggler in order to illegally enter a country do so willingly, and the relationship between the two ends once at the destination.¹⁰¹

CASE STUDY

Between 21 and 31 January 2020, the INTERPOL-supported operation SARRAOUNIA in Niger led to the rescue of 232 victims of human trafficking, including 46 minors, who were saved from forced begging and sexual exploitation. The operation revealed that 180 male victims had been recruited online from Ghana and were promised 'decent work'. Traffickers also promised that travel fees and costs relating to the recruitment, including commissions, would be deducted from future wages.

Source: 'Niger: Police rescue 232 victims of human trafficking', *INTERPOL*, 26 February 2020, <https://www.interpol.int/News-and-Events/News/2020/Niger-Police-rescue-232-victims-of-human-trafficking> (accessed 01 July 2020)

In Africa, trafficking in human beings and people smuggling are of significant concern, with nearly all countries considered as source, transit, and/or destination countries. The 2018 ENACT threat assessment revealed that all forms of human trafficking, including sexual and labor exploitation as well as organ removal are occurring on the continent. In this same context, migrants moving illegally across the continent were found to be vulnerable to human trafficking and high levels of violence. The analysis also concluded that Northern Africa is a transit hub for migrants smuggled towards Europe.¹⁰²

Trafficking in human beings and smuggling of migrants, like other crimes, have benefited from the globalization and the emergence of

new technologies. The use of technology has led to the emergence of new organized structures with less or no physical contact between the supplier and customer, between members of OCGs, or between offender and victim. The African continent is no exception to this phenomenon. For example, a recent study demonstrated the existence of correlation between Internet growth and the increase in human trafficking in Rwanda, as it "provides a platform for traffickers to exploit the potential victims".¹⁰³

In Africa, human traffickers use the Internet to identify, recruit, coerce and control victims as well as to advertise the services or products resulting from their exploitation.

In Africa, human traffickers use the Internet to identify, recruit, coerce and control victims as well as to advertise the services or products resulting from their exploitation. They also use it to launder the illicit revenue earned from their activities. Migrant smugglers use the Internet for similar purposes. Evidence of human trafficking and people smuggling related to Africa was also found on the dark web.

4.2.1. Human trafficking facilitated online

Recruitment

OCGs in Africa use social networking sites to study the profiles of potential victims, tailor their approach towards them and eventually recruit victims online.

Criminals have access to a wide pool of potential victims online, using emails, instant messaging applications and social networking

sites, etc. The analysis of available information on potential victims online (i.e. location, contacts, images, personal taste, etc.) allows traffickers to tailor their approach to fit the victim's expectation and/or exploit their emotional vulnerability.

In its 2018 threat assessment, ENACT INTERPOL indicated that "women may be lured by fraudulent Internet marriage proposals or offers of well-paid jobs, and subsequently subjected to forced prostitution or forced labor within their countries and/or abroad, primarily in Europe and the Middle East."¹⁰⁴

A recent Europol public report revealed that "sexual exploitation is the most reported purpose for human traffickers in the European Union (EU) and that the non-EU national victims of the traffic are mainly originating from Nigeria." Nigerian networks, or confraternities, are known for the sexual exploitation of their female compatriots in Europe where they developed links with local criminal groups. They are involved in trafficking in human beings, and active in other criminal businesses linked to the crime such as fraud, corruption, migrant smuggling, forging documents and money laundering. Victims are recruited in their own country using false promises of jobs in Europe, and are often obliged to reimburse the 'free' trip to EU through prostitution. Abroad, they are controlled by their traffickers after being indoctrinated into voodoo beliefs and rituals.¹⁰⁵ Reports from the French authorities also confirm that Nigerian criminal confraternities use social networks "when recruiting future victims of human trafficking."¹⁰⁶

A 2019 report by the International Organization for Migration (IOM) warned about the increased number of women and girls being trafficked from Côte d'Ivoire to Europe and Northern Africa, suffering abuse,

slavery and prostitution. The report specifies that often, friends of the victim, relatives and people who attend their families carry out the recruitment. Traffickers also use social media to entice potential victims.¹⁰⁷ In Côte d'Ivoire, according to the US Department of State, human traffickers "often operate in well-established networks consisting of both Ivoirians and foreigners and, in cases of transnational trafficking, use social media, making networks difficult for law enforcement to detect".¹⁰⁸

In Western Africa, domestic servant trafficking networks typically involve destination-country recruitment agencies that use Africa-based intermediaries to fraudulently recruit the victims for work abroad.

In some cases, victims of human trafficking can be used to commit financial cyber-enabled crimes. In March 2019, a gang of Nigerian nationals was arrested in Dakar, Senegal. Their modus operandi was to exploit victims of human trafficking by using them to make online scams through social networking sites to deceive individuals in several countries, including Ghana.¹⁰⁹

In Central Africa, trafficking networks are often composed of local community members, including religious leaders as well as former victims who have now become perpetrators. They use the Internet and media to advertise jobs and eventually sell other Central Africans as domestic servants to families abroad.¹¹⁰ Similar MOs are perceived in Western Africa, where domestic servant trafficking networks typically involve destination-country recruitment agencies that use Africa-based intermediaries to fraudulently recruit the victims for work abroad.¹¹¹

In Central Africa, a specific modus operandi has been depicted. To attract their potential victims, OCGs use social media, WhatsApp groups advertised on posters in the streets, shops, universities, fake advertisement on e-commerce websites, etc. Typically, offers are fake proposals of work in Europe or in the Gulf countries, study opportunities in universities (i.e. in China, Cyprus, Italia, Turkey, etc.), or musical, fashion and modelling contests, fake online romance, etc. No matter the scheme, victims will have to pay important sums, send pictures and personal data required for the 'registration process', airline tickets, or the provision of forged passports. Based on the profiles of victims, traffickers select the ones to be smuggled for sexual or labor exploitation. In some cases, corruption of lawyers or law enforcement facilitates the process. The entire process is completed online through WhatsApp or Facebook.¹¹² In Eastern Africa, open sources report the use of online platforms to facilitate human trafficking and migrant smuggling. For instance, OCGs' members based in Burundi communicate with accomplices in the Gulf region through WhatsApp. They use fake job advertisements to traffic young girls in the Gulf countries, where they are reportedly sexually exploited.¹¹³

Human trafficking has been found to have a cyber-component in the Southern African region as well. Recruitment of both victims of domestic servitude or sexual exploitation occurs online, and related services are advertised and negotiated on a range of online platforms.¹¹⁴ In Zambia, WhatsApp and Facebook groups are also used to link people involved in prostitution and sex-buyers.¹¹⁵

Controlling victims

Technology allows traffickers to exert control over victims without meeting them personally. When contact is established via social media or

messaging applications, traffickers are able to manipulate the victims and exert a remote control over them. Threats and deception may be used by traffickers to gather compromising information on the victim (i.e. images, videos, etc.) as a means to gain control. In some cases, traffickers blackmail the victim, threatening them to send the compromising material to their relatives and families.

Advertisement and exploitation

Victims of human trafficking are considered as commodities and the Internet facilitates their exploitation. Open sources report that Internet websites and social networks platforms such as Instagram, Haraj and 4Sales allow the illegal buying and selling of victims of human trafficking from Eastern and Western Africa to be exploited in the MENA region as domestic workers. Users also share on these online platforms best practices and technics for controlling trafficked housemaids better by locking them in the house or confiscating their passports.^{116,117}

A recent study reports how Western African OCGs use online platforms to offer victims to potential customers in Europe. Advertisement with pictures of the victims are posted online and customers can arrange a meeting with the victims. They can also leave a comment or even evaluate the sexual services offered on Facebook and Twitter, where new potential customers can see this.¹¹⁸

4.2.2. Smuggling of migrants facilitated online

The Internet, and particularly social media, are likely used to facilitate migrant smuggling in Africa. According to the United Nations Office on Drugs and Crime (UNODC), smugglers use the Internet to promote their services by posting advertisements online including images, payment and visa modalities, etc. This typically occurs on Facebook groups used by

migrants. Usually, the potential customer can contact the smuggler using encrypted messaging applications.¹¹⁹

Social networking sites and applications such as Facebook, Viber, Skype and WhatsApp, are At the meeting point, she was identified by the smugglers and had to give the code.¹²⁰

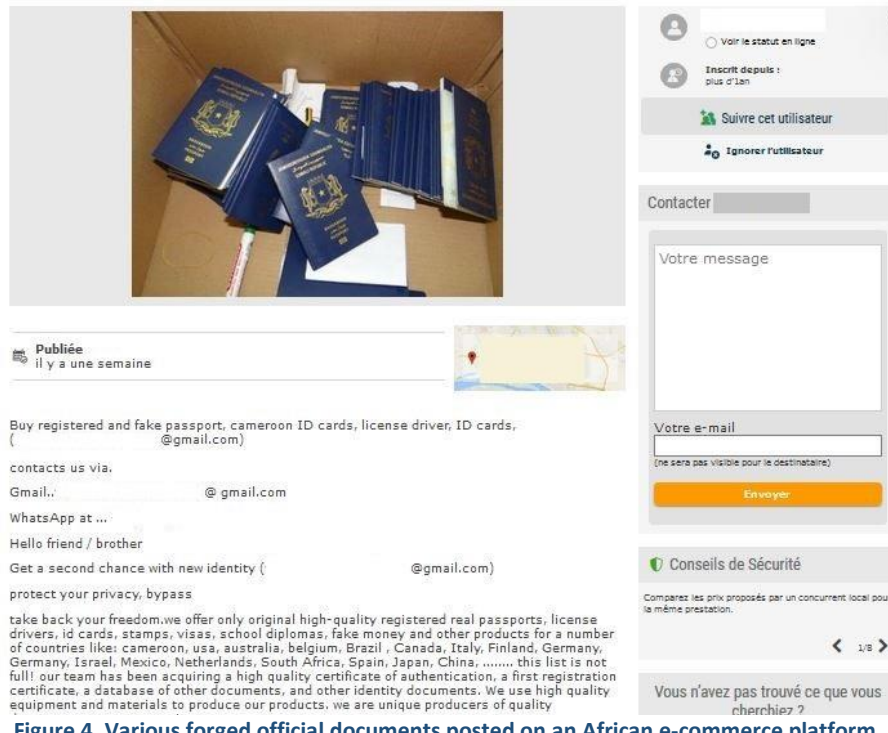


Figure 4. Various forged official documents posted on an African e-commerce platform

Migrants also use social media as ‘consumer forums’. To reduce possible risks before and during their travel, they consult reviews and feedbacks posted by other migrants to select the best route, avoid violent smugglers and compare prices and services.¹²¹ The use of social media such as Facebook, Viber, Skype and WhatsApp, both on mobile phones and computers, has been documented for smugglers from Eritrea and Ethiopia.¹²²

Sub-Saharan African migrants “tend to rely on personal connections and recommendations from friends or family members rather than gathering information from the social media or open sources” to cross the Mediterranean Sea. They often hire local smugglers recommended by fellow citizens who work with the smugglers.¹²³

Available information suggests that a migrant willing to travel is likely to be exploited by smugglers.¹²⁴ In some cases, the Internet is a way to blackmail the family of the migrant. The torture of migrants from Eritrea and Somalia, for example, was recorded and later sent to their families via social media in an attempt to have them released against the payment of a ransom.¹²⁵

4.3. Crimes against children online

African and non-African cyber criminals, some likely members of OCGs, use social networking sites to contact, solicit and sometimes blackmail their young victims as well as sell sexual materials produced.

The main online platforms used: *Facebook Messenger, e-mail, WhatsApp, Snapchat,*

Instagram, Skype, Telegram, Badoo, Gaydar, Afribaba, eDonkey, BitTorrent, Gigatribe, etc.

Children can be victims of various forms of violence, including trafficking, forced labor and abduction as well as sexual abuse and exploitation.

Child sexual abuse	Contacts or interactions between a child and an older or more knowledgeable child or adult (i.e. stranger, sibling or person in a position of authority such as a parent or caretaker), where the child is being used as an object for the older child's or adult's sexual needs. These contacts or interactions are carried out against the child using force, trickery, bribes, threats or pressure.
Child sexual exploitation	Child sexual abuse and/or other sexualized acts using children that involve an exchange of some kind (i.e. affection, food, drugs, and shelter). Child sexual abuse and child sexual exploitation are often linked.
Online child sexual abuse and online child sexual exploitation	Involves the use of the Internet as a means to sexually abuse and/or exploit children.

Table 1. Distinction between child sexual abuse, child sexual exploitation and online child sexual abuse and online child sexual exploitation

The Internet facilitates sexual exploitation and abuse of children by increasing the number of potential victims and expanding access to them, since it provides many means to contact and solicit victims. It also allows the exchange of information between child sex offenders and provides a space to share, buy and sell child sexual abuse/exploitation material.

The African continent is not spared from this developing phenomenon. In 2013, End Child Prostitution, Child Pornography and Trafficking (ECPAT) conducted a youth-lead survey to prevent sexual exploitation online in Central Africa, Eastern Africa, and Western Africa. At the time, 54 per cent of children had seen someone of their age in pornographic material online and about 10 per cent of children had been approached by online contacts to share sexualized images. It is estimated that these percentages have continued to increase over the years.

A 2019 report by the African Child Policy Forum (ACPF) and the OAK Foundation, suggested that the rise in child sexual exploitation in Africa draws on two trends: the development of Information and Communications Technology (ICT) and travel, which allow abusers to commit their crimes online as well as offline. The report notes that this fast-growing form of crime affects many countries across the continent, particularly those that benefit the most from Internet coverage. The lack of adequate legislation in most African countries aiming at protecting children in cyberspace further exacerbates the problem on the continent.

In Western Africa, according to recent reports, young girls are recruited to take part in pornographic films and bestiality. Eastern Africa also witnesses this type of crime. In Kenya, children of single parents and those living in urban slums are the most exposed to

pornographic material, making them the most vulnerable to sexual exploitation online. In Uganda, a high number of children is estimated to be victims of sexual child abuse weekly through videos, photos and films, sometimes linked to 'ekimansulo', a form of strip dancing. In South Africa, reports indicate that girls have fallen victims to men that they met online and later were sexually abused and exploited by them. Countries in Eastern Africa, Southern Africa, and Western Africa have reported of tourists sexually abusing children and producing child pornography material.

Below are some of the most popular MOs of child sexual exploitation found across the African continent.

Online grooming

Online grooming is witnessed across the African continent. This modus operandi refers to when an adult, most often male, befriends a child with the aim of sexually abusing him/her. The adult uses social media platforms and communication applications to access children's accounts and choose their potential victims. Using the information gathered on their target (i.e. interests, family, social situations, etc.), criminals initiate contact with the child and try to gain their friendship and trust. Generally, the perpetrator also seeks to assess the risk of being detected, and/or to convince the child to keep their relationship secret. The final aim is to sexually abuse and/or exploit the child, offline or online. Cases of

Members of the 'diva clubs' communicate mainly online using social media platforms such as WhatsApp, Facebook Messenger, Snapchat and Instagram. They mostly share stories and photos of socialization, including sexual experiences.

online grooming have been reported in Eastern Africa and Western Africa.

In Western Africa, a survey shows that 70.8 per cent of the victims are contacted on social media platforms including Facebook, Badoo, Gaydar and Afribaba, for discretion. In Eastern Africa, online grooming involves individuals and OCGs using social media platforms. Sources indicate that the emerging trend of 'diva clubs' involves girls in secondary schools getting invited by current or former students and associate adults. Members of the 'diva clubs' communicate mainly online using social media platforms such as WhatsApp, Facebook Messenger, Snapchat and Instagram. They mostly share stories and photos of socialization, including sexual experiences.

Production of child sexual abuse/exploitation material

Cases of child sexual exploitation and sextortion are increasingly reported across the African continent. Child sexual exploitation and abuse material is the "representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child for primarily sexual purposes".¹²⁶

These representations (i.e. images, videos) are distributed via e-mail, instant messaging applications, chat rooms, peer-to-peer file sharing networks (i.e. eDonkey, BitTorrent, and Gigatribe), social media platforms, and unencrypted and encrypted communication applications (i.e. Skype, Telegram and WhatsApp). Child sexual exploitation and abuse material is also traded on password-protected sites, bulletin boards and forums, on the visible, deep and dark web.

According to open sources, a large number of cases of sale or diffusion of child sexual abuse/exploitation material is reported in Eastern Africa, Southern Africa, and Western Africa.

Sextortion cases, when child exploitation material is used to blackmail the victim, have been also reported in Eastern Africa and Western Africa. Typically, children are asked to pay a certain amount of money, or the material will be published online.

In a survey conducted in Western Africa, young girls between 14 and 17 years confided that they were approached by individuals in order to take pictures or film them naked. In total, 2.8 per cent of the children surveyed said that they were involved in child sexual abuse or exploitation material. Despite this low percentage, several cross sources show that the circulation of material is increasingly popular in the Ivorian society and develops through easy access.

Live streaming of child sexual abuse

Streaming of child sexual abuse is increasingly perpetrated in Africa. This criminal activity can occur on online chat rooms, social media platforms and communication applications. Viewers can be passive (i.e. they pay to watch) or active (i.e. they pay to communicate with the child, the sexual abuser, and/or facilitator of the child sexual abuse). Open Sources suggest that live streaming of child sexual abuse is perpetrated in Eastern Africa and Southern Africa.¹²⁷

Role of social networks

Social networking sites facilitate a wide range of activities linked to online sexual exploitation in Africa. In Southern Africa, social networks have facilitated exploitation of children for prostitution with Facebook as the main platform used due to its free nature and lack of oversight. Social networks have also enabled the sexual exploitation of minors. Fake online advertisement for modelling jobs or material goods lead minors into prostitution networks. Social networks also permit abusers to access online services easier, making child exploitation even more profitable.¹²⁸

The growing phenomenon has prompted police authorities in some African countries to develop policies and strategies to combat this form of crime. In Kenya for example, authorities expanded their Police Child Protection Unit to include an online/cybercrimes unit in August 2018 to monitor and arrest suspected perpetrators of child abuse and exploitation.¹²⁹

4.4. Trafficking in works of art online

African OCGs, mainly North African, are likely using social networking sites to facilitate the looting and trafficking of stolen works of art across the continent but also transnationally.

The main online platforms used: *Facebook, Instagram, etc.*

Trafficking in works of art is an increasingly attractive activity for OCGs as there is a high market demand for cultural objects, which makes their illegal commerce profitable. Due to poor socio-economic and security conditions in some regions, these objects are fairly easy to obtain through theft, illicit excavation and removal of cultural property. In addition, regulations and detection are not very effective due to the interrelatedness between the licit and illicit antiquity sectors.

The African continent is more and more affected by the illicit trafficking in cultural heritage,¹³⁰ which is increasingly being facilitated by the use of Internet and social media.

In Northern Africa for example, Internet and social media facilitate looting as well as trafficking in works of art.¹³¹ According to the 2018 ENACT threat assessment of Serious and Organized Crime in the Southern African Region, works of art are mostly trafficked from the African continent to Europe, North America and the Gulf states.¹³²

Looting

OCGs are increasingly using social networking sites, such as Facebook, to foster works of art looting in Africa. According to research online, Facebook pages or groups are dedicated to looting and sharing information on how to illegally dig and find tombs, as well as the types of material to look for.

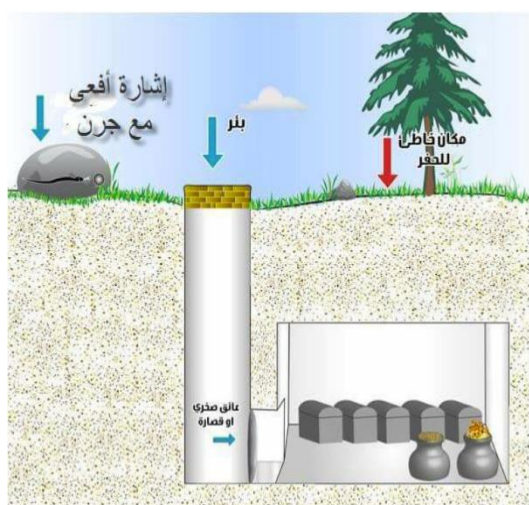


Figure 5. An infographic in Arabic on how to access and loot a Roman tomb posted on Facebook

For example, in October 2017, a member of a Facebook group posted on the group page detailed instructions on how to find and steal Roman tombs, including the material the looter should expect to find (see figure 5).¹³³ Featured photos were attached to the instructions. Analysis indicated that soon after this was posted, material relating to the Roman-era were posted on the same page.¹³⁴

Sellers also post on these groups photos of sales made by major auction houses in order to select items, according to market demands (see figure 6).¹³⁵

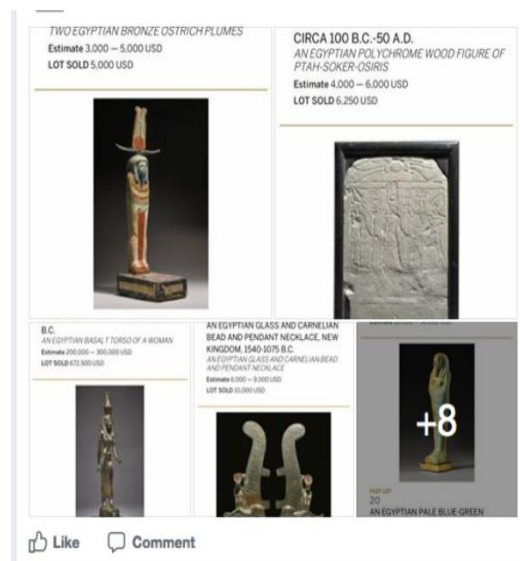


Figure 6. Sample of auction house catalogue showing works of arts as a reference for looters

Trafficking

Northern Africa emerges as a hub for trafficking of works of art in Africa, based on available social networking data. The online sale of works of art is not the main method used by traffickers. Illicit cultural property is mainly sold through art dealers and galleries, auction houses, newspaper adverts, flea

markets and antique shops. However, Internet facilitates and boosts the trafficking of artefacts.¹³⁶ ¹³⁷ An increase of this phenomenon has been noted according to the United Nations Educational, Scientific and Cultural Organization (UNESCO).¹³⁸

The online sales of cultural objects can be operated in two different ways:

- Business to consumer (B2C): companies sell directly to the public (Internet dealers) and/or organize online auctions (Internet auctions);
- Consumer to consumer (C2C): an individual sells an artefact to another individual.

Internet platform providers, which usually charge a flat fee or commission for this activity,

are considered to be intermediaries.¹³⁹ Online sellers also use social media sites, such as

Facebook, to complete deals (see figure 7).¹⁴⁰
¹⁴¹.



Figure 7. Facebook page offering ISIS plunders for sale

According to UNESCO, “most of the objects offered for sale on the Internet do not have authentic documentation”. The lack of documentation is an useful factor to identify an artefact that have been obtained through illegal excavation and offered for sale in violation of relevant national legislation.¹⁴² Most often, online C2C sellers do not provide export permission from the country where the object is located at the time of sale.

B2C websites are also affected by the sale of illegally exported works of arts and antiques. In 2016, MILLON, a French auction house listed Egyptian antiques in its online catalog. After investigations, it appeared that the objects had been declared stolen and were returned to Egypt.¹⁴³ Social media sites,¹⁴⁴ such as Instagram¹⁴⁵ or Facebook groups dedicated to trafficking, are used as online marketplaces, mainly to facilitate and arrange the moving of pieces and establish connections between buyers and middlemen/women. Some members of the groups make also loot-to-order requests.^{146 147}

The examination of the members’ profiles of some of these Facebook groups identifies the

origin of some of the traffickers as the Middle East and North Africa, including Algeria, Egypt and Morocco, in addition to locations outside the region. The online sale attracts users from Europe as well as the USA. The analysis also reveals that most users appear to use their personal Facebook profiles when engaging in the aforementioned activities.¹⁴⁸

Open sources suggest that Northern Africa,¹⁴⁹ ¹⁵⁰ in particular Egypt,¹⁵¹ is the most affected region in Africa by this type of crime. As previously mentioned, a great deal of Egyptian artefacts were found to be sold via Facebook. The International Council of Museums (ICOM) also documented sales of Egyptian artefacts on eBay.¹⁵² In May 2018, media reports indicated that a specialized unit of the Tunisian police had dismantled an antiquity trafficking network operating on the dark web. The group, which was composed of 6 persons

based in Tunis, attempted to sell Hebrew manuscripts of great historical value.¹⁵³

A recent study on the trafficking of illicit antiquities on Facebook, including mosaics, architectural elements, and pharaonic coffins, confirms Northern Africa as a hub on the continent, based on sale offers posted in a number of Facebook groups. Group members from Côte d'Ivoire, Mauritania, Nigeria, South Africa and Sudan also made offers on group pages. The study uncovers a transnational network of traffickers with active members based in Northern Africa. The network was composed of "488 individual administrators controlling a total of 1,947,195 members across 95 Facebook groups". Members of the groups appear to be average citizens, middlemen/women as well as violent extremists.

Figures 8 and 9 are screenshots taken in the framework of the study, showing a variety of illicit items offered on the platform.¹⁵⁴



Figure 8. Photos offering a large church bell posted by a user in Zintan, Libya



Figure 9. Photos of a tombstone still in situ posted by a user in Tunis, Tunisia

4.5. Environmental crimes online

African OCGs, almost certainly connected with transnational counterparts, are increasingly using social-media based trade for IWT through the help of middlemen/women.

The main online platforms used: *Facebook, Instagram, WhatsApp, Twitter, e-commerce platforms, Jiji.ng, Nairaland, etc.*

In a 2017 report, the International Fund for Animal Welfare (IFAW) examined the availability of wild animals and their products on online marketplaces and social media platforms in Ethiopia, Ivory Coast, Kenya, Nigeria, South Africa, Tanzania and Uganda or used by traders that indicated they were based in these countries. The study found endangered and threatened wildlife advertisements across 33 online marketplaces and 3 social media platforms across seven African countries, offering 9,481 specimens of animals evaluated at approximately USD 5,828,608. The study also highlighted Nigeria and South Africa for having significant levels of protected species trade with respectively 72.5 per cent, and 22 per cent of the advertisements linking back to them. In contrast, Côte d'Ivoire, Ethiopia, Kenya, Tanzania and Uganda had very little wildlife for sale online.¹⁵⁵

According to the study, Kenya is “one of the world’s major sources of trafficked wildlife products¹⁵⁶” and experiences a high Internet access rate.¹⁵⁷ However, in the IFAW study, Kenya only accounts for 2.9 per cent of the endangered and threatened wildlife advertisements found online. The study revealed that East African countries, including Ethiopia, Kenya, Tanzania and Uganda only represented 36 advertisements out of the 990 retrieved, corresponding to 3.6 per cent of the total.¹⁵⁸ Moreover, it is worth noting that

TRAFFIC has identified Tanzania as a key country regarding wildlife cybercrime.¹⁵⁹

The study revealed that 90 per cent of the advertisements were posted on e-commerce platforms. Wildlife trade was found on social media in Côte d'Ivoire, Nigeria and South Africa.¹⁶⁰ In addition, some studies have already noted a shift of traders from e-commerce platforms towards more discreet social media platforms on the deep web. It is probable that such a phenomenon occurs in the studied countries, in particular in regions that witness a strengthening of control and enforcement on local e-commerce platforms.

Western Africa

In its 2018 threat assessment, ENACT indicates that in Western Africa, OCGs tend to “use the Internet to offer and sell their illegal products”.¹⁶¹ In Nigeria, according to open sources, local criminals are using social networks or online platforms such as the free classified site Jiji.ng (where ivory trade is permitted), business directory Vconnect.com or the online forum Nairaland to advertise pangolin scales and ivory artefacts. Buyers have been identified as rich Nigerians, Asians and Europeans living in Nigeria.¹⁶² Open sources recently reported ongoing activity on Facebook of pages selling illegal wildlife products such as pangolin scales, from Western Africa to Asian markets.¹⁶³ It is worth mentioning that some of these illicit traders are former ‘Yahoo Boys’, Nigerian online scammers well-known for their 419 scams. It is likely that these criminals expanded their illegal activities online due to the “general decline in proceeds from 419 scams and growing police trouble.”¹⁶⁴ They act as middlemen/women in real life now, bringing their customers who have been contacted online to the Jakande Ivory Market in Lagos, to check out the products. However, the level of dependency of these middlemen/women in

their role on the Internet cannot be confirmed.¹⁶⁵

Multiple reports also indicate traffickers using social networking sites (i.e. Facebook and Instagram) to trade Pangolin scales online. In Nigeria, Pangolin traders are moving to online undergrounds for business, and increasingly adhering to code languages and temporary contact numbers.¹⁶⁶ In this context, middlemen/women place the advertisement online to demonstrate their access to products to buyers.¹⁶⁷ A representative of the Nigerian Conservation Foundation (NCF) points out in this regard that after contact is initiated online, locals based in Nigeria and other African countries are contacted to provide the requested pangolin parts. Products are later sent via seaports to buyers, mostly in Asia.¹⁶⁸

The use of multiple languages, the privacy setting options, the use of code languages and the lack of technology to make species identification in photographs easier further complicates enforcement measures.

Central Africa

According to open sources, several wildlife specimens, including African Grey parrots, one of the most trafficked birds, were recently advertised on several social networking sites such as on WhatsApp, Weibo, Facebook, and Instagram. Data collected suggests that social network facilitates trafficking mainly from Central Africa, but also from Eastern and Western Africa to Asia, Europe, the Middle East and the USA.¹⁶⁹

Sources from Central Africa indicate that many wildlife products offered online for sale often turn out to be scams. After having received the payment, the offender breaks all ties with the victim. For example, cases of scams involving monkeys were reported.¹⁷⁰

In another example relating to the region, UK-based customers ordered chimp skulls online from Cameroon-based hunters. These skulls were by-products of traditional Cameroonian hunting practices. However, Cameroonian hunters have likely increased production with the emergence of new demands in the West.¹⁷¹

Southern Africa

Endemic reptile's trade online is common in Madagascar. The species is increasingly traded via social media sites. With minimal internal monitoring and the possibility to control members within a closed group, social media is facilitating the access to global markets such as in China, Europe, Southeast Asia and the USA. Similarly to other wildlife trade areas, a shift from e-commerce platforms to more discreet Facebook and WhatsApp groups has been noted. The use of multiple languages, the privacy setting options, the use of code languages and the lack of technology to make species identification in photographs easier further complicate enforcement measures.¹⁷²

In the social media-based trade, middlemen/women are expanding trading networks by reposting information of the illegal products on their own platforms, and in case an individual from their circle is interested in buying the product, the middle-agent buys it and resells it to the contact in their circle at a higher price. This is practiced remarkably on social-media platforms operating in China. Actors involved in this trade were not identified as part of OGCs or centralized and hierarchical networks. Rather, the study identifies traders as private individuals and buyers of reptiles as 'enthusiasts' and individual collectors.¹⁷³

However, connections between individual online species sellers and underpinning OGCs active in Madagascar cannot be excluded as open sources report significant seizures of specimens that suggest a likely organized

effort to be completed. Such cases include the April 2018 seizure of nearly 10,000 tortoises¹⁷⁴ and the January 2018 combined seizure of tortoises and illegal drugs (3.5 kilos of cannabis) in the coastal city of Toliara.¹⁷⁵

4.6. Illicit trade in diamonds online

Illicit diamond traders likely use communication and social networking sites to reach the global market and possible new partners.

The main online platforms used: *Facebook, Messenger, WhatsApp, etc.*

In its 2018 threat assessment, ENACT INTERPOL indicates that diamonds “illicitly mined from Central African countries are often smuggled, traded and trafficked within and beyond the region providing a means for criminals and OCGs to gain, conceal and move illicit funds”.¹⁷⁶

A recent report reveals that illegal diamond trafficking from Central African Republic is facilitated by online communication tools and social networks. Sources indicate that smugglers and middlemen/women active in the region use Facebook, Messenger, and WhatsApp (see figure 10). Through social networking sites, they activate the supply chain and introduce the available diamonds to the global market. It is also how they find new trading partners.



Figure 10. Photo of diamonds posted by a dealer on social media

Diamonds transit via countries neighboring the Central African Republic including, Chad, Democratic Republic of Congo, Cameroon and Sudan before getting transferred to destination countries such as Belgium, Brazil, China, France, Israel, Lebanon, Liberia, Qatar, Sierra Leone, South Africa and the UAE. Diamond middlemen/women reportedly originate from India and/or Lebanon. Smugglers are reported to be Central African Republic nationals and nationals of neighboring countries.¹⁷⁷

4.7. Trafficking in small arms and light weapons online

OCGs active in SALW trafficking in Africa are increasingly using social networking sites to conduct trade. They are likely engaged in other online criminal activities as well.

Initial contact starts on Facebook groups but then negotiations are conducted via more private means, such as telephone and secure messaging mobile applications.

The main online platforms used: *Facebook, WhatsApp, Instagram, Telegram, etc.*

The trafficking of weapons and small arms across Africa is a significant criminal threat. Firearms enable a range of criminal behaviors including, armed robbery, kidnapping, hijacking, terrorism, piracy, genocide, war crimes, and crimes against humanity.¹⁷⁸

Many, if not all African countries, are affected at various degrees by the proliferation of SALW. Many African countries are source, transit and destination points for the trafficking of weapons. The 2018 ENACT continental threat assessment suggests that SALW trafficking is often linked to post-conflict countries or to those plagued by internal armed conflicts, where weapons influx are

frequent. In Africa, trafficking of firearms is a major crime facilitator and enabler, and armed groups appear to be among the major actors responsible for this illicit trade.¹⁷⁹

Multiple sources report that the Internet, in particular social media platforms, are used to sell or buy arms and weapons. In Libya, following the fall of the Qaddafi regime in 2011, two factors favored the emergence of online markets. On the one hand, access to the Internet, previously strictly regulated, increased and led to an important growth in social media use. On the other hand, the illicit flow of arms fostered the development of black market sellers, with firearms being traded openly in marketplaces in major Libyan cities. Soon, traffickers moved to social media to expand their illegal activities. An example of such markets is 'The Libyan Firearms Markets'.

Small Arms Survey examined six Facebook groups, most of which were 'closed' or 'secret' groups. The level of activity varied between groups with the number of members ranging between 385 to nearly 14,000 members. Users appeared to be mostly males, in their 20s and 30s. Similarly to other crime areas, initial contact would start on these groups but then negotiations are conducted via more private means, such as telephone and secure messaging mobile applications. Payments were found to be made in cash and buyers were mostly from Libya as well as other Northern African countries and Sudan.

Some platforms that explicitly forbid private sales of firearms managed to close some of these groups. However, not long after shutting a group down, another would emerge gathering members from the former group.

The analysis suggests that online trading in firearms appears to be an extension of the physical black market in Libya. Online trading attracts four types of customers, namely the persons buying for self-defense and hobbyist

reasons, small-scale traders (mostly individuals), large-scale traders (mostly linked to physical shops), and traffickers linked to non-state armed groups.¹⁸⁰

The study reveals that online illicit arms markets in the Middle East and North Africa will continue to grow and increase in volume of sales.¹⁸¹ Also, in addition to Facebook, illicit trade could be conducted via WhatsApp, Instagram and Telegram.¹⁸²

Finally, members found on the aforementioned Facebook groups were also offering other items in addition to firearms, such as electronics, used vehicles, forged passports, counterfeit currency and trafficking of migrants' services. It is possible that these individuals are part of established OCGs operating in the region and active in multiple crime areas, including trafficking of SALW.

4.8. Drug trafficking online

OCGs active in Africa probably use the Internet to sell drugs and contact local as well as international customers/providers. The main online platform used: *anonymous networks, chat rooms, social media platforms, online messaging applications, etc.*

The African continent is a growing global transit hub for the trafficking of a large array of drug commodities en route to other continents. It is also a developing market where drugs are increasingly abused.¹⁸³ In Africa, illicit narcotics and legitimate drugs (pharmaceuticals) are being sold and bought online, on the surface, deep and dark web.¹⁸⁴

The use of the Internet to facilitate drug trafficking in Africa is growing.

Open sources confirm that the use of the Internet to facilitate drug trafficking in Africa is growing. According to an ENACT study, "the

illicit financial transactions of continental drug economies are increasingly taking advantage of secure innovations such as blockchain technology, cryptocurrencies and dark net trading platforms.”¹⁸⁵

Multiple reports show that drug traffickers are using the Internet in various ways to further their activities, including:

- Chat forums, allow Internet users to exchange new addresses of crypto-markets, as well as opinions on sellers and products. Illegal transactions are not openly practiced on these forums;¹⁸⁶
- Online sale, practiced mostly on the dark web through vendor shops and online markets on anonymous networks, but also on social media platforms, and on online messaging applications.¹⁸⁷

Payment methods for these activities include cryptocurrency, money remittance services, traditional banking, etc. In Western Africa,¹⁸⁸ an increase in advertisements and selling of

drugs online has been noted on the surface and dark web. Drugs are ordered online and later transported in parcels to customers through traffickers.¹⁸⁹

In the Southern Africa region, the Internet is also used to sell drugs. In the 2018 ENACT regional threat assessment, it was reported that “once cocaine has been supplied to street-level traffickers, the most common method of distribution on the streets to users is through open markets with the use of drug orders over the phone or with the use of Internet-based communication platforms”.¹⁹⁰

Overall, traffickers on the continent use the Internet to sell drugs locally or to contact customers. In addition, according to open sources, cases of international deliveries ordered via the Internet have been reported. Also, khat from the Horn of Africa region appears to be regularly mailed to France after online orders.^{191 192 193} Moreover, the Internet is used to order chemical products used for the production of synthetic drugs. In Mauritius for example, precursors are ordered online,

420 Monkeys Weed & Edibles
Make Winter colorful

Local R10 p/g Grinded

- ◆ Skunk (S)

Outdoor R40 p/g

- ◆ Durban Poison (S)
- ◆ Gorilla Glue (H)

Green House R60 p/g

- ◆ Chernobyl (S)
- ◆ Pineapple Express (S)
- ◆ Sour Diesel (S)
- ◆ Sour Willie (S)
- ◆ Strawberry Cough (S)
- ◆ Cheese (I)
- ◆ Cookie Monster (I)
- ◆ Lavender Kush (I)
- ◆ OG 18 (I)
- ◆ Pitbull (I)
- ◆ Area 51 (H)
- ◆ Chronic (H)
- ◆ Space Candy (H)

Indoor R150 p/g

- ◆ Cinderella 99 (S)
- ◆ Durban Poison (S)
- ◆ Jack Herer (S)
- ◆ Blueberry (I)
- ◆ Coffee Super Cheese (I)
- ◆ Purple Afghan Kush (I)
- ◆ Super Bud (I)
- ◆ Super Cheese (I)
- ◆ Blue Kush (H)

Aquaponics R300 p/g

- ◆ Bruce Banner (S)
- ◆ Strawberry Cheesecake (I)

Vaping

- ◆ THC Smoking Pen 0.5ml THC (Pen, Cartridges & Charger) - R900
- ◆ THC Smoking Pen Cartridge 0.5ml - R700
- ◆ Vapresso Pod Device - R650
- ◆ Vapresso Pod Device with THC 2ml Vape distillate - R1100
- ◆ Distillate Vape THC Liquid (10ml) - R700
- ◆ Distillate Vape CBD Liquid (30ml) - R600 (With Nicotine)

Medical

- ◆ RSD/Feco Oil (1ml) - R150
- ◆ Micro-Dose Shrooms (30 capsules) - R800
- ◆ Canna Caps:
 - 15mg - R400
 - 25mg - R500
 - 50mg - R700
 - 100mg - R900
- ◆ Canna Ointment - R550
- ◆ Canna Cream - R600
- ◆ Spectrum Canna Drops:
 - 10ml - R400
 - 30ml - R800
- ◆ 10ml THCA Drops - R550

Bongalongs Bongas

- ◆ Buddy Bong - R500
- ◆ BuddyLong - R600
- ◆ Potjie Bongas - R699

All Bong colours: Yellow, Dark Blue, White & Black

Miscellaneous

- ◆ Bubble Hash - R150 p/g
- ◆ Black Shatter Wax - R150 p/g
- ◆ Kiev - R150 p/g
- ◆ Greenhouse/Indoor Mix - R80 p/g
- ◆ Distillate Syringe (Dab or THC pen refill) - R900
- ◆ Infused Vodka (750ml) 2000mg - R750
- ◆ Dry Herb Smoking Device - R600

Edibles

- ◆ 500mg Biscuit (Very Strong) - R120
- ◆ Lollipop (100mg) - R40
- ◆ Gummies (250mg) - R100
- ◆ Pocket Rocket Sweets (200mg) - R50

4:20 MONKEYS

Details:
Visit our Website:

(S) Sativa; (I) Indica & (H) Hybrid

Figure 11. Cannabis card of an online drug dealer in South Africa

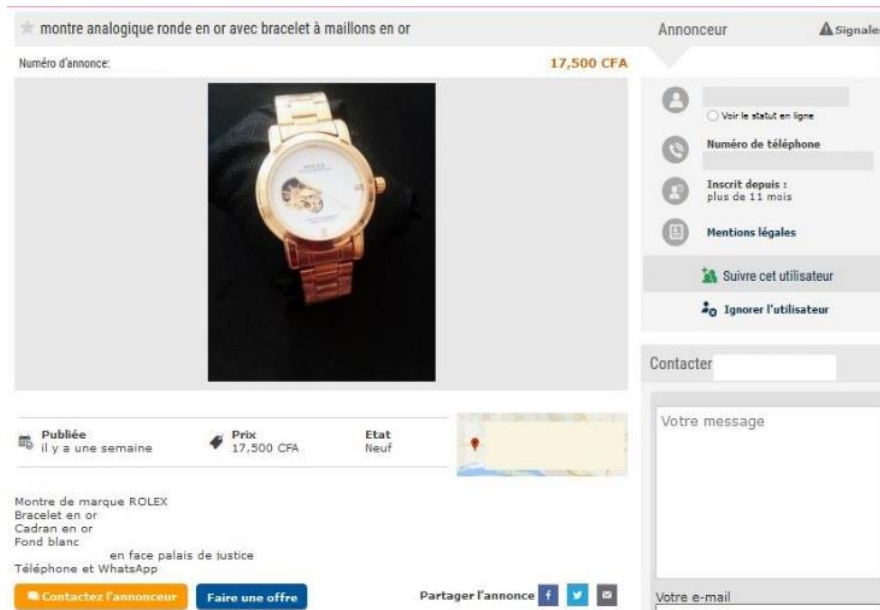


Figure 12. Counterfeit Rolex watch advertised on an African e-commerce platform

imported from China and used on the island to create new psychoactive substance.¹⁹⁴

4.9. Trafficking in counterfeit goods online

Trafficking in counterfeit goods is very common on the African continent; and with the increase in Internet coverage, online trade of illicit goods is likely increasing on the African continent. OCGs play a central role in the trade of counterfeit and pirated goods and generate important revenues from such illicit markets in Africa.¹⁹⁵ In addition, this type of trafficking facilitates money laundering and as a result provides fronts for OCGs to invest proceeds procured illegally.¹⁹⁶ Available data suggests that by the year 2022, it is estimated that the total value of piracy and counterfeiting could

Among products subject to counterfeiting in Africa, counterfeit pharmaceuticals are trafficked the most across Africa.²⁰³ According to the World Health Organization (WHO), between 2013 and 2017, 42 per cent of detected cases of substandard or falsified pharmaceuticals occurred in Africa. As a consequence, every year, around 100,000

reach a staggering USD 2.3 trillion with a negative global impact of USD 4.2 trillion.¹⁹⁷

In Africa, many products, such as software, currencies, apparel, consumer electronics, automotive parts, pharmaceuticals, food and drink and chemicals, are affected by counterfeiting and piracy.¹⁹⁸⁻¹⁹⁹ Trafficking in counterfeit products is conducted physically and online. A wide range of counterfeit products are advertised and sold on the Internet.²⁰⁰ The increase in Internet connectivity and availability of cyber-tools nowadays allow traffickers of counterfeit goods to access a huge and global market place.²⁰¹ For example, in South Africa, about 30 per cent of consumers admitted to unknowingly buying fake goods when making online purchases.²⁰²

individuals die in Africa as a result of counterfeit products. These fake drugs account for approximately 30 to 60 per cent of the total market of pharmaceuticals on the continent.²⁰⁴⁻²⁰⁵

Traffickers use the Internet to trade counterfeit goods in different ways, including:

- Spam,²⁰⁶ online advertisement,²⁰⁷

- Fake Internet sites similar to legitimate ones;²⁰⁸
- Forums;
- Manipulation of search engines.²⁰⁹

According to UNICRI, online advertisement, through the use of spam, has become one of the main means used by criminals to lure their potential victims and boost their sales. Spammers - recruited by or members of OCGs - tailor the products offered depending on online users' preferences and information,²¹⁰ which allow them to maximize the chances of the user buying the products.²¹¹ This is how online counterfeiters create online 'bazaars' that offer replicate goods.²¹²

A study conducted by the pharmaceutical company Sanofi in 2018 on more than 2500 individuals from Côte d'Ivoire, Egypt, Kenya, Nigeria and South Africa, revealed that 23 per cent of participants have already bought medicine online and 65 per cent of them admitted to taking a risk while purchasing online.²¹³

Coordinated by INTERPOL, Operation PANGEA is an international effort to disrupt the online sale of counterfeit and illicit health products. PANGEA also works to raise awareness of the risks associated with buying medicines from unregulated websites. Twenty-two African countries²¹⁴ took part in PANGEA.^{215 216}

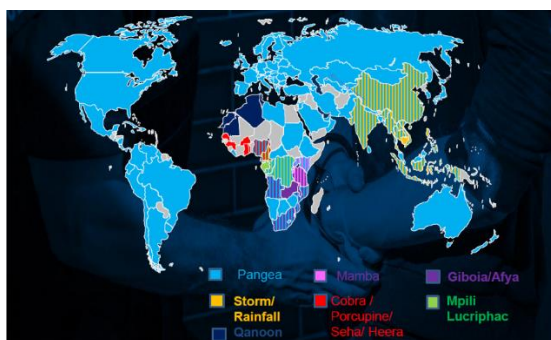


Figure 13. Map of INTERPOL operations against pharmaceutical crime since 2008

Since its launch in 2008, the Operation has removed more than 105 million units (including pills, ampoules, sachets, bottles, etc.) from circulation and made more than 3,000 arrests. The operation also shut down 82,000 websites.²¹⁷

Considering the limited available data, it is difficult to estimate the link between trafficking in counterfeit products and the use of the Internet on the continent. However, given the ease and increase in the use of the Internet and individuals reporting buying products online in Africa, in particular pharmaceutical products, in addition to the number of websites shut down by PANGEA, it is likely that online trade in illicit products in Africa is increasing.

4.10. Trafficking in stolen motor vehicles online

OCGs active in Africa are likely increasingly using the Internet to complete various stages of the process of trafficking in SMV. OCGs rely on SMV to support their criminal activities, such as trafficking in illicit goods, drugs and firearms, people smuggling, etc. SMV is also considered a currency in drug deals, a system which bypasses traced money transactions. For OCGs, the acquisition, shipment and trade of SMVs is also a low-risk way to make profit.²¹⁸

In Africa, there are two dimensions of trafficking in SMV: international trafficking originating abroad (i.e. Asia, North America and Western Europe) towards the African continent as well as intracontinental trafficking. OCGs are responsible for the movement, theft and resale of large volumes of SMV throughout Africa. Many countries are at the same time, source, transit and destination points for SMV. All involved actors generate high volumes of profit which allow them to continuously fuel the trade in this commodity. Additionally, the illicit market in

spare parts is a lucrative source of income for criminal organizations. Not only does this phenomenon have a financial impact on the industry, but it also puts drivers in danger as illicit spare parts are likely to fall below recognized safety standards.²¹⁹

OCGs involved in this criminal market use illegitimate websites to deceive genuine buyers that pay online for non-existent vehicles.

The Internet and social media can facilitate SMV trafficking in various ways, including:

- Electronic cars: criminals are able to program blank key fobs to start cars, using key-programming devices meant for locksmiths and car dealerships.²²⁰ These machines can be bought online for a few hundred dollars.²²¹
- Forged identification documents and license plates as well as other vehicle parts;
- Sale of stolen cars;
- Resale of illicit vehicle components.²²²

In Western Africa, vehicle crimes involve fraud and the use of forged documentations, particularly false VINs, which make them difficult to detect by customers and resellers. In addition, OCGs involved in this criminal market use illegitimate websites to deceive genuine buyers that pay online for non-existent vehicles.²²³

Online fraud involving SMV has been witnessed in the Southern Africa region as well. It is reported that genuine buyers of vehicles have been defrauded by criminals in a number of schemes. Cases of imported vehicles diverted to other destinations following Internet scams have also been reported. Some financial transactions to sellers

have been rerouted or manipulated by criminals for deposit into other third party or anonymous accounts. OCGs have been found to use Internet auction sites to sell stolen and cloned vehicles, false identification documents, license plates, and other vehicle components.^{224 225}

5. DARK WEB

5.1. Background

Despite a widespread belief, the dark web is not a modern concept. In 1969, a University of California, Los Angeles (UCLA) student sent the first electronic message using a computer and the ARPANET system, a predecessor to the modern Internet. Soon after that, Internet users created covert networks or dark nets, using the ARPANET system; and in early 1970's, the first e-commerce transaction took place between university students.²²⁶ It was a drug deal. The network allowed students to keep their dealings secret and undetected.

Throughout the 1980's, with computers becoming more and more available for personal purchases, worries about storing data increased and data havens²²⁷ emerged as possible solutions. In the 1990's, the World Wide Web became popular and new technologies were introduced, such as peer-to-peer transmission of data using the Internet, mostly for compressed music. Also, the 'Onion routing', an online communication system first developed by the US Naval Research Laboratory to protect military intelligence, saw light.

In the early 2000's, the Freenet software²²⁸ was launched, a peer-to-peer platform that allows uncensored online communication. In late 2002, an early version of The Onion Router (TOR), which anonymizes the IP address of its downloader, was released by the USA Naval

Research Laboratory. Today, TOR is the most popular software used to access the dark web.

In 2009, the untraceable cryptocurrency, Bitcoin, was first introduced. The anonymity of the Bitcoin made it a very attractive tool for online criminal activity. The online currency would become an important component of dark net transactions.

In 2011, the first dark net market, Silk Road, was launched. An exposé²²⁹ published that same year compared the market to Amazon.com but for drugs, one that "makes buying and selling illegal drugs as easy as buying used electronics." Within days, the value of the Bitcoin surged. Around this period, publications started better differentiating between the dark and deep web. This same year also witnessed the emergence of rival cryptocurrencies, such as Namecoin and Litecoin.

In 2013, following long-term investigations, the FBI shut down Silk Road²³⁰ and arrested its alleged administrator, Ross William Ulbricht, also known as Dread Pirate Roberts²³¹. Between 2011 and 2013, it is reported that the site made more than USD 1.2 billion in sales. During this same year, Bitcoin prices crashed from around USD 1000 to almost USD 300.

Following the dismantling of the marketplace, several others emerged such as Silk Road 2.0, with some even surpassing Silk Road in size, including Evolution and Agora markets. By 2014, 10 per cent of retailers were operating across several marketplaces at the same time. In that same year, Operation ONYMOUS²³² seized several dark net markets, including the Silk Road 2.0. What followed was a period of instability among dark net markets, sometimes caused by external factors such as DDoS attacks and law enforcement; and some by internal factors such as fluctuations in the numbers of retailers, measures to improve

security and exist scams.^{233 234} The Bitcoin market also witnessed exit scams.²³⁵

The emergence of new marketplaces on the dark net was associated with a growing demand for cryptocurrency and its value reached USD 10 000 by 2017, with the market value growing from USD 11 billion to USD 300 billion. By 2018, countries around the world were developing cryptocurrency regulations in an attempt to control its growing market.^{236 237}

5.2. How to access the dark web?

Accessing the dark web requires the user to follow essential steps to ensure their security and protection online. These steps will be elaborated in the following section. The first two steps, which deal with the use of Virtual Private Network (VPN) and TOR, will later be examined in light of available information on the use of these tools on the African continent.

Before accessing the dark web, users likely refer to the detailed guidelines on how to access the dark web securely, which can be found on the surface web. Most of these guidelines are drafted in an easy-to-understand and user-friendly manner, most likely by experienced deep and dark web users.

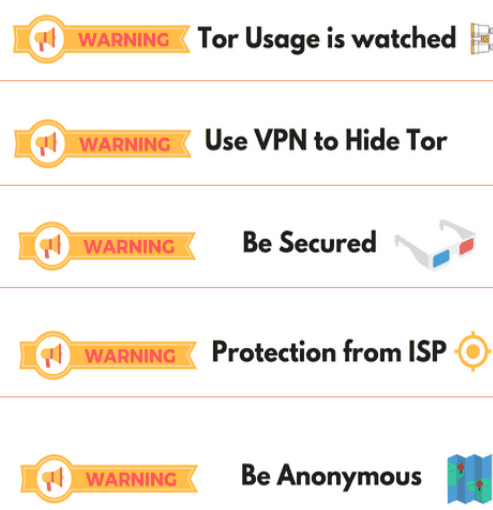


Figure 14. Warnings found on the surface web that explain to users how to access the dark web

Step 1: Connect to a VPN first

A VPN provides anonymity and privacy online “by creating a private network from a public Internet connection”. This tool masks the IP address of the user, making their activities online almost undetectable.²³⁸

After downloading the VPN onto the device, the user is given options of servers to which they wish to connect – servers in a country different from the one they are connecting from.²³⁹

Step 2: Install the TOR browser

TOR is an Internet browser that hides the IP address through multiple layers of encryption and allows the user to surf the web anonymously.

Once the VPN has been launched and running, the TOR should be downloaded and installed onto the device from the official website.²⁴⁰

The TOR browser is a necessary tool to access the dark net.²⁴¹ After accessing TOR, users are advised to use a VPN, as shown in figure 14, and enable the Java Script to increase security.

In this context, it should be mentioned that alternative anonymous networks exist, such as I2P and Freenet. However, the TOR browser, known for its safety and user-friendly approach, is the most popular anonymous network used. Due to the scope and purpose of this report, only data relevant to the TOR browser will be considered in the assessment.

Step 3: Browse .onion websites

Once the TOR is launched, the user is directed to the search engine, DuckDuckGo. This search engine does not collect personal information, hence, does not show users any ads while using it.²⁴² Nevertheless, this engine browses the surface web and not the dark web. When a user types in a search term, the results would be similar to those found on the regular Internet.

Dark web search engines that lead the user to .onion sites, include:

- Welcome to Dark Web Links (<http://bnjntqphs2lp4xdd.onion/>)
- Candle (<http://gjobqjj7wyczbqie.onion/>)
- not Evil (<http://hss3uro2hsxfogfq.onion/>)²⁴³

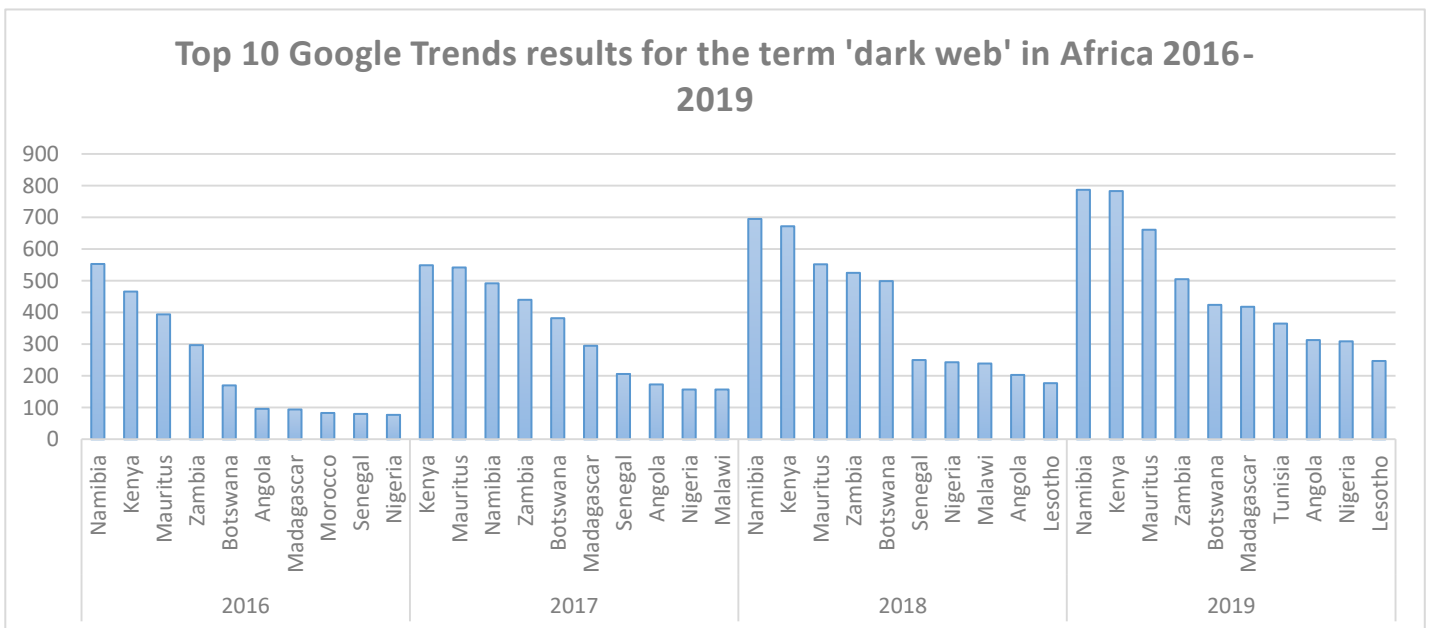


Figure 15. Top 10 Google Trends results for the term 'dark web' in Africa 2016-2019

5.3. Africa and the dark web

Multiple reports have predicted the shift in certain crime areas in Africa from the surface to the dark web, where undergrounds will probably be established and grow, as law enforcement intensifies its enforcement on the surface web.

With time, it is predicted that advanced technology will be required to take part in operations on dark net markets leading to a further complication of enforcement.

According to Google Trends, the topic 'dark web' has gained popularity between 2016 and 2019. The search has steadily increased over the past four years across the continent²⁴⁴ which could suggest an increased interest in this dark side of the Internet in some African countries. However, confirmed interaction or illegal engagement on the dark web related to the continent requires further investigation.

In a 2018 report, The Global Initiative against Transnational Organized Crime (GIATOC) suggests that wildlife trafficking, which is among the most spread transnational organized crime in Africa, is taking place on the surface web, such as on open listings, e-commerce websites, etc. and the deep web, including private messaging apps and closed groups. As suggested previously, some sources indicate that contact often starts on the surface web and then moves to the dark net, with the success of many transactions highly dependent on middlemen/women, trust and discretion. Multiple sources argue that the pressure that law enforcement is increasingly exerting on traffickers is forcing the latter to change tactics and pushing them to go deeper into the hidden part of the Internet, the dark net, where an organized and specialized

market will be established. GIATOC argues that this trade will become reserved for individuals with the required technological knowledge who are able to pay the high fees of the exclusive service, which will further complicate the process of monitoring it. With time, it is predicted that advanced technology will be required to take part in operations on dark net markets leading to a further complication of enforcement. Given the continued low perceived risk concerning illicit operations - despite regulations and demands to protect endangered species – GIATOC predicted that illicit trafficking in wildlife will move according to the suggested path.²⁴⁵

In 2017, Trend Micro examined the Middle East and North Africa underground, and in association with INTERPOL, studied the Western African underground. Trend Micro describes the Middle East and North Africa underground as a melting pot for cybercrime, culture and ideology, where culture and ideology make the market unique and highly influence the services and products offered. In their study based on data extracted between July and December 2016, Trend Micro finds that markets and clientele are present in North

CASE STUDY

In 2019, a wave of attacks on home routers in South Africa was believed to be aimed towards building a bigger botnet. Between 22 April and 10 May 2019, a 5 per cent increase in exploit attempts originating in Egypt and targeting consumers in South Africa has been registered. According to specialists, such attacks are in many instances the result of the consumers' lack of awareness of the need to manage appropriately the router to protect themselves against threats.

Source: 'New SOAP Attack Hits South African Home Routers', *Dark reading*, 31 May 2019.

African countries with a variety of products and services being sold on their websites. The analysis argues that despite not being as big as its counterparts, the Middle East and North African underground is active with a growing client base. As the underground develops, the expertise and resources needed to manage it will develop as well.²⁴⁶

According to the INTERPOL and the Trend Micro report, Western African cybercriminals are becoming more sophisticated and shifting to more complex business models and operations. They are gaining more social engineering expertise that is allowing them, complemented by increasingly available tools and services such as crypters, key loggers, etc. to steal money via elaborated crimes from individuals and companies around the world. INTERPOL and Trend Micro predicted that these skillful criminals will eventually establish their own online criminal communities to sell their products and promote crimes, leading to a Western African underground market. Accordingly, younger West African cybercriminals will continue to be bold. While cybercrime in Western Africa is not as sophisticated as in other parts of the world, crimes originating in the region, such as BEC, have had in previous years highly negative impact on companies and individuals around the world.²⁴⁷

In 2017, INTERPOL, in collaboration with IFAW, measured the scale and nature of the trade in rhinoceros, elephants and tigers on the dark net. The report shed light on the growing problem of online wildlife trade. Conducted between December 2016 and April 2017, the research found, among other findings, 21 advertisements related to offers of rhino horns products, ivory and tiger parts on the dark net. Despite the limited amounts of products found for sale on the dark net, the advertisements concerned some of the most critically

endangered species, which further highlights the urgency of the problem.²⁴⁸

A report from 2018 mentions that the dark web is contributing to the worsening of the human trafficking crisis in Ghana. According to the non-profit organization, Thorn, 63 per cent of surveyed individuals stated that they were sold online.²⁴⁹

5.4. Use of cryptocurrency

The surge of cryptocurrency in Africa is possibly linked to an increased use of cryptocurrencies for illegal purposes on the continent. Since the first cryptocurrency, Bitcoin, emerged in 2009, the value of the cryptocurrency has skyrocketed. A software developer with the pseudonym Satoshi Nakamoto introduced the electronic payment system, a decentralized currency that requires very low transaction fees. Since then, several other cryptocurrencies have emerged with many of them being sold at a cheaper rate, such as Litecoin and Ethereum.

Cryptocurrency allows the user to transfer money anonymously and securely. The anonymity aspect of this currency is further enhanced through the blockchain system, the online ledger of Bitcoin transactions, which records cryptocurrency transactions and secures the process.²⁵⁰

In recent years, interest in cryptocurrency and cryptocurrency-related operations has steadily grown across the continent with Bitcoin leading the online currencies in Africa, followed by Litecoin, XRP, Dash, Lixs and Monero.²⁵¹ In this context, Hootsuite's 2019 Global Digital Yearbook indicates that "10.7 per cent of South Africans possess crypto - the highest of any country surveyed. Nigeria also makes the list at 7.8 per cent, with Ghana at 7.3 per cent".²⁵² These numbers are above the worldwide average for adult Internet users

owning digital currency, which stands at 5.5 per cent.²⁵³

Whereas some African countries are embracing the online currency, others are adopting a more cautious approach regarding the new payment system. The use of cryptocurrency has many advantages, but also drawbacks.

Advantages

Some of the advantages that cryptocurrency offers is that it provides a high level of transparency through the blockchain, or the open ledger, which makes it possible for anyone at any time to view the data related to any transaction. Ease of access is another characteristic of cryptocurrency, since anyone can access it using a mobile phone. This means that even individuals with limited tech-knowledge are able to handle their finances easily, attracting as a result previously unlikely customers into the online world. Cryptocurrency is also unregulated and decentralized, which makes it unaffected by political changes. In 2018, the United Nations reported that many of the African countries facing inflation were experiencing a surge in Bitcoin use, including, Botswana, Ghana, Kenya, Nigeria, South Africa and Zimbabwe with the interest in the cryptocurrency in Uganda increasing as well.

The online nature of the currency allows its user to bypass some challenges faced as a result of certain restrictions. In April 2019, Google Trends statics indicated that Lagos in Nigeria scored the highest numbers of online searches for Bitcoin in the world. This is partly driven by the challenges faced by locals who cannot receive international money transfers due to Nigeria's reputation for fraud.²⁵⁴ In Kenya, start-ups and businesses are opting for cryptocurrency to protect themselves from theft as well as to "prove their creditworthiness for loans",²⁵⁵ despite

increasing bank regulations on cryptocurrency.²⁵⁶

The fear of the collapse of banks and monetary currencies regulated by governments have increased the interest of Africans in cryptocurrency. In 2013, the first Luno Exchange based in South Africa was established with now over 1.5 million customers worldwide. In 2018, approximately 15 cryptocurrency-related activities have started in Africa. Cryptocurrency-based remittances services have been introduced in many African countries.²⁵⁷ In Tunisia, governments are embracing the virtual currency with the e-Dinar, a digital currency issued by the government. Senegal is also in the process of creating a similar currency that could open opportunities for other Francophone countries on the continent.²⁵⁸

As a result, cryptocurrency is showing great promise in Africa with the growing belief that ledger technology will play a big role in solving developmental issues and launching economic growth. Politicians in Nigeria believe that cryptocurrency will lead to an industrial revolution. Nigerian companies also hope to improve the infrastructure through blockchain. Sierra Leoneans for example, are working on a block-chain ID system in an attempt to make it possible for financial institutions to do identity checks. Uganda is also working with blockchain startups to combat the supply of counterfeit medicine.²⁵⁹

Drawbacks

The complex idea of a decentralized payment system that stores data using a blockchain alarms some people and prohibits them from using it.²⁶⁰ Price volatility is another drawback of cryptocurrency. The value of cryptocurrencies changes drastically over short periods. For example, in January 2018, the value of the Bitcoin reached USD 17,000 before dropping to less than USD 7,000 in

February 2018. Another disadvantage of using cryptocurrency is the no-security policy. Emerging technologies could expose their users to the risk of fraud and stealing due to online inexperience.²⁶¹ A report published in January 2019 highlights the security problem that cryptocurrency suffers from, with the volume of stolen coins increasing significantly between 2016 and 2018. The biggest challenge faced when using cryptocurrencies, according to the report, is the risk of being hacked. SIM swapping and fraud are also reported risks when dealing with cryptocurrencies in addition to theft, as a result of exit scams.²⁶²

Cryptocurrency offers its customers absolute anonymity, which could be perceived by some as an advantage, whereas others perceive it as the biggest drawback of using the currency.

Finally, cryptocurrency offers its customers absolute anonymity, which could be perceived by some as an advantage, whereas others perceive it as the biggest drawback of using the currency. As previously mentioned, the details of the transactions are visible on the public ledger, however, the names and locations are hidden, making it a private online payment tool despite its transparency. Anonymity has inevitably attracted criminals who take advantage of this extra layer of security to complete financial transactions on the dark web.²⁶³

The informality, anonymity and volatility of the currency, in addition to other factors, have driven countries worldwide to push for regulations. In Africa, countries including Algeria, Libya, Morocco, Namibia and Zambia have banned cryptocurrency. Others do not have a clear stance concerning the

cryptocurrency, which put their citizens in a grey area. Countries such as South Africa have expressed a rather positive stance on cryptocurrency, with official bodies trying to collaborate with financial institutions and cryptocurrency companies to move forward with the online payment system.

According to an university study that examined a number of bitcoin transactions²⁶⁴, “44 per cent of bitcoin transactions and 25 per cent of all users were associated with illegal activity”, meaning almost half of the transactions studied were linked to illegal activity. Researchers have linked the currency to crimes including money laundering, distribution of illegal pornography and drug trafficking.²⁶⁵ These findings from 2017 indicate that approximately 24 million users used Bitcoin for mainly illegal purposes.²⁶⁶

The growth of cryptocurrency on the continent has also manifested through the spread of Bitcoin ATMs. Instead of dispensing cash, this ATM dispenses Bitcoin. Some even allow their customers to sell Bitcoin and withdraw cash, which render transactions quick and anonymous. In November 2019, there were around 6000 ATMs worldwide, with Africa hosting 14 Bitcoin ATMs, 7 in South Africa, 2 in Ghana and one in each of Botswana, Djibouti, Kenya, Uganda and Zimbabwe.²⁶⁷ Many of these ATMs have high fees associated with using them ranging between 8 and 14 per cent, which in many cases discourage people from using them.²⁶⁸

Not a lot of information is available on the extent or nature of the use of these ATMs yet. However, according to open sources, given factors such as buying, selling and anonymity which are involved in the process, money laundering is a risk to be considered. In a case from 2019, EUROPOL and Spanish law enforcement dismantled an OCG using ATMs to transform criminal cash into cryptocurrency

for other OCGs.²⁶⁹ This suggests that cryptocurrency ATMs could be associated with a risk of money laundering by operators and/or users.

Given the growing role that cryptocurrency and crypt-based services are playing on the African continent, the anonymity factor that cryptocurrency allows, and the high risk of use for illegal activity that the currency can foster, it is possible that Africans currently using cryptocurrency for financial purposes, will, once they understand the full benefits that this virtual currency could present to them, attempt to use it for illegal purposes. It is also likely that currently, a portion of Africans using cryptocurrency – who mostly have a good knowledge in technology – are already using it for illegal purposes (namely financial crimes, fraud, etc.) or are experimenting with it.

5.5. What can the user find on the dark web?

It is widely believed that the dark web is accessed exclusively for criminal purposes.²⁷⁰ The anonymity factor that the dark web provides, makes it a haven for individuals looking to buy and sell illicit goods and services. However, the dark web could be accessed for legitimate reasons as well. Mainly, the dark web has become associated with freedom online as it transformed into a safe space for activists, journalists and whistleblowers who experience Internet censorship and/or social and political media restrictions in their countries.

This growing role is exemplified through the creation of mirror sites by several news and media outlets on the dark web, such as ProPublica, Intercept, WikiLeaks, etc. In late 2019, BBC News launched a dark web TOR mirror of its website “in a bid to thwart censorship attempts”.²⁷¹ ²⁷² BBC News followed Facebook and the New York Times

which have also mirrored their sites, in 2014 and 2017 respectively,²⁷³ proving the growing worldwide impact of the dark web.

Law enforcement agencies also use the dark web to keep tabs on criminals and terror groups active online. In addition, Information Technology departments and analysts, among others, monitor the dark web searching for stolen data and accounts as well as signs of identity theft.²⁷⁴

The dark web has become associated with freedom online as it transformed into a safe space for activists, journalists and whistleblowers who experience Internet censorship and/or social and political media restrictions in their countries.

5.5.1. Hidden services

Hidden services are websites, similar to the ones found on the surface web. In the following section, the three main types of hidden services (.onion services on the TOR) will be elaborated:

- Marketplaces;
- Forums;
- Vendor shops.

Marketplaces

As previously mentioned, Silk Road was the first dark net market launched in 2011 and was compared to an eBay or Amazon for drugs²⁷⁵ which embraces the use of cryptocurrency. Marketplaces are platforms for sellers and buyers to exchange information and specifications on categorized products and services, such as drugs, weapons, hacking services, etc. Differently from a vendor shop, marketplaces allow multiple individuals to offer their products and services on their platforms, sometimes in exchange of a vendor fee. Some marketplaces are in one specific

language, such as English, Russian, French, etc. Most marketplaces require the user to register before accessing them.

Figure 16²⁷⁶ is a screenshot of the description of a vendor from Kenya indicating that they only accept orders on this market.

About Vendor

We are a team of professional hackers from Kenya. We have been working in the shadow market for 2 years now and send money transfers to any country.

We do not work via e-mail. We only accept orders in this market.

If you still do not know what a cash transfer is, do not waste our time and ask unnecessary questions.

If you want a quick money transfer, after you place an order, we send your money within 1 hour!

Figure 16. Dark web screenshot of a vendor indicating they are “a team of professional hackers from Kenya”

Forums

Forums are sites for online discussions where users engage in conversations by posting messages. Many of the forums include popular categories on which users ask questions and provide answers. Some forums are dedicated to specific topics such as pedophiles, cryptocurrencies, explosives and weapons, financial services, etc. others are hosted by marketplaces. Some forums are platforms for more technical discussions such as on

cryptography, website pen-testing, operating system, etc. There are also forums offered in specific languages, such as Polish, Turkish, Chinese, Spanish, Italian, French, Japanese, Korean, Portuguese, Dutch, etc. Forums include The Hub, DNM Avengers, 8chan, etc.

Most forums require the user to sign up and register before any interaction. But some of the forums allow users to access threads²⁷⁷ without signing up. Figure 17²⁷⁸ is an example of a discussion on a forum concerning buying credit, with Kenya mentioned in the thread.



Figure 17. Dark web screenshot of a discussion on a forum about buying credit with Kenya mentioned in the thread

Vendor sites

Unlike marketplaces, vendor sites are owned by a single vendor, in most cases selling a specific category of products or services, such as drugs, weapons, child sexual abuse material, hitman services, hacking services, etc. Vendor sites can be managed by one individual or a group of people. It should be noted that there is a higher chance that vendor sites are scams than marketplaces, considering that

marketplaces usually include users' reviews and feedback on the different sellers.

Vendor shops could be scams, in particular, when they offer services that are very unlikely to be managed by a single individual, such as hitmen services and red room organizations.²⁷⁹

Figure 18²⁸⁰ is a screenshot of a vendor site called AngelPharm.

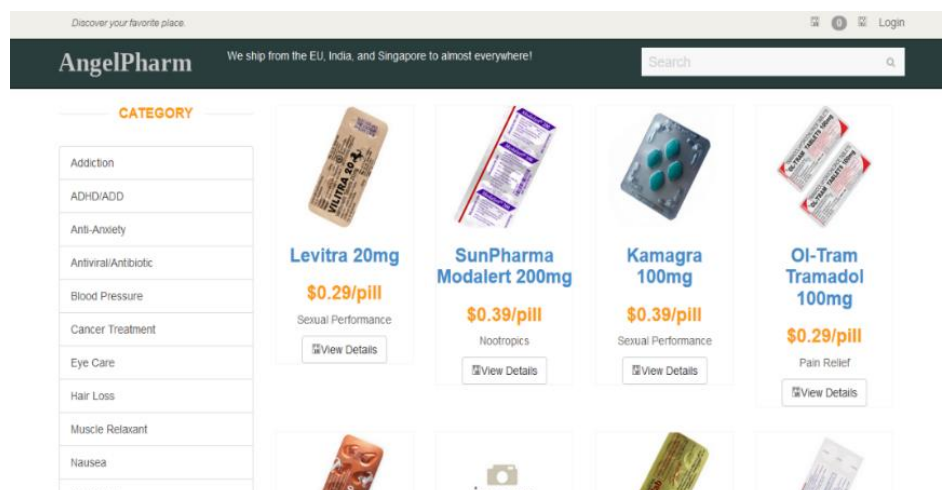


Figure 18. Dark web screenshot of a vendor site

5.5.2. Crime areas on the dark web - Africa

The diversity of crime-related products and services found on the dark web connected to the region 'Africa' and African countries suggests active dark web activity on the continent. The analysis of the MENA underground reveals that products and services available in their websites include malware, fake documents, crimeware, stolen data, weapons and drugs. Among the products found on North African forums are passport scans and identity documents, sometimes sold on Arabic forums, such as 'hack-int', known in Egypt. These documents were also found to be sold on social media websites such as Facebook, and on English language forums on the dark web, such as Valhalla.

Drugs were found to be mostly sold on English language marketplaces such as AlphaBay, Dream Market and Valhalla which supply customers outside the region as well. Weapons were also found to be sold on English language-based markets that have clients worldwide.²⁸¹

Unlike drugs, weapons cannot be easily shipped or delivered, which is why buyers tend to refer to clandestine black markets rather than use dark web sites, according to the Trend Micro study on the Middle Eastern and North African underground. Other services and products sold on the underground include hosting services, cash out services, hacking as a service, DDoS as a service, malware as a service, credit card dumps, stolen credentials and online accounts, malware and hacking tools, VPNs, etc.²⁸²

Available information suggests that the illegal trade of rhinoceros, tigers and elephants is occurring over the dark net, yet it is not a booming market, it remains limited²⁸³ compared to other commodities such as drugs, counterfeit documents, child abuse material and others.

High volumes of personal information of Nigerian and South African origins were found to be leaked on the dark web.

Furthermore, based on data gathered between 2016 and 2020 through a dark web crawler,²⁸⁴ high volumes of personal information of Nigerian and South African origins were found to be leaked on the dark web. Targets of these leaks included companies that offer financial services, asset management, chemicals, mobile telecommunication, insurances, bank holdings, e-commerce, online marketplaces, manufacturing, airlines, and etc. Targeted websites also included websites related to language tests, lighthouses, astrology, selling hunting, fishing, scuba and cycling equipment, hospitals, healing schools, e-mail and web security, data portals, universities, pension funds, insurances, bookstores, business solutions, etc.

CASE STUDY

In 2015, cybercriminals stole the personal data of millions of users of the adultery website Ashley Madison, including credit card details and nude photographs, of which 175,000 belonged to South Africans. The data dump, 9.7 gigabytes in size, was later leaked on the dark web using an onion address.

Source: 'Hackers Finally Post Stolen Ashley Madison Data', *Wired*, 18 August 2015.

In order to conduct searches for crime areas on the dark web using crawlers, specific keywords related to crime areas were identified. A deeper examination of dark web data gathered through the crawler between 2016 and early 2020 reveals that more than 90 per cent of searched dark web domains, related to Africa, mentioned the crime-specific keyword 'porn', followed by 'drug', 'credit', 'murder', 'hitman', 'trafficking', and 'smuggling'. Considering the framework of this report, the keyword 'porn' in the context of the dark web will not be examined. Some of the aforementioned keywords were found on domains that specialize in one specific crime area and others were found on domains that offer services and products related to multiple crime areas.

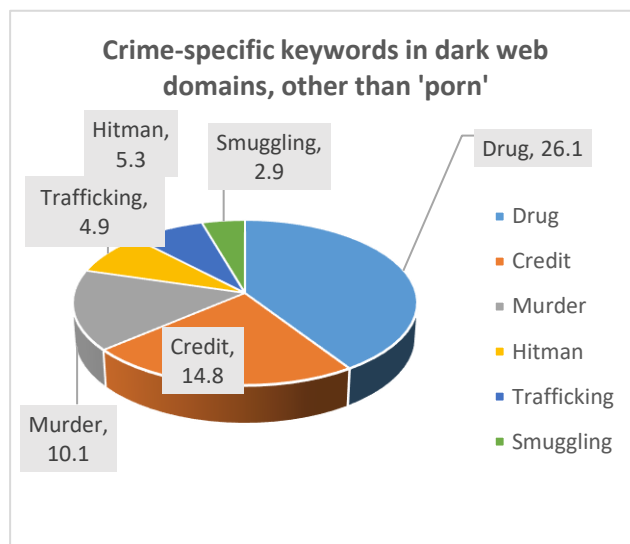


Figure 19. Crime-specific keywords in dark web domains, other than 'porn'

The mention of crime words on dark web domains and pages could be made for many purposes. The keyword could be mentioned in the offer of the product or service. The keyword could also be mentioned when an user is inquiring about options for purchasing a product or service. As previously mentioned, access to dark web domains does not necessarily imply illegal activity. However, given the nature of crime-specific keywords

used, the purpose in these cases is probably of criminal nature.

Domains with single-crime specific keywords

The seller or vendor offering services and products through this domain could be specializing in one crime area with a more limited list of clients. In some cases, this could mean a bigger geographical area over which users are spread as many users might prefer referring to a specialized vendor rather than one that offers various services and products.

Domains with multi-crime specific keywords

This could mean that the seller or vendor has a more diversified list of clients, as some users, most of whom interested in more than one type of criminal activity, prefer referring to one source that could provide them with multiple services and products. This could also suggest that the seller or vendor has connections with users from different groups specialized in different crime areas. Such vendors could be perceived as members of more online established OCGs which have connections across a multitude of crime areas that are needed to finalize trading. This could include inter-regional and transnational connections.

As shown in the figures²⁸⁵ below, evidence of human trafficking, hitman services, forged documents, counterfeit currency, child sexual abuse material and trading of financial information, among other crimes, in connection to the region 'Africa' have been found on the dark web.²⁸⁶

Documentation from Africa

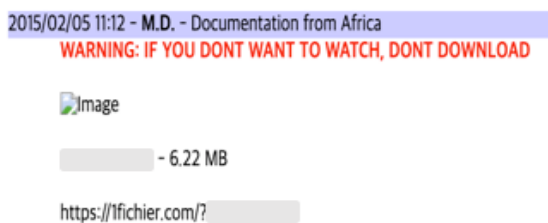


Figure 24. Dark web screenshot offering suspicious “Documentation from Africa”

Tempting Me Jay 15yo From Africa



Figure 20. Dark web screenshot offering child sexual material, titled “Tempting Me Jay 15yo From Africa”

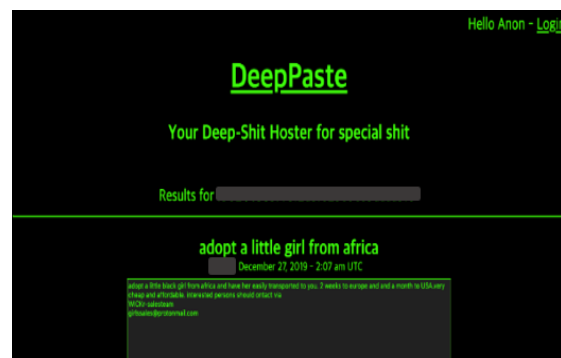


Figure 21. Dark web screenshot with the ad “adopt a little girl from Africa”



Figure 22. Dark web screenshot promoting hitman services with the ad “x-military African man need jobs”



Figure 23. Dark web screenshot offering financial information with the ad “South African bank account Needed”

- Positiiviset palautteet: 367
- Negatiiviset palautteet: -5
- Kauppojen kokonaisarvo: 10 000+ EUR
- Kirjautunut viimeksi: päivä sitten
- Ennakkomaksut: Sallittu
- Lähetysmaa: Etelä-Afrikka

We are fine retailers of medical grade African Sativa.
 We were previously on Silk Road from 08/2011.
 Our medicine is grown naturally in the highlands of Swaziland, [redacted] A genuine Sativa, African landrace strain.
 Grown organically by rural Swazi farmers. No fertilizers or pesticides, just sunshine and rain.
 These buds are not manicured, they are leafy, twiggy and with some seeds.
 This weed has a surprising high that is enjoyed by millions.
 If you are accustomed to home-grown hydroponic, manicured, super-strong, trophy buds, then our weed is probably not for you.
 We sell African bush-weed, it passes 8 different hands before we get it, and our vacuum-packer really flattens the buds. Otherwise our weed is great for price and it has an amazing Sativa high.
 We also sell 100% Sativa Kief, made at source by the farmers using the Moroccan method of screen sieving the dry weed.
 We use an industrial strength vacuum packer and thick plastic when packing our products, so you can be assured that your letter is safe.

Figure 25. Dark web screenshot with the description “We are free retailers of medical grade African Sativa”



Counterfeit US Dollar Banknotes \$2000

Vendor: Franklin Company
\$150.00

Available Options

Shipping method

Regular Delivery 8-14 days

Express Delivery 4-7 Days (+\$21.00)

Total price

Unmaged

Buysd product: Counterfeit US Dollar Banknotes \$3000

7 days and parcel in Kenya :) thank you, guys

on 02/07/2019

Add to Cart

Figure 26. Dark web screenshot offering counterfeit US dollar banknotes with a discussion mentioning the location Kenya

Locations mentioned

The mentioning of the region 'Africa' and African countries as origins and/or destinations in offers and requests for information on dark web domains suggests likely transnational criminal links. In the following section, the mentioning of African country names on dark web domains and pages will be examined. The mention of a location is an important part of the offers on dark web domains and pages. It could play a role in attracting traffic in different ways.

Country of origin and destination

Specifications concerning shipping origins and destinations are included on dark web domains and pages.

In figure 27,²⁸⁷ shipping origins and destinations are indicated as "Location: Worldwide" and "Location: Germany". An indication to the origin of the drug is specified in the second announcement, "Dutch made imported LSD". The announcement also indicates the possibility of shipping the product to Germany, USA, Western EU, Eastern EU, Asia, South America, Africa and the rest of the world, with a variation in shipping time.

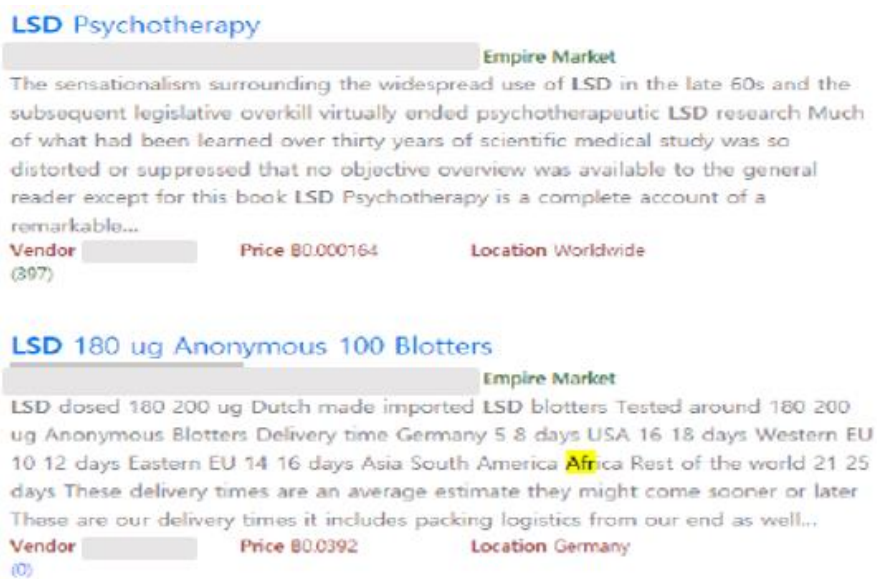


Figure 27. Dark web screenshot showing locations, origins of the product and possible shipping destinations

The distinction of some regions from ‘the rest of the world’ could indicate that the vendor has more established connections and previous experience in shipping to these particular locations. This could encourage individuals residing in these specific regions to choose this vendor.

Figure 28,²⁸⁸ shows more accuracy concerning shipping origins and destinations, such as “we ship orders 5 times a week from the USA worldwide, we don’t ship on weekends.” The vendor also offers tracking options.

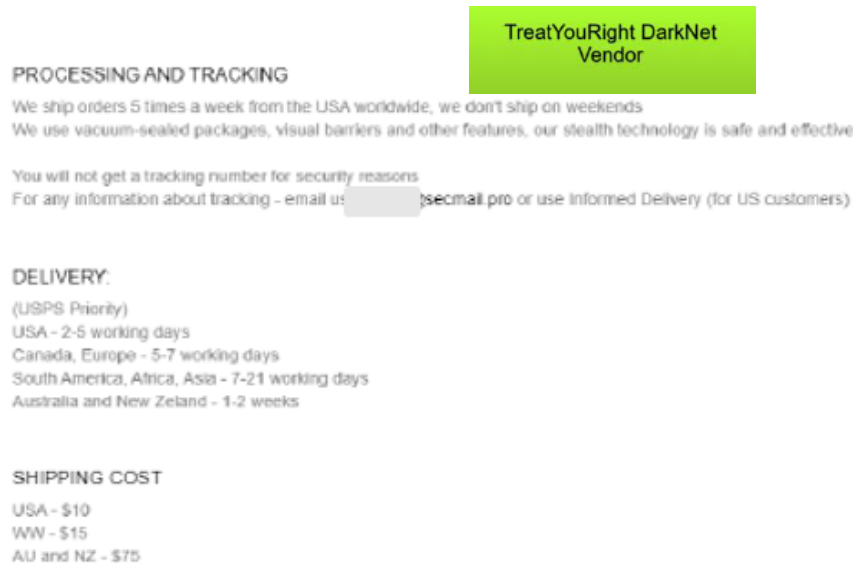


Figure 28. Dark web screenshot showing more accurate shipping origins, destinations as well as tracking options

Shipping time is specified, for Africa for example, delivery time is ‘7-21 working days’. Delivery to some regions includes shipping cost.

Figure 29²⁸⁹ is an offer of fake credit card and accounts. The seller includes Botswana among the “available countries.



Figure 29. Dark web screenshot of fake credit card and accounts with Botswana mentioned in “available countries”

Figure 30²⁹⁰ shows a request for information concerning the shipping of “Cloned credit cards with PIN code” to Uganda.



Figure 30. Dark web screenshot of a user asking for information concerning shipping to Uganda

The name of the country or region could also be mentioned to indicate the locations where a service could be delivered, such as in figure 31.²⁹¹



Figure 31. Dark web screenshot showing an offer of hitman services with destinations including Africa

The offer includes locations where hitman services could be offered, including Africa for the price of USD 15,000.

For weapons, for example, a 2015 INTERPOL report examining firearms sales over the dark net concludes that shipping is available for all continents and worldwide.²⁹²

Overall, some of the mentioned locations on Darknet markets appear to be general (i.e. continents) and refer to expected locations, possibly linked to the concerned product. However, in some cases, posts include more precise description related to possibilities or impossibilities of delivery to certain destinations. This could be the result of previous bad trading experiences in particular locations.

In this context, it is necessary to consider the limitations that examining location data presents. The 'shipping from' information may not always be accurate as in many cases, intermediaries could be handling the shipment before its arrival to the customer. However, in marketplaces, disappointed customers could leave negative feedback for the vendor which affect their business. In some instances, the sender could be travelling to another country and sending the package from that location in order to decrease the risk of seizure. Also, in some cases, vendors do not mention the specific country from which they are sending the product, they only mention a region such as 'Europe (EU)'. Others prefer not to mention specific geographical description, indicating 'Worldwide'. In addition, unless mentioned or hinted at, the customer's location cannot be easily determined.²⁹³ Such factors further complicate attempts of identifying the location of involved actors.

Origin of the product

Another reason why a country name could be mentioned is because the product itself originates or is manufactured in the mentioned region or country.

Figure 32²⁹⁴ below shows several offers of drugs. Among the offers, is "Morocco Hash" with the announcement indicating "Original high-quality Hashish from Morocco!"

There is a possibility that this drug is indeed originating from Morocco, and shipped from there or from a different country. However, there is also the possibility that this is a scam and the reference to Morocco is included to increase the value of the product and attract traffic.

Figure 33²⁹⁵ shows the site of a market that offers African products, originating from Africa such as gold bars, diamonds and rhino horns.

Figure 34²⁹⁶ is a screenshot of a dark net market offering the South African drug Durban to countries worldwide. The screenshot also shows that Durban is re-distributed to other countries.



Figure 32. Dark web screenshot showing an offer of "Moroccan Hash"

Africa Products: Featured

2g

\$ 0.7000

2 oz Gold Bar

We are offering 2 Troy Ounce bars of Gold. The purity is about 99% gold. Low pricing and quantities are limited time offers. We are able to sell you discounted gold courtesy of the cheap labor it took to procure it. We do not pay our workers. Discounts Available are automatically calculated as you [Scroll over about 2 oz Gold Bar](#)...

Add to cart

\$ 0.7000

1oz - Rhino Horn

Excellent Quality Rhino Horn sold by the Ozone

Add to cart

\$ 1.0000

1.125 Carat Diamond

We offering 1 RANDOM diamond that will fall within the 4 category parameters below: Carat: From "1" to "1.25" Clarity: From "VS2" to "FL" Color: From "White" to "E" or "F" Slope: Round Cut: Ideal or Signature Ideal It would be reasonable to assume these diamonds can be re-sold for between \$7,000 [Scroll over about 1.125 Carat Diamond](#)...

Add to cart

Secure world-wide business from Africa

Figure 33. Dark web screenshot showing offers of African products

The screenshot shows a dark web marketplace interface. At the top, there are three product listings:

- 28g DURBAN POISON - UK: Price 221.90€, 7.58€/g - 9.18€/g
- 25 gram Durban Poison A++ (Outdoor & Organic): Price 98.75€
- 3.5g Durban Poison The Classic Sativa Strain Dutch: Price 40.88€

Below these listings is a search bar for 'CANNAZON' and a 'Security warning: JavaScript is enabled. Please disable it in your browser.' A 'CATEGORIES' sidebar is visible on the left, listing various cannabis types like WEED, HASH, and CONCENTRATES. The main product grid below shows:

- 20g DURBAN POISON - TRACKED: Price 90.99€
- 10g WHITE WIDOW: Price 54.59€
- 10g GENUINE DURBAN POISON: Price 54.59€

A red box highlights the shipping origin 'ZA = South Africa' for the '20g DURBAN POISON - TRACKED' product. The shipping origin for all three products in the bottom row is 'ZA' (South Africa).

Figure 34. Dark web screenshot showing an offer of South African Durban

5.5.3. User profiles

Products and/or services customized for the mentioned country

The name of a country could be mentioned if the product being sold is customized specifically for the mentioned country, in particular forged documents. Figure 35 (see page 59)²⁹⁷ shows a dark net shopping site of forged documents and credit card information such as, 'customized credit card Photoshop', passport scans, IDs, driver's license, etc. Among the listings is an offer for a "Template Driver's License Angola".

In figure 36 (see page 59),²⁹⁸ Africa is mentioned as number 5 on the list of top best places for Child Sex Tourism with a description of the experience as well as categories offered.

An examination of data gathered between 2016 and early 2020 through the dark web crawler revealed that most African countries were found to be mentioned in dark web domains, in addition to the keyword 'Africa'. The majority of location-related keywords mentioned in domains were of the region 'Africa'. The majority of location-related keywords mentioned in domains were of the region 'Africa'. The remaining location-related keywords were mentioned either in single country domains, where only the name of one African country is mentioned in a domain, or in multi-country domains where more than one country name, including the names of African countries, are mentioned in the same domain.²⁹⁹

With 69 per cent of domains mentioning the keyword 'Africa', this could suggest that users from Africa and/or users supplying the continent are becoming more aware of the different aspects of the darkest side of the Internet. Dark web users have established transnational connections which allow them to ship products and deliver services to likely the five regions of the continent.

The examination of profiles found on dark web domains in available data demonstrates different linguistic and technological skills between users as well as different approaches to online selling. Most users make language mistakes and show poor linguistic skills in posts on dark web domains and pages, including markets, vendor shops and forums. However, many dark net traders demonstrate good levels of technological encryption knowledge, which allow them to engage in activity on the dark web.

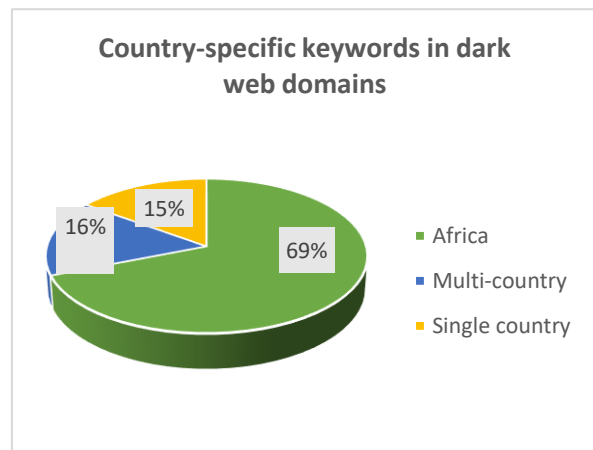


Figure 37. Country-specific keywords in dark web domains

Figure 38 (see page 59)³⁰⁰ is an example of a post on a forum showing poor linguistic skills.

While searching for Africa-related keywords using the dark web crawler, multiple clone sites were found, where the same offer appears on two different sites, only the domain and contact info are different. Users could adhere to this technique for many reasons. A seller could be associating with a competitor to attract their clients or attempting to grow the value of their site on the expense of a more popular site.

Also, sellers appear to be engaged in the trade of many illegal products and not one product exclusively with many of them advertising on many sites. The strategy could help the seller

to maximize chances of trade and attract the most traffic possible.

72	Template Driver's Licence Argentina	yesnan18	0.114	\$ 40.0
73	Template SSN CARD USA	yesnan18	0.114	\$ 48.0
74	Template SSN CARD USA	yesnan18	0.114	\$ 48.0
75	Template Driver's Licence Canada	yesnan18	0.114	\$ 48.0
76	British 4g Identity Ukran Scan	FaceBook	0.114	\$ 48.0
77	10 Passport Scan China	Passpor...	0.114	\$ 48.0
78	Template Driver's Licence Angola	yesnan18	0.114	\$ 40.0
79	ELECTRIC UTILITY BILL TEMPLATE R...	Pactain...	0.125	\$ 43.00
80	Custom forged: Bavstubs Utility	artific	0.1282	\$ 45.0
81	10 Passport Scan Qatar Various C...	Passpor...	0.1282	\$ 45.0
82	10 Passport Scan of the Russian ...	Passpor...	0.1282	\$ 45.0
83	10 Passport Scan Mexico	Passpor...	0.1282	\$ 45.0
84	10 Passport Scan Kingdom of Saud...	Passpor...	0.1282	\$ 45.0
85	10 Passport Scan of Pakistan	Passpor...	0.1282	\$ 45.0

Figure 35. Dark web screenshot showing offers of forged documents and credit card information

The world's 5 best places for Child Sex Tourism


Number 5: Africa

Poorest countries in Africa can be considered as good places to find children for sex. Unfortunately, there are a lot of diseases and it can be very dangerous to have sex with someone there. Moreover, some countries in Africa are not only very poor but also dangerous, and if you do not know anybody here, you could be attacked, hurt and even killed for your money... So be careful!

Category

- Software (no ...)
- Traditional Hardcore (...)
- Voyeurism/Exhib
- Zoo
- Piss/Sex/Vomit
- BDSM/Violence
- Rape
- Hardcore Torture/Ore
- Murder
- Bizarre

Figure 36. Dark web screenshot showing offers of Child Sex Tourism

301.  says:
[November 21, 2016 at 3:40 pm](#)

Pls I have sent you and email. Pls reply me.
 I need one card shipped expressly to Ghana.
 What is the daily withdrawal limit and do u also include the 0% balance on it?


 Mitni says:
[November 23, 2016 at 8:13 am](#)

Figure 38. Dark web screenshot of a forum post

Figure 39³⁰¹ shows the same ad posted by the same user (with domain) posting on different sites

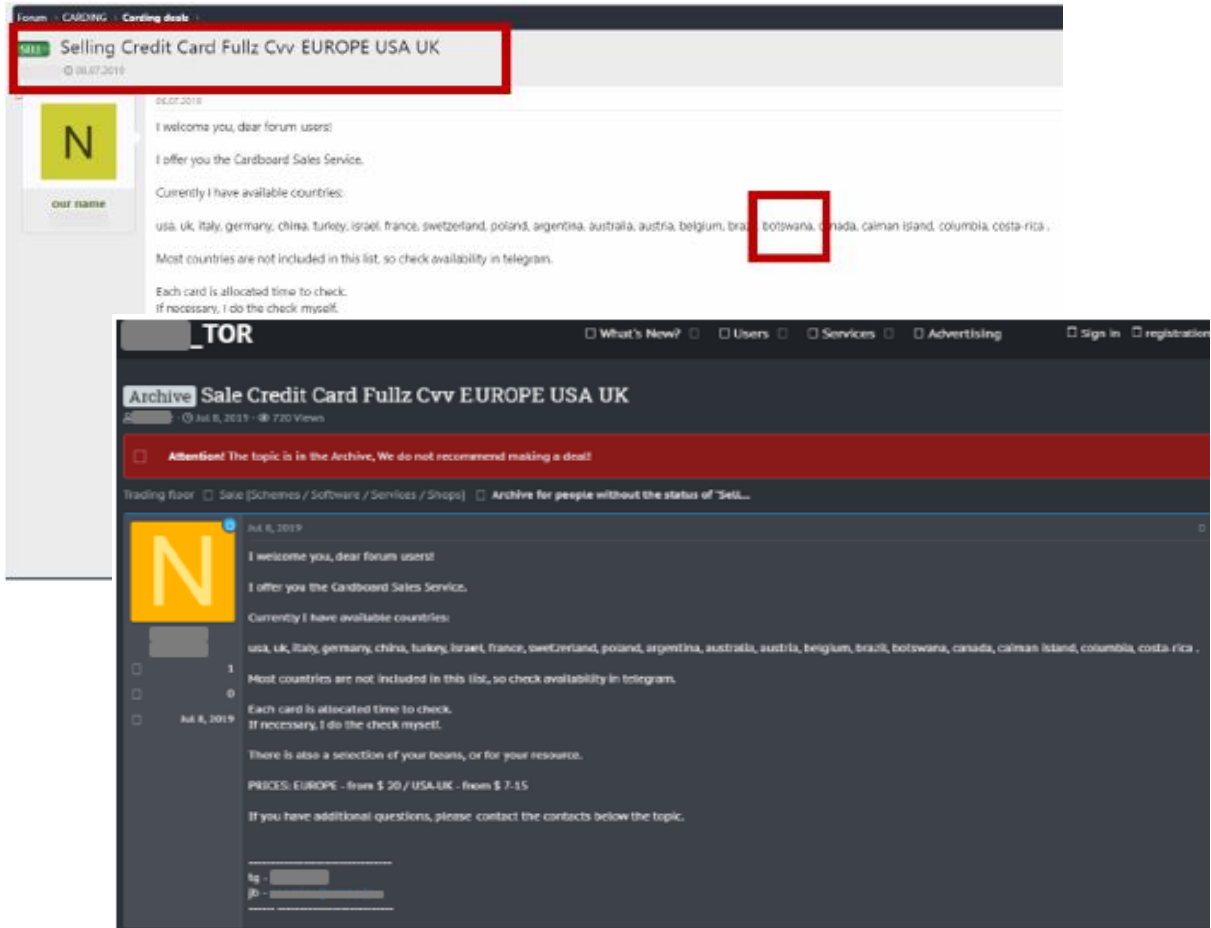


Figure 39. Dark web screenshots of the same advertisement on different sites

5.5.4. Payment methods

The large pool of offers and facilitation options that dark web users are offering clients suggests their likely growing flexibility and ease in handling trade on the dark net. As previously mentioned, interest in cryptocurrency and related operations have increased over the years in Africa. In addition, the number of Bitcoin ATMS grew, more types of cryptocurrency are now used on the continent and related regulations are being introduced in many African countries. As concluded in the cryptocurrency section, the online payment system can be associated with multiple risks, mainly due to the anonymity factor. The analysis suggests that many Africans using cryptocurrency could already be possibly using it for illegal purposes, or will possibly experiment with it once they understand its different characteristics.

Bitcoin is the main payment method for dark web transactions.³⁰² Other methods include Western Union and PayPal. Analysis suggests that as criminals move progressively to the dark web, cryptocurrency will be increasingly used for payment in transactions.³⁰³

Figure 40 (see page 62)³⁰⁴ is a screenshot of a dark net market that offers forged documents with the price in Bitcoin indicated on the right.

The website dark weblinks.com offers a description on what the user can find on dark web pages. Crime areas are divided into categories and description for each of the categories is provided based on user reviews, presentation of the domain, individual experience, etc. In many cases, the description is complemented by advice before or when using websites. Based on data extracted between October and December 2019, the following information were gathered concerning payment methods on different dark web links.³⁰⁵

- The types of payment allowed is Bitcoin;
- Services offered include Western Union Transfers, MoneyGram transfers, Anonymous Bank Accounts, etc;
- Refund and return possibilities;
- Security features include authentication via PGP, Escrow and Multisig for safer transaction and trades, PIN for withdrawal and refund address changes;
- Warning of exit scams;
- Possibility of using hardened Bitcoin escrow on some markets instead of depositing Bitcoins;
- Discussion of payment through e-mail exchange;
- On some markets, prices change on a daily basis;
- Escrow accepted;
- Use of the bidding system;
- For some services, payment is released after completion.

The detailed description and advice offered by some vendors and markets suggest that dark web vendors and sellers are becoming increasingly flexible. They are smart and knowledgeable Internet users that have studied the advantages and disadvantages of operating online anonymously, but also their clients. Accordingly, they are providing convenient services and options to attract bigger traffic. They are also proving to be not only technologically knowledgeable, but also strong advertisers, sales and business players.

Original Degrees, Diplomas, Certificates full registered in records with full transcripts	
Diploma (almost any School)	0.1565 B
Bachelor Degree (almost any University)	0.2151 B
Master (almost any University)	0.3325 B
Certificate (any type)	0.1369 B
Medical prescriptions (N.20 of any drug)	0.1369 B
Hacking Services change status in official records	

Figure 40. Dark web screenshot showing an offer of forged documents with prices in Bitcoin

5.5.5. Use of language

The use of language could be perceived as an important element of the dark web search that could possibly offer some indications on users' profiles and origins.

As previously mentioned, overall, sources show that many of the users have poor linguistic skills. This could suggest that the user is writing in a language that is not their native language. It could also be a tactic to confuse clients on their origins and remain anonymous.

Results generated from running a dark web crawler suggest that in addition to English, French and Portuguese, local African languages and dialects are found to be used on dark web domains and pages.³⁰⁶

The use of expressions in local African languages also appeared in an initial scan of dark web pages.

In Figure 41,³⁰⁷ the use of the term “no wahala”, which in Nigerian local slang means “no problem” is assumed to be written by a Nigerian user.

Anyway, I have no beef with any kind of substance use or abuse as long as the person in question is able to maintain and comport his/herself. You want to shoot up? Just don't cause no wahala with me or my friends and family. You want to blaze or booze? By all means, as long as you are able to maintain your integrity and decency. Sadly, this is where most addicts fail.

As for death, were all gonna die. And none of us asked to be born in the first place. And life is mostly full of shit. So enjoy yourselves while it lasts. If possible...

Figure 41. Dark web screenshot showing the use of local African dialect

Many of the posts found in markets and forums offer options of supporting languages, such as Chinese, Dutch, French, Italian, Japanese, Korean, Polish, Portuguese, Russian, Spanish, Turkish, etc. Figure 42,³⁰⁸ is an example of a suspicious domain in Russian.

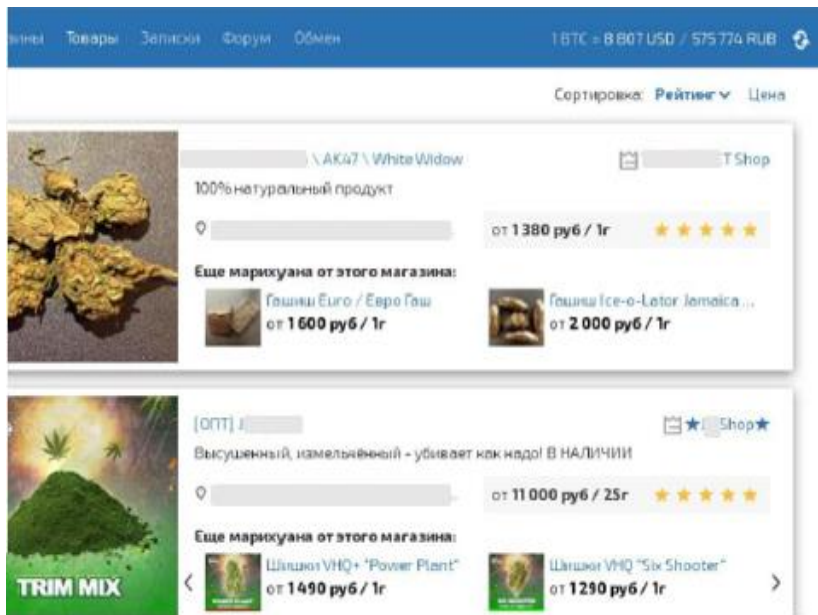


Figure 42. Dark web screenshot showing a suspicious domain in Russian

In some cases, the language of the keyword searched could highly affect the results found, in particular in relation to countries with two or more official languages. This is applicable for country-name keywords but also for crime-specific keywords. In cases where results in multiple languages were found, the majority of the domains found were in English, followed by French.³⁰⁹ In addition to English, French was found to be used on dark web domains for the country names of Algeria (Algérie), Guinea (Guinée), Morocco (Maroc), Senegal (Sénégal), and Tunisia (Tunisie). Results in French, in addition to English, were also found to be used

for the keywords counterfeit (contrefait) and rhinoceros (rhinocéros).

5.6. VPN and TOR usage in Africa

As previously mentioned, the two initial steps required to access the dark web will be examined in the following section in light of available information on their use in Africa.

5.6.1. Usage of VPN in Africa

Increased interest in and usage of VPN in Africa is possibly linked to an increased access to illegal/suspicious dark web sites.

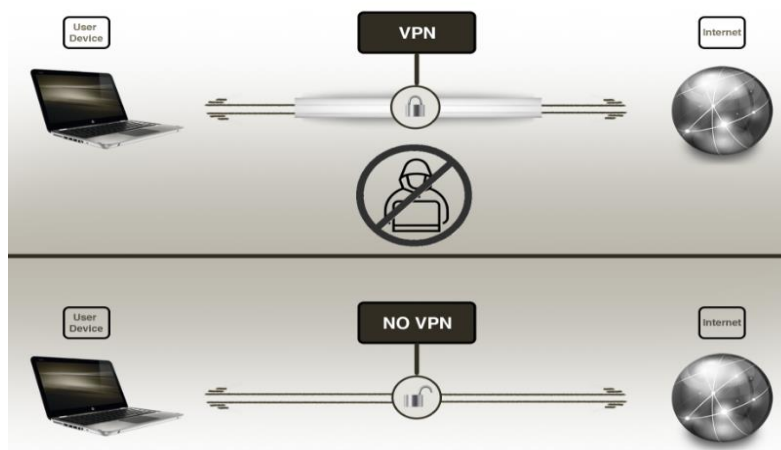


Figure 43. How VPN works

VPN usage statistics suggest that since 2013, around 25 per cent of Internet users worldwide have used a VPN to access the web each month. In 2017, the percentage of VPN users increased by 185 per cent compared to

In 2018, it was estimated that 47 per cent of VPN usage in the Middle East and Africa was aimed at accessing better entertainment content, whereas 34 per cent of the usage aimed at remaining anonymous while browsing online.

the previous year, and in 2018, this number increased by 165 per cent from 2017. In addition, the VPN global market grew steadily between 2016 and 2018, with the value increasing from USD 15.46 billion in 2016 to USD 20.60 billion in 2018. It is estimated that by the year 2022, the value of the VPN global market will reach approximately USD 35.73 billion.

In terms of the percentage of VPN users in the region, Africa represents 20 per cent of VPN users worldwide, compared to 23 per cent in Latin America and 30 per cent in Asia and the Pacific. Africa shows percentages higher than in Europe and North America, where the percentage stands at 18 per cent.³¹⁰ In 2018, it was estimated that 47 per cent of VPN usage in the Middle East and Africa was aimed at accessing better entertainment content, whereas 34 per cent of the usage aimed at remaining anonymous while browsing online.³¹¹ Though no African country appears among the top 10 countries worldwide, South Africa appears among the 24 countries globally with the highest VPN usage with a percentage of 28 per cent. The figures indicate that the main reasons for using a VPN in South Africa is to access torrent websites, such as the Pirate Bay, as well as to browse anonymously.³¹²

According to Google Trends, the term 'Virtual Private Network' is a popular keyword in many African countries. The service indicates that users from Côte d'Ivoire, Ghana, Kenya, Nigeria, Madagascar, Morocco and Rwanda have searched the most for the keyword between 2016 and 2019. The search has mostly increased across countries in the mentioned timeframe and the highest search recorded was in Côte d'Ivoire in 2019, with 4,046 searches throughout the year.³¹³

These figures suggest an increased interest in VPN in Africa over the past four years. Statistics also reveal that the interest of Africans is divided mostly by the desire to access better entertainment but also to browse the web anonymously. At this point, it is not possible to quantify or examine the reasons why some Africans wish to remain anonymous online through a VPN. As previously mentioned, detailed guidelines on how to access the dark web safely are widely spread on the surface web. Among the first instructions that guidelines indicate is to download and turn on a VPN before accessing TOR. In this context, this interest in VPN could suggest a possible usage to access the dark net.

5.6.2. Usage of TOR in Africa

As previously mentioned, the examination of estimated TOR usage in Africa in light of multiple factors indicates its usage for a possible access to the dark web. As already stated, TOR was created by the Office of Naval Research in the USA and the Defense Advanced Research Project Agency in the mid-1990's to protect online intelligence communication through an anonymous network. The software allows web pages to remain anonymous "by configuring a server to connect with clients as a tor relay in between".³¹⁴ In this case, there is no need for an IP address, a 16 character code known as an 'onion address' is used by clients in place of a

URL. Through this process, TOR allows clients to access dark nets.³¹⁵

In the following section, TOR statistics³¹⁶ will be examined in light of multiple factors. TOR has many advocates that claim protection online as their endgame. Many activists and journalists use it, in particular in countries suffering from oppression and restrictions on freedom of speech. It is also a platform for whistleblowers to share information. In addition, users who wish to keep their searches online private use the software.

Despite the possible positive usage of the software, TOR is known for the negative usage it fosters online, which has transformed it into a safe haven for criminals over the years. The software is widely known as gateway into the dark corners of the Internet, where online users could use it to access the dark web and conduct illegal activity.

Limitations

According to the TOR project website, statistics generated on users' usage are limited. These numbers do not count actual users but requests to directories or bridges that are made by users. Based on these requests, estimates are made and an average number of users is generated. Hence, it is impossible at this stage to quantify this usage or to assess whether it is used for legal purposes, such as surfing the web free from restrictions, or for malicious reasons, namely accessing the dark web and engaging in illegal activity.

TOR usage in Africa

According to the TOR project statistics, several African countries showed high levels of usage between 2016 and 2019.

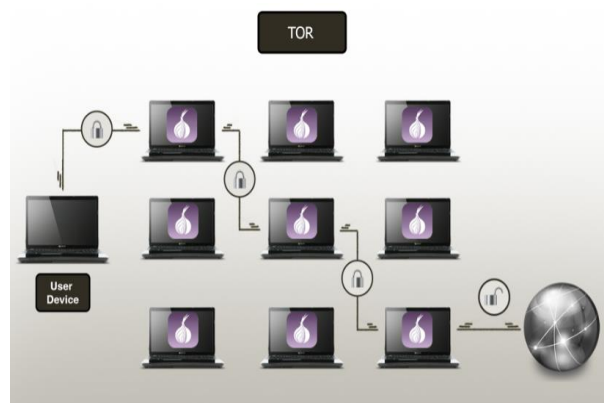


Figure 44. How TOR works

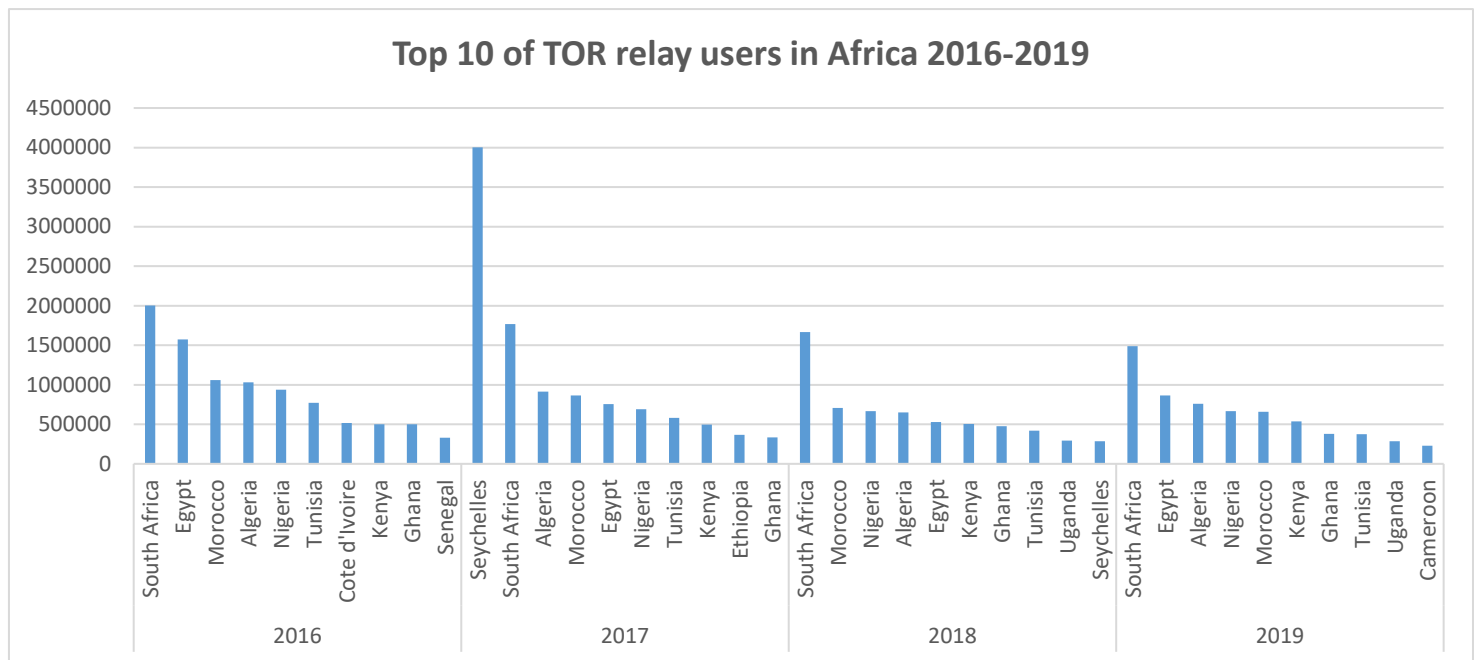


Figure 45. Top 10 of TOR relay users in Africa 2016-2019

In 2016, the estimated number of TOR relay users in Africa connecting directly to the software was the highest in South Africa with more than 2 million users. North Africa also recorded high levels of usage, with Egypt recording the highest number in the region. Western African countries also made the top 10 list of countries with Nigeria recording the highest number of TOR users in the region. Between 2016 and 2019, the top 10 countries that recorded high usage of the software in Africa, remained mostly the same over the four years with minimal changes in percentages. Overall, the TOR project estimates that over the last 4 years, over 44 million Africans connected to the software. The volume of users peaked in 2017 with more than 13 million users accessing the network, and then decreased to approximately 9 million users in 2019.

The above graph concerns users who connected using relays. The IP address of these relays is public and is listed in the public TOR directory. This usage can be blocked by Internet providers and governments. In order to circumvent this, users can use TOR bridges, which are nodes that are not public and not as

easy to be blocked. According to the TOR project, TOR bridges are useful for users “under oppressive regimes or for people who want an extra layer of security because they're worried somebody will recognize that they are contacting a public TOR relay IP address.”

According to the TOR project, there are three main reasons why a customer would use a bridge to access TOR:

1-Because the TOR software is blocked and the user wants to find a way to access it, then the user is assessed as ‘an annoying user but not very dangerous’.

2-The software is not necessarily blocked, but the user ‘is trying to hide the fact they’re hiding Tor’, in this case the user is assessed as possibly very dangerous.

3-Miscellaneous non-dangerous reasons such as not knowing or testing the effectivity of the bridge.

As such, there is a 1/3 chance that bridge users use the access granted to TOR for malicious reasons. When comparing the relay users and bridge users in Africa, overall, the same countries figure in the top 10 countries in

terms of highest usage, with Algeria, Egypt, Morocco, Nigeria and South Africa occupying the top 5 mostly in both categories between 2016 and 2019.

As previously mentioned, bridge users are mostly users trying to overpass obstacles forbidding them to access a software or a specific website. Most African countries do not present exceptional numbers in terms of bridge users between 2016 and 2019.

At this stage, given that TOR is currently the most popular software to access the dark web and based on the available data on its usage in Africa, the usage of TOR in African countries indicates a possible access to the dark web. However, this hypothesis cannot be tested or proven at this time.

In its Organized Crime Index, GIATOC, in the framework of Project ENACT examined the level of criminality in African countries, based on multiple factors. The comprehensive assessment analyzes criminal markets and criminal actors in member countries and generates a percentage of criminality for each African country.³¹⁷

Based on this assessment and the estimative TOR usage in Africa, few hypotheses could be drawn. The examination of the top ten countries for TOR relay and bridge users between 2016 and 2019 and the top 10 countries for highest and lowest levels of criminality - criminal markets and criminal actors³¹⁸ in Africa, sheds light mainly on four countries, South Africa, Nigeria, Kenya and Tunisia.

According to the Organized Crime Index, Kenya, Nigeria and South Africa present high levels of crime as well as high levels of resilience against organized crime.³¹⁹ All three countries are “the socio-economic powerhouses of their respective continental regions” and present large criminality profiles

and the four types of criminal actors, including criminal networks. They are also perceived as hubs in the wider region and the continent.

Given the high score of criminality that Kenya, Nigeria and South Africa present according to the Organized Crime Index, and the estimative high usage of TOR related to these countries as shown in figure 45, it is likely that crime elements from these regions are engaged in dark web activities.

The comparison also highlights the case of Tunisia. According to the Organized Crime Index, Tunisia is classified as having low criminality and high resilience against organized crime.³²⁰ According to TOR usage estimates, a high number of requests originate from Tunisia. Given the low score of criminality that Tunisia presents, and the estimated high TOR usage, it is possible that access to TOR is intended for preserving privacy and anonymity online and not for malicious purposes.

6. DRIVING FACTORS

Various factors are driving cyber and cyber-enabled crime on the continent and fostering the growth of its impact on national, regional and continental levels. These factors include:

- Easy financial gain;
- Ignorance and mal-usage of ITC, neglect of updates’ requirements for technical material, use of software without licenses and use of outdated technology;
- Poverty, unemployment and a high number of jobless IT students;
- Under-reporting of the crime by victims;
- Ease of access to the Internet;
- Lack of technical and infrastructural frameworks to combat cybercrimes;
- Political instability and social problems;
- Absence of specialized investigators;

- Lack of general awareness of society;
- Lack of national policies and specific legislations to combat cyber and cyber-enabled crime;
- Lack of knowledge on the risks and dangers of newly acquired technologies;
- Access to equipment that facilitates online piracy;
- Increased use of electronic devices for multiple functions;
- Increased usage of social media.

Conclusion

The objective of this threat assessment was to explore the major aspects of OCGs active online in Africa on the surface, deep and dark web. The report highlighted the growing impact of the Internet and the threat of cyber-enabled crimes on security and development in Africa.

The analysis outlined some of the main emerging and current cyber trends and modus operandi employed by African cybercriminals on national, regional and international levels. Some of the main techniques used by OCGs in Africa online were also defined in light of available information and data provided by member countries. Cyber OCGs active online in Africa will continue to exploit the Internet to further their illegal activities as long as the socio-economic and security landscapes in Africa provide the opportunity. They are flexible and capable of adapting and evading law enforcement tactics. They have also proven that they are able to quickly change

modus operandi in light of circumstantial changes. This was witnessed during the recent COVID-19 pandemic which has given way for cybercriminals to exploit the crisis to their benefit across the world.

Regarding the surface and deep web, the report distinguished between cyber and cyber-enabled crimes and allocated a detailed section to online financial cyber-enabled crimes as they are the most prevalent online crimes in Africa. Based on available information, the report examined illegal activity online in Africa in relation to human trafficking and people smuggling, crimes against children, trafficking in works of art, environmental crimes, illicit trade in diamonds, trafficking in SALW, drug trafficking, trafficking in counterfeit goods and trafficking in SMV. The report also examined the dark web and attempted to identify connections to the African continent in light of open source statistics, dark web sources and data from the private sector.

This threat assessment also considered some of the driving factors enabling this type of crime.

In summary, this threat assessment suggests that cybercriminals active in Africa have the intent and capabilities to continue exploiting the web for criminal gain. Attempts to measure the scale and impact of cybercrime in Africa through intelligence analysis, such as this threat assessment, is intended to inform and empower law enforcement authorities and decision makers when developing strategies to counter cyber-enabled crime³²¹ as well as to identify and dismantle OCGs.

References

- ¹ Countries that have ratified the convention are: Chad, Ghana, Guinea, Mauritius, Namibia, Rwanda and Senegal.
- ² N. Kshetri, 'Cybercrime and Cybersecurity in Africa', *Journal of Global Information Technology Management*, Vol. 22, Issue 2, 2019, p. 77-81, <https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527> (accessed 24 February 2020).
- ³ Central African Police Chiefs Coordination Organization.
- ⁴ East African Police Chiefs Coordination Organization.
- ⁵ Southern African Regional Police Chiefs Coordination Organization.
- ⁶ Western African Police Chiefs Coordination Organization.
- ⁷ Cybersecurity Spotlight - The Surface Web, Dark Web, and Deep Web', *Center for Internet Security*, May 2019, <https://www.cisecurity.org/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web/> (accessed 27 January 2020).
- ⁸ 'Illegal Wildlife Trade in the Dark net', *INTERPOL*, 2017, <https://www.interpol.int/en/News-and-Events/News/2017/Research-identifies-illegal-wildlife-trade-on-the-Darknet> (accessed 26 June 2020).
- ⁹ 'The Dark Web: Myths, Mysteries and Misperceptions', *Kaspersky Lab*, 2017, <https://go.kaspersky.com/rs/802-IJN-240/images/Dark%20Web%2010172017.pdf?aiid=521973948> (accessed 21 July 2020).
- ¹⁰ M. Roser, H. Ritchie and E. Ortiz-Ospina, 'Internet', *Our World in Data*, 2020, <https://ourworldindata.org/Internet#note-1> (accessed 06 February 2020).
- ¹¹ 'Measuring Digital Development: Facts and Figures 2019', *International Telecommunications Union*, 2019, p.2 <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf> (accessed 06 February 2020).
- ¹² Information in this figure are gathered from the following sources: '2018 Digital Yearbook', *Hootsuite & We Are Social*, 2018; 'Digital 2019: Global Digital Yearbook', *Hootsuite & We Are Social*, 2019; 'Digital 2020: Global Digital Overview', *Hootsuite & We Are Social*, 2020 (accessed 07 February 2020).
- ¹³ Definitions retrieved from INTERPOL public website and documents www.interpol.int.
- ¹⁴ G. P. Paoli, J. Aldridge, N. Ryan, R. Warnes, 'Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web', *Rand Corporation*, 2017, p. 66, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf (accessed 24 February 2020).
- ¹⁵ At the time of writing the concerned report, South Africa had a cybercrime law in place and Kenya was in the stage of developing the law.
- ¹⁶ R. Medugno, 'Africa: A New Safe Harbor for Cybercriminals?', *Trend Micro*, 2013, <https://blog.trendmicro.com/africa-a-new-safe-harbor-for-cybercriminals/> (accessed 24 February 2020).
- ¹⁷ N. Kshetri, 'Cybercrime and Cybersecurity in Africa', *Journal of Global Information Technology Management*, Vol. 22, Issue 2, 2019, p. 77-81, <https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527> (accessed 24 February 2020).
- ¹⁸ Telegram and WhatsApp services include an end-to-end encryption feature with which only the communicating users can read the messages.
- ¹⁹ U. Kadri, 'Inside the world of 'Apprentice Yahoo Boys'', *The Moment*, <https://themomentng.com/index.php/2019/02/24/inside-the-world-of-apprentice-yahoo-boys/> (accessed 09 June 2020).
- ²⁰ 'EFCC Busts 'Yahoo Academy' in Akwa Ibom', *EFCC*, 01 December 2019, <https://efccnigeria.org/efcc/news/5226-efcc-busts-yahoo-academy-in-akwa-ibom> (accessed 09 June 2020).
- ²¹ 'Cybercriminalité et utilisation d'Internet par des groupes criminels africains', *Service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée (SIRASCO), Direction centrale de la police judiciaire (DCPJ)*, 19 June 2020.
- ²² Thomson Reuters World Check database, organized crime coded information for Africa queried (accessed 23 April 2020). The World Check database is an aggregate of nominal data derived from open sources. This database is not limited to media coverage specifically; rather, it combines media results with official sanction lists and other governmental data from law enforcement and regulatory agencies (information made available via press releases or through official filings) and also official and business resources, such as corporate databases and delisting records. Open INTERPOL information can also be found in this data.
- ²³ Thomson Reuters World Check database, organized crime coded information for Africa queried (accessed 23 April 2020).
- ²⁴ 'Cybercriminalité et utilisation d'Internet par des groupes criminels africains', *Service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée (SIRASCO), Direction centrale de la police judiciaire (DCPJ)*, 19 June 2020.
- ²⁵ A. Al Azm, K. A. Paul, 'Facebook's Black Market in Antiquities: Trafficking, Terrorism and War Crimes', *Alliance to Counter Crime Online*, June 2019, <https://static1.squarespace.com/static/5e3a7fb845f8c668df48d437/t/5e4e58ef0caa64606351a54b/1582192944742/ATHAR-FB-Report-June-2019.pdf> (accessed 02 May 2020).
- ²⁶ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Central African Region', public version, *INTERPOL*, 2018.
- ²⁷ As defined by INTERPOL, "refers to the scams used by criminals to exploit a person's trust in order to obtain money directly or obtain confidential information to enable a subsequent crime. Social media is the preferred channel but it is not unusual for contact to be made by telephone or in person".
- ²⁸ Definition retrieved from INTERPOL public website and documents www.interpol.int.
- ²⁹ '2019 Internet Crime Report', *FBI Internet Crime Complaint Center*, 10 February 2020, https://pdf.ic3.gov/2019_IC3Report.pdf (accessed 01 April 2020).
- ³⁰ 'Africa Cyber Security Report 2016. Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness', *Serianu Cyber Threat Intelligence Team*, 15 December 2016, <https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf> (accessed 15 September 2019).
- ³¹ 'La cybercriminalité en RDC en chiffres', *Tresor Kalonji Blog*, 24 September 2018, <http://tresorkalonji.pro/2018/09/la-cybercriminalite-en-rdc-en-chiffres.html> (accessed 12 June 2020).
- ³² 'Arnaque aux faux ordres de paiement : La DGSN appelle à la vigilance', *2M.ma*, 22 October 2019, <https://2m.ma/fr/news/arnaque-aux-faux-ordres-de-paiement-la-dgsn-appelle-a-la-vigilance-20191022/> (accessed 12 June 2020).
- ³³ M. Daghar, 'Is Kenya the new playground for cyber criminals?', *ENACT*, 04 February 2020, https://enactafrica.org/research/trend-reports/is-kenya-the-new-playground-for-cyber-criminals?utm_source=BenchmarkEmail&utm_campaign=ENACT_Review&utm_medium=email (accessed on 11 June 2020).

- ³⁴ E. Mugisha, 'What you should know about cybersecurity', *The New Times*, 11 October 2019, <https://www.newtimes.co.rw/news/what-you-should-know-about-cybersecurity> (accessed 11 June 2020).
- ³⁵ M. Nkurunziza, 'Cyber crime cost Rwanda economy Rwf6bn in 2018', *The New Times*, 30 May 2019, <https://www.newtimes.co.rw/news/cyber-crime-cost-rwanda-economy-rwf6bn-2018> (accessed 11 June 2020).
- ³⁶ 'SABRIC Annual crime Stats 2018', *SABRIC*, 28 June 2019, <https://www.sabric.co.za/media/1227/sabric-annual-crime-stats-2018.pdf> (accessed 11 June 2020).
- ³⁷ 'Beware: business email compromise fraud', *SABRIC*, 25 September 2019, <https://www.sabric.co.za/media-and-news/press-releases/beware-business-email-compromise-fraud/> (accessed 10 June 2020).
- ³⁸ Thomson Reuters World Check database, organized crime coded information for Africa queried (accessed 23 April 2020).
- ³⁹ 'Ghana Extradites Accra-Based Nigerian to U.S. for Wire Fraud', *AllAfrica*, 12 December 2019, <https://allafrica.com/stories/201912120698.html> (accessed 14 June 2020).
- ⁴⁰ 'Cybercriminalité : L'opérateur Orange grugé de près d'un milliard par 50 Nigériens', *Seneweb*, 04 November 2019, <https://www.seneweb.com/news/Societe/cybercriminalite-l-operateur-orange-gruge-n-299344.html> (accessed 15 June 2020).
- ⁴¹ 'Arnaque aux sentiments sur Internet : les "brouteurs" migrent pour mieux sévir chez nous', *DH*, 17 December 2019, <https://www.dhnet.be/actu/faits/arnaque-aux-sentiments-sur-internet-les-brouteurs-migrent-pour-mieux-sevir-chez-nous-5df7d2aff20d5a0c460ab0c2> (16 June 2020).
- ⁴² Y. Ciyow, 'En Côte d'Ivoire, les cyber-arnaqueurs se réinventent au gré des nouvelles technologies', *Le Monde*, 11 October 2019, https://www.lemonde.fr/afrique/article/2019/10/11/en-cote-d-ivoire-les-cyber-arnaqueurs-se-reinventent-au-gre-des-nouvelles-technologies_6015132_3212.html (accessed 27 May 2020).
- ⁴³ 'Behind the "From" Lines: Email Fraud on a Global Scale Ten Cybercriminal Organizations Unmasked', *AGARI Data*, 7 January 2020, <https://www.agari.com/cyber-intelligence-research/whitepapers/behind-the-from-lines.pdf> (accessed 5 February 2020).
- ⁴⁴ 'Intelligence Report: Nigerian Confraternities Emerge as Business Email Compromise Threat', *Crowdstrike Global Intelligence team*, 03 May 2018 <https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf> (accessed 15 January 2020).
- ⁴⁵ Such as key-loggers and encryption service providers.
- ⁴⁶ 'Cybercrime in West Africa: Poised for an Underground Market', *Trend Micro & INTERPOL*, 2017, <https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf> (accessed 02 February 2019).
- ⁴⁷ According to AGARI Data, the OCG members were involved in the following function: "business intelligence (lead generation), sales management (assignment of leads), email marketing (semi-customized BEC attack emails), sales (the scam itself, conducted while paying specific attention to the victim), financial operations (receiving, moving and extracting the funds) and human resources (recruiting and managing money mules.)" 'London Blue UK-Based Multinational Gang Runs BEC Scams like a Modern Corporation', *AGARI Data*, 09 November 2018, <https://www.agari.com/cyber-intelligence-research/whitepapers/london-blue-report.pdf> (accessed 18 March 2020).
- ⁴⁸ *ibid.*
- ⁴⁹ 'Cybercrime in West Africa: Poised for an Underground Market', *Trend Micro & INTERPOL*, 2017, <https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf> (accessed 2February 2019).
- ⁵⁰ '281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes', *U.S. Department of Justice*, 10 September 2019, <https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds> (accessed 12 February 2020).
- ⁵¹ 'Intelligence Report: Nigerian Confraternities Emerge as Business Email Compromise Threat', *Crowdstrike Global Intelligence team*, 03 May 2018, <https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf> (accessed 15 January 2020).
- ⁵² J. Munshaw, J. Schultz, 'Hiding in Plain Sight', *Talos Blog*, 5 April 2019, <https://blog.talosintelligence.com/2019/04/hiding-in-plain-sight.html> (accessed 10 April 2020).
- ⁵³ 'Deleted Facebook Cybercrime Groups Had 300,000 Members', *Krebs Security*, 16 April 2018, <https://krebsonsecurity.com/2018/04/deleted-facebook-cybercrime-groups-had-300000-members/> (accessed 10 April 2020).
- ⁵⁴ J. Munshaw, J. Schultz, 'Hiding in Plain Sight', *Talos Blog*, 5 April 2019, <https://blog.talosintelligence.com/2019/04/hiding-in-plain-sight.html> (accessed 10 April 2020).
- ⁵⁵ 'EFCC Arrests Ismaila Mustapha (a.k.a Mompha) for Alleged Fraud and Money Laundering', *EFCC*, 22 October 2019, <https://efccnigeria.org/efcc/news/5004-efcc-arrests-ismaila-mustapha-a-k-a-mompha-for-alleged-fraud-and-money-laundering> (accessed 09 June 2020).
- ⁵⁶ 'FBI probe: Banker, wife in EFCC net over alleged \$1.49m laundering', *The Sun*, 04 November 2019, <https://www.sunnewsonline.com/fbi-probe-banker-wife-in-efcc-net-over-alleged-1-49m-laundering> (accessed 09 June 2020).
- ⁵⁷ 'Report of Nigeria National risk assessment on money laundering and terrorism financing 2016', *National (money laundering & terrorist financing) risk assessment forum*, 2016, https://www.giaba.org/media/f/1049_Nigeria%20-%20AML-CFT%20Nationa%20Risk%20Assessment2017.pdf (09 June 2020).
- ⁵⁸ 'Money laundering: BDC operators urged to embrace self-regulation', *Punch*, 06 September 2019, <https://punchng.com/money-laundering-bdc-operators-urged-to-embrace-self-regulation/> (accessed 09 June 2020).
- ⁵⁹ 'Scarlet Widow BEC Bitcoin Laundry: Scam, Rinse, Repeat. Part 2: Nigeria-Based Scammer Group Targets Nonprofits and Schools; Lauanders Stolen Gift Cards Through Online Cryptocurrency Exchanges', *AGARI Data*, 26 February 2019, <https://www.agari.com/cyber-intelligence-research/whitepapers/scarlet-widow-bec-scams.pdf> (accessed 05 February 2020).
- ⁶⁰ Definition retrieved from INTERPOL public website www.interpol.int.
- ⁶¹ 'Cybercriminalité : 8 Nigériens arrêtés à Mbao pour «sextorsion»', *Seneweb*, 6 April 2020, <https://www.seneweb.com/news/Societe/cybercriminalite-8-nigeriens-arretes-a-m-n-313868.html> (accessed 15 June 2020).
- ⁶² Sextortion expert: Men targeted more often', *WKBW Buffalo*, <https://www.wkbw.com/news/sextortion-expert-men-targeted-more-often> (accessed 15 June 2020).
- ⁶³ 'Beware of sextortion - Cyber Security', *Ghana News Agency*, 11 February 2020, <https://ghananewsagency.org/social/beware-of-sextortion-cyber-security-163861> (accessed 15 February 2020).
- ⁶⁴ 'Cybercriminalité et utilisation d'Internet par des groupes criminels africains', *Service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée (SIRASCO), Direction centrale de la police judiciaire (DCPJ)*, 19 June 2020.
- ⁶⁵ 'Moroccan Police Set Up Laboratories to Fight Sextortion', *MWN*, 25 February 2017, <https://www.morocoworldnews.com/2017/02/209454/moroccan-police-set-five-laboratories-fight-sextortion/> (accessed 15 June 2020).
- ⁶⁶ 'Sextortion scams on the rise', *ENCA*, 3 September 2019, <https://www.enca.com/life/cyber-criminals-blackmail-unsuspecting-victims> (accessed 15 June 2020).

- ⁶⁷ 'WhatsApp 'sextortion' scam back on the rise in SA', *BusinessTech*, 13 August 2018, <https://businesstech.co.za/news/mobile/264357/whatsapp-sextortion-scam-back-on-the-rise-in-sa/> (accessed 15 June 2020).
- ⁶⁸ 'La cybercriminalité en RDC en chiffres', *Tresor Kalonji Blog*, 24 September 2018, <http://tresorkalonji.pro/2018/09/la-cybercriminalite-en-rdc-en-chiffres.html> (accessed 12 June 2020).
- ⁶⁹ 'Sextorsion et chantage à la Webcam : la triste histoire de la Camerounaise Christelle N.', *Digital Business Africa*, 28 April 2016, <https://www.digitalbusiness.africa/chantage-et-arnaque-a-la-webcam-la-triste-histoire-de-la-camerounaise-christelle-n/> (accessed 15 June 2020).
- ⁷⁰ '\$105m Lost In 2018 Through Cybercrime – Dr. Yankson', *Modern Ghana*, 05 May 2019, <https://www.modernghana.com/news/930163/105m-lost-in-2018-through-cybercrime-dr-yankso.html> (accessed 07 May 2020).
- ⁷¹ Interview with representative of Mayina Non-Governmental Organization (NGO), Yaoundé, January 2020.
- ⁷² Definition retrieved from INTERPOL public website and documents www.interpol.int.
- ⁷³ 'Le Bénin serre la vis contre les cybers criminels', *RFI*, 05 April 2018, <http://www.rfi.fr/fr/afrique/20180405-benin-serre-vis-cyber-criminels> (accessed 15 June 2020).
- ⁷⁴ 'État de la menace liée au numérique en 2019', *Ministère de l'intérieur*, 2019, <https://www.interieur.gouv.fr/content/download/117535/942891/file/Rapport-Cybermenaces2019-HD-web-modifi%C3%A9.pdf> (accessed 10 May 2020).
- ⁷⁵ 'Guinée: une fille se fait arnaquer par un homme qu'elle a rencontré sur Facebook', *Radio FM Liberte*, <https://www.fmliberte.com/accueil/zoom-news/item/5359-guin%C3%A9e-une-fille-se-fait-arnaquer-par-un-homme-qu%E2%80%99elle-a-rencontr%C3%A9-sur-facebook.html?start=10> (accessed 15 June 2020).
- ⁷⁶ 'Behind the "From" Lines: Email Fraud on a Global Scale Ten Cybercriminal Organizations Unmasked', *AGARI Data*, 7 January 2020, <https://www.agari.com/cyber-intelligence-research/whitepapers/behind-the-from-lines.pdf> (accessed 5 February 2020).
- ⁷⁷ 'Man from Ghana duped Virginia woman out of \$300K in online romance scam, feds say', *06News*, 03 October 2019, <https://wtvr.com/2019/10/03/man-from-ghana-swindles-virginia-woman-out-of-300000-feds-say/> (accessed 15 June 2020).
- ⁷⁸ 'Anatomy Of A Scam: Nigerian Romance Scammer Shares Secrets', *Forbes*, 25 November 2019, <https://www.forbes.com/sites/ajdellinger/2019/11/25/anatomy-of-a-scam-nigerian-romance-scammer-shares-secrets/#54b7e6657638> (accessed 16 June 2020).
- ⁷⁹ 'La DGSN sensibilise à diverses escroqueries au Maroc et à l'étranger', *Media24*, 31 October 2019, <https://www.medias24.com/la-dgsn-sensibilise-le-public-a-diverses-escroqueries-au-maroc-et-a-l-etranger-5241.html> (accessed 16 June 2020).
- ⁸⁰ 'Internet Financial Scams', *US Embassy in Egypt*, <https://eg.usembassy.gov/u-s-citizen-services/local-resources-of-u-s-citizens/scams/> (accessed 16 June 2020).
- ⁸¹ 'Cybercriminalité : Trois camerounais interpellés par la police congolaise', *ACP*, 15 November 2019, <https://www.agencecamerounpresse.com/societe/soci%C3%A9t%C3%A9/cybercriminalit%C3%A9-trois-camerounais-interpell%C3%A9s-par-la-police-congolaise.html> (accessed 16 June 2020).
- ⁸² 'SABRIC Cautions Women to be Alert on Dating Sites and Social Media Platforms', *SABRIC*, <https://www.sabric.co.za/media-and-news/press-releases/sabric-cautions-women-to-be-alert-on-dating-sites-and-social-media-platforms/> (accessed 16 June 2020).
- ⁸³ M. Edwards, 'The Geography of Online Dating Fraud', *Cyber Security Group - University of Bristol*, 8 April 2018, <https://www.ieee-security.org/TC/SPW2018/ConPro/papers/edwards-conpro18.pdf> (accessed 15 April 2020).
- ⁸⁴ Definition retrieved from INTERPOL public website and documents www.interpol.int.
- ⁸⁵ '2018 Phishing trends and Intelligence report', *Phishlab*, May 2018, https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf (16 June 2020).
- ⁸⁶ 'South Africa At Higher Risk Of Data Breaches, Says Phishing Trend Report', *Cofense*, 15 January 2018, <https://cofense.com/south-africa-higher-risk-data-breaches-says-phishing-trend-report/> (accessed 16 June 2020).
- ⁸⁷ 'Demystifying Africa's Cyber Security Poverty Line', *Serianu Cyber Threat Intelligence Team*, 27 July 2018, <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf> (accessed 28 March 2020).
- ⁸⁸ Based on 800 respondents across South Africa, Kenya, Nigeria, Ghana, Egypt, Morocco, Mauritius and Botswana. 'Whitepaper: African Cybersecurity Research Report', *KnowBe4*, 11 December 2019, <https://www.knowbe4.com/hubfs/African%20Cybersecurity%20Research%20Report.pdf> (accessed 16 June 2020).
- ⁸⁹ Definition retrieved from INTERPOL website and documents www.interpol.int.
- ⁹⁰ 'Cybercrime in West Africa: Poised for an Underground Market', *Trend Micro* 2017, <https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf> (accessed 30 May 2020).
- ⁹¹ Definition retrieved from INTERPOL public website and documents www.interpol.int.
- ⁹² 'Cybercrime in West Africa: Poised for an Underground Market', *Trend Micro* 2017, <https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf> (accessed 30 May 2020).
- ⁹³ 'UEMOA : De nouveaux modes de fraude au Mobile Money détectés par la BCEAO', *DMF*, 29 January 2020, <https://droitmediasfinance.com/uemoa-de-nouveaux-modes-de-fraude-au-mobile-money-detectes-par-la-bceao/> (accessed 19 June 2020).
- ⁹⁴ 'Les arnaques récurrentes', *French Ministry of Foreign Affairs*, 20 July 2019, <https://cm.ambafrance.org/Les-arnaques-recurrentes> (accessed 17 June 2020).
- ⁹⁵ 'DCI warns Kenyans against falling for online scams', *Citizen Digital*, 20 November 2019, <https://citizentv.co.ke/news/dci-warns-kenyans-against-falling-for-online-scams-304661/> (accessed 17 June 2020).
- ⁹⁶ 'La DGSN sensibilise à diverses escroqueries au Maroc et à l'étranger', *Media24*, 29 October 2019, <https://www.medias24.com/la-dgsn-sensibilise-le-public-a-diverses-escroqueries-au-maroc-et-a-l-etranger-5241.html> (accessed 17 June 2020).
- ⁹⁷ 'Common Scams In Zimbabwe: Beware!', *Startupbi.co.zw*, 18 February 2019, <https://startupbiz.co.zw/common-scams-in-zimbabwe-beware/> (accessed 17 June 2020).
- ⁹⁸ Ongoing armed conflict that started in late 2017 between separatist groups seeking independence for Northwest (NW) and Southwest (SW) English-speaking regions from mostly French-speaking Cameroon.
- ⁹⁹ 'Cameroon 2019 Crime & Safety Report', *U.S. Department of State*, 19 June 2019, <https://www.osac.gov/Country/Cameroon/Content/Detail/Report/b1678858-8009-43c5-9c7b-160eea6972d9> (accessed 30 March 2020).
- ¹⁰⁰ Information retrieved from INTERPOL public website, <https://www.interpol.int/> (accessed 12 May 2020).
- ¹⁰¹ *ibid.*
- ¹⁰² 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in Africa', public version, *INTERPOL*, 2018.

- ¹⁰³ G. John, 'Analyzing the Influence of Information and Communication Technology on the Scourge of Human Trafficking in Rwanda', *Innovative Journal*, 01 January 2018, <http://innovativejournal.in/index.php/assj/article/view/1940/1592> (accessed 16 January 2020).
- ¹⁰⁴ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in Africa', public version, *INTERPOL*, 2018.
- ¹⁰⁵ 'European Migrant Smuggling Centre 4th Annual Report 2019', *Europol*, 2019 (accessed 15 May 2020).
- ¹⁰⁶ 'Cybercriminalité et utilisation d'Internet par des groupes criminels africains', *Service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée (SIRASCO), Direction centrale de la police judiciaire (DCPJ)*, 19 June 2020.
- ¹⁰⁷ Sertan Sanderson, 'More Ivorian women smuggled into slavery and sexual abuse', *Infomigrants*, 21 October 2019, <https://www.infomigrants.net/en/post/20273/more-ivorian-women-smuggled-into-slavery-and-sexual-abuse> (accessed 18 January 2020).
- ¹⁰⁸ 'Trafficking in persons report', *Department of State*, June 2019, <https://www.state.gov/wp-content/uploads/2019/06/2019-Trafficking-in-Persons-Report.pdf> (accessed 23 October 2019).
- ¹⁰⁹ 'Trafic d'êtres humains: La Dic neutralise une mafia nigérienne à Ovest Foire', *leral.net*, 14 March 2019, https://www.leral.net/Trafic-d-êtres-humains-La-Dic-neutralise-une-mafia-nigerienne-a-Ovest-Foire_a245115.html (accessed 18 January 2020).
- ¹¹⁰ 'Trafficking in Persons Report – Cameroon', *United States Department of State*, 28 June 2018, <https://www.refworld.org/docid/5b3e0b814.html> (accessed 29 January 2020).
- ¹¹¹ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in Africa', public version, *INTERPOL*, 2018.
- ¹¹² Subject-matter expert interview, Mayina Africa NGO, January 2020.
- ¹¹³ 'Why Human Trafficking is breaking up families in Burundi', *Burundi Times*, 12 September 2019, <https://www.burunditimes.com/why-human-trafficking-is-breaking-up-families-in-burundi/> (accessed 23 June 2020).
- ¹¹⁴ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Southern African Region', public version, *INTERPOL*, 2018.
- ¹¹⁵ 'Sexual exploitation', *New challenges, new answers*, *Fondation Scelles*, 4 July 2019, http://fondationscelles.org/pdf/RM5/5th_Global_Report_Fondation_SCELLES_2019_download.pdf (accessed 23 March 2020).
- ¹¹⁶ O. Pinnell, J.Kelly, 'Slave markets found on Instagram and other apps', *BBC*, 31 October 2019, <https://www.bbc.com/news/technology-50228549> (accessed 04 March 2020).
- ¹¹⁷ M. Vidal, 'Discounted maids!': How Ads Trap Women in Modern-Day Slavery in Jordan', *The World*, 14 June 2019, <https://www.pri.org/stories/2019-06-14/maids-sale-how-ads-trap-women-modern-day-slavery-jordan> (accessed 04 March 2020).
- ¹¹⁸ 'Rapport annuel 2017, Traite et trafic des êtres humains en ligne', *Myria - Migration Federal Center*, September 2017, <https://www.myria.be/fr/publications/rapport-annuel-2017-traite-et-traffic-des-êtres-humains-en-ligne> (accessed 19 March 2020).
- ¹¹⁹ 'Global study on smuggling of migrants 2018', *UNODC*, June 2018, https://reliefweb.int/sites/reliefweb.int/files/resources/GLOSOM_2018_web_small.pdf (accessed 15 December 2019)
- ¹²⁰ 'Tackling the root causes of human trafficking and smuggling from Eritrea', *International Refugee Rights Initiative (IRRI)*, 8 November 2017, <https://www.refworld.org/docid/5a5f5ed44.html> (accessed 29 January 2020).
- ¹²¹ 'Global Study on Smuggling of Migrants 2018', *UNODC*, June 2018.
- ¹²² 'Conditions and Risks of Mixed Migration in North East Africa', *Mixed Migration Hub*, November 2015, <http://www.mixedmigrationhub.org/wp-content/uploads/2015/11/Conditions-and-Risks-in-Mixed-Migration-in-North-East-Africa.pdf> (accessed 18 January 2020).
- ¹²³ 'Focus on Western Mediterranean Route: Frontex in Spain', *Frontex*, 3 August 2017, <https://frontex.europa.eu/media-centre/focus/focus-on-western-mediterranean-route-frontex-in-spain-isGpCE> (accessed 12 May 2020).
- ¹²⁴ Information retrieved from INTERPOL public website, <https://www.interpol.int/> (accessed 23 June 2020).
- ¹²⁵ 'Rapport annuel 2017, Traite et trafic des êtres humains en ligne', *Myria - Migration Federal Center*, September 2017, <https://www.myria.be/fr/publications/rapport-annuel-2017-traite-et-traffic-des-êtres-humains-en-ligne> (accessed 19 March 2020).
- ¹²⁶ 'Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography', Article 2, *United Nations*, 2000 (accessed 15 May 2020).
- ¹²⁷ Information gathered on crimes against children in Africa from the following sources: 'Module 12: Interpersonal Cybercrime - Online child sexual exploitation and abuse', *UNODC*, <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html> (accessed 14 May 2020); 'Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse', *ECPAT International and ECPAT Luxembourg*, Interagency Working Group - Luxembourg, 28 January 2016, pp. 23-25-28-49 (accessed 15 May 2020); 'The dark side of the Internet for children, online child sexual exploitation in Kenya - a rapid assessment report February 2018', *Terre des hommes*, p. 7 https://www.terredeshommes.nl/sites/tdh/files/uploads/tdhnl_ocse_in_kenya_research_report_feb_2018.pdf (accessed 15 May 2020); 'Understanding African Children's use of ICT', *ECPAT International*, 2013 (accessed 15 May); 'Sexual Exploitation of Children in Africa: A Silent Emergency', *African Child Policy Forum*, November 2019, <https://app.box.com/s/sukg04vmka7xcfib1tp05i9alsdrj45l> (accessed 15 May 2020); 'Rapport Global suivi de la mise en œuvre des actions de lutte contre l'exploitation sexuelle des enfants - Burkina Faso', *ECPAT*, 2016, p. 17, https://www.ecpat.org/wp-content/uploads/2016/04/a4a_v2_af_burkina_faso_2.pdf (accessed 15 May 2020); 'L'exploitation sexuelle des enfants en Côte d'Ivoire', *SOS Violences Sexuelles, ECPAT France, ECPAT Luxembourg and ECPAT International*, 4 October 2018, p. 11 (accessed 15 May 2020); 'Analyse situationnelle de l'Exploitation Sexuelle des Enfants à des fins Commerciales en Côte d'Ivoire', *ECPAT*, 2016, pp.37-39-50, <https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Etude-Cote-Ivoire-30-mars-version-web-HD-compressed.pdf> (accessed 15 May 2020); 'Rapport Global suivi de la mise en œuvre des actions de lutte contre l'exploitation sexuelle des enfants - Niger', *ECPAT*, 2017, p. 14, https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/A4A_NIGER-min.pdf (accessed 15 May 2020); 'Rapport sur l'exploitation Sexuelle des enfants au Sénégal', *ECPAT France, ECPAT Luxembourg and ECPAT International*, 29 March 2018, <http://www.ecpat.org/wp-content/uploads/2018/07/Universal-Periodical-Review-Sexual-Exploitation-of-Children-Senegal-FR.pdf> (accessed 15 May 2020); 'The Dark Side of the Internet for Children: Online Child Sexual Exploitation in Kenya - A Rapid Assessment Report', *Terre des Hommes*, February 2018, pp. 25-26, https://www.terredeshommes.nl/sites/tdh/files/uploads/tdhnl_ocse_in_kenya_research_report_feb_2018.pdf (accessed 15 May 2020); 'Country Overview: A Report on the Scale, Scope and Context of the Sexual Exploitation of Children: Uganda', *ECPAT*, 2019, p. 12, <https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2019/05/ECPAT-Country-Overview-Report-Uganda-April-2019.pdf> (accessed 15 May 2020); 'Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography', Article 2, *United Nations*, 2000. (accessed 15 May 2020); 'Rapport Global suivi de la mise en œuvre des actions de lutte contre l'exploitation sexuelle des enfants - Mali', *ECPAT*, 2017, p. 15, https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/A4A_MALI-min.pdf (accessed 15 May 2020); 'Rapport global de suivi de la mise en œuvre des actions de lutte contre l'exploitation sexuelle des enfants à des fins commerciales - Madagascar', *ECPAT*, 2018, <https://ecpat-france.fr/www.ecpat->

- france/wp-content/uploads/2018/10/rapport-global-de-suivi-2015-madagascar-ilovepdf-compressed.pdf (accessed 15 May 2020); Supplementary report on 'Sexual Exploitation of Children in Mozambique', *ECPAT International and Rede da Criança*, 1 November 2018, <http://www.ecpat.org/wp-content/uploads/2018/07/Convention-on-the-Rights-of-the-Child-report-on-Sexual-Exploitation-of-Children-to-the-Committee-on-the-Rights-of-the-Child-Mozambique-English-2018.pdf> (accessed 15 May 2020).
- ¹²⁸ 'Sexual exploitation', New challenges, new answers', *Fondation Scelles*, 4 July 2019, http://fondationscelles.org/pdf/RM5/5th_Global_Report_Fondation_SCELLES_2019_download.pdf (accessed 23 March 2020).
- ¹²⁹ 'Trafficking in persons report', *Department of State*, June 2019, <https://www.state.gov/wp-content/uploads/2019/06/2019-Trafficking-in-Persons-Report.pdf> (accessed 23 October 2019)
- ¹³⁰ S. A. Hardy, "Illicit Trafficking, Provenance Research and Due Diligence: The State of the Art", *UNESCO*, 30 March 2016 (accessed 11 May 2020).
- ¹³¹ A. Al-Azm, K. A. Paul, 'How Facebook Made It Easier Than Ever to Traffic Middle Eastern Antiquities', *World Politics Review*, 2018, 14 August 2018, <https://www.worldpoliticsreview.com/insights/25532/how-facebook-made-it-easier-than-ever-to-traffic-middle-eastern-antiquities> (accessed 11 May 2020).
- ¹³² 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in Africa', public version, *INTERPOL*, 2018.
- ¹³³ A. Al-Azm, K. A. Paul, 'How Facebook Made It Easier Than Ever to Traffic Middle Eastern Antiquities', *World Politics Review*, 2018, 14 August 2018, <https://www.worldpoliticsreview.com/insights/25532/how-facebook-made-it-easier-than-ever-to-traffic-middle-eastern-antiquities> (accessed 11 May 2020).
- ¹³⁴ *ibid*
- ¹³⁵ *ibid*.
- ¹³⁶ 'Most Antiquities Sold Online Are Fake or Illegal', *Smart News*, 03 November 2017 <https://www.smithsonianmag.com/smart-news/most-antiquities-sold-online-are-fake-or-illegal-180967062/> (accessed 11 May 2020).
- ¹³⁷ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Southern African Region', public version, *INTERPOL*, 2018.
- ¹³⁸ 'Fighting the Illicit Trafficking of Cultural Property', *UNESCO*, 2018, p. 79 (accessed 11 May 2020).
- ¹³⁹ *ibid*, p. 80.
- ¹⁴⁰ L. Daftari, 'Facebook Purges Pages Offering Priceless ISIS Plunder for Sale', *Fox News*, 11 June 2015, <http://www.foxnews.com/world/2015/06/11/facebook-purges-pages-offering-priceless-isis-plunder-for-sale.html> (accessed 11 May 2020).
- ¹⁴¹ A. Al-Azm, K. A. Paul, 'How Facebook Made It Easier Than Ever to Traffic Middle Eastern Antiquities', *World Politics Review*, 2018, 14 August 2018, <https://www.worldpoliticsreview.com/insights/25532/how-facebook-made-it-easier-than-ever-to-traffic-middle-eastern-antiquities> (accessed 11 May 2020).
- ¹⁴² *ibid* p. 80.
- ¹⁴³ 'Egyptian Embassy in Paris Retrieves Stolen Artefact', *Aswat Masrya*, 30 June 2016, <https://allafrica.com/stories/201606301179.html> (accessed 11 May 2020).
- ¹⁴⁴ E. Beswick, 'Revealed: The Usage of Looted Artefacts from Middle East Sold in Europe via Social Media', *Euro News*, 04 May 2019, <https://www.euronews.com/2019/05/03/revealed-thoUnitedStatesnds-of-looted-artefacts-from-middle-east-sold-in-europe-via-social-media> (accessed 11 May 2020).
- ¹⁴⁵ S. A. Hardy, "Illicit Trafficking, Provenance Research and Due Diligence: The State of the Art", *UNESCO*, 30 March 2016, p. 5 (accessed 11 May 2020).
- ¹⁴⁶ A. Al-Azm, K. A. Paul, 'How Facebook Made It Easier Than Ever to Traffic Middle Eastern Antiquities', *World Politics Review*, 14 August 2018, <https://www.worldpoliticsreview.com/insights/25532/how-facebook-made-it-easier-than-ever-to-traffic-middle-eastern-antiquities> (accessed 11 May 2020).
- ¹⁴⁷ *ibid*, p. 8.
- ¹⁴⁸ 'How Facebook Made It Easier Than Ever to Traffic Middle Eastern Antiquities', *World Politics Review*, 14 August 2018, (accessed 11 May 2020).
- ¹⁴⁹ *ibid*, p.5.
- ¹⁵⁰ 'How Facebook Made It Easier Than Ever to Traffic Middle Eastern Antiquities', *World Politics Review*, 14 August 2018, (accessed 11 May 2020).
- ¹⁵¹ 'Egypt Grapples with Smuggling of Artifacts', *Arab News*, 08 February 2020, <https://www.arabnews.com/node/1624881/middle-east> (accessed 11 May 2020).
- ¹⁵² 'Countering Illicit Traffic in Cultural Goods, The Global Challenge of Protecting the World's Heritage', *ICOM*, 2015 (accessed 11 May 2020).
- ¹⁵³ 'Démantèlement d'un réseau de trafic d'antiquités sur le dark web', *Mosaïque FM*, 29 mai 2018, <https://www.mosaiquefm.net/fr/actualite-faits-divers/351454/arrestation-d-un-reseau-de-traffic-d-antiquites-sur-le-dark-web> (accessed 25 June 2019).
- ¹⁵⁴ A. Al Azm, K. A. Paul, 'Facebook's Black Market in Antiquities: Trafficking, Terrorism and War Crimes', *Alliance to Counter Crime Online*, June 2019, <https://static1.squarespace.com/static/5e3a7fb845f8c668df48d437/t/5e4e58ef0caa64606351a54b/1582192944742/ATHAR-FB-Report-June-2019.pdf> (accessed 02 May 2020).
- ¹⁵⁵ 'Out of Africa: Byting Down on Wildlife Cybercrime', *IFAW*, July 2017, https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/%28Pixelated%20Webversion%29SAInvestigationReport_lores.pdf (accessed 16 December 2019).
- ¹⁵⁶ 'Combating Wildlife Crime Linked to the Internet: Global Trends and China's Experiences', *TRAFFIC*, July 2019, <https://www.traffic.org/site/assets/files/12352/combating-wildlife-crime-online-chinas-experiences.pdf> (accessed 03 June 2020).
- ¹⁵⁷ L. Nitsche, 'Mobile solutions a catalyst for Internet penetration in Kenya', *DW*, 17 January 2019, <https://www.dw.com/en/mobile-solutions-a-catalyst-for-internet-penetration-in-kenya/a-47078206> (accessed 03 June 2020).
- ¹⁵⁸ 'Out of Africa: Byting Down on Wildlife Cybercrime', *IFAW*, July 2017, https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/%28Pixelated%20Webversion%29SAInvestigationReport_lores.pdf (accessed 16 December 2019).
- ¹⁵⁹ 'Wildlife Cybercrime in Asia Wildlife Cybercrime in Asia', *TRAFFIC*, <https://www.traffic.org/what-we-do/projects-and-approaches/wildlife-crime/wildlife-cybercrime-in-asia/> (accessed 03 June 2020).
- ¹⁶⁰ *ibid*.
- ¹⁶¹ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Western African Region', public version, *INTERPOL*, 2018.

- ¹⁶² T. Alimi, 'Yahoo Boys: Nigeria's Newest Players in the Illegal Ivory Trade', *The Nation*, 24 November 2018, <http://thenationonlineng.net/yahoo-boys-nigerias-newest-players-illegal-ivory-trade> (accessed 06 May 2020).
- ¹⁶³ 'Wildlife Traffickers Are Setting Up Fake Zoos On Facebook To Sell The Scales Of Endangered Pangolins', *BuzzFeed News*, 06 May 2020, <https://www.buzzfeednews.com/article/ryanhatethis/fake-pangolin-zoos-facebook-trafficking> (accessed 25 June 2020).
- ¹⁶⁴ *ibid.*
- ¹⁶⁵ S. Haysom, 'In Search of Cyber-Enabled Disruption', *GIATOC*, February 2019, p.5 (accessed 07 May 2020).
- ¹⁶⁶ J. Okojie, 'Pangolins: Vanishing in the Wild', *BusinessDay Online*, 06 December 2018, <https://businessday.ng/investigation/investigation-investigation/article/pangolins-vanishing-in-the-wild> (accessed 07 May 2020).
- ¹⁶⁷ S. Haysom, 'In Search of Cyber-Enabled Disruption', *GIATOC*, February 2019, p.11 (accessed 07 May 2020).
- ¹⁶⁸ J. Okojie, 'Pangolins: Vanishing in the Wild', *BusinessDay Online*, 06 December 2018 (accessed 07 May 2020).
- ¹⁶⁹ 'African Grey Parrot: Complex web of trafficking thrives despite CITES rule', *The East African*, 9 March 2019, <https://www.theeastafrican.co.ke/scienceandhealth/African-grey-parrot-complex-web-of-trafficking-thrives/3073694-5016160-1252pfe/index.html> (accessed 26 June 2020).
- ¹⁷⁰ 'Scams Warning', *U.S. Embassy in Cameroon*, <https://cm.usembassy.gov/u-s-citizen-services/local-resources-of-u-s-citizens/scams-warning/> (accessed 29 June 2020).
- ¹⁷¹ S. Haysom, 'In Search of Cyber-Enabled Disruption', *GIATOC*, February 2019, p.5 (accessed 07 May 2020).
- ¹⁷² S. Rebekka Runhovde, 'Illegal online trade in reptiles from Madagascar', *GIATOC*, 2018, <https://globalinitiative.net/illegal-online-trade-in-reptiles-from-madagascar> (accessed 07 May 2020).
- ¹⁷³ *ibid.*, p.12.
- ¹⁷⁴ 'Stench Leads to Home Crawling with Stolen Tortoises—10,000 of Them', *National Geographic*, 20 April 2018, <https://www.nationalgeographic.com/news/2018/04/wildlife-watch-radiated-tortoises-poached-madagascar> (accessed 16 March 2020).
- ¹⁷⁵ 'Madagascar: 76 tortues radiées et du cannabis saisis dans une maison à Tuléar', *RFI*, 24 January 2018, <http://www.rfi.fr/fr/afrique/20180124-madagascar-76-tortues-radiées-cannabis-saisis-une-maison-tulear> (accessed 10 April 2020).
- ¹⁷⁶ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Central African Region', public version, *INTERPOL*, 2018.
- ¹⁷⁷ 'A Game of Stones', *Global Witness*, June 2017, <https://www.globalwitness.org/en/campaigns/central-african-republic-car/game-of-stones/> (accessed 24 May 2020).
- ¹⁷⁸ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Central African Region', public version, *INTERPOL*, 2018.
- ¹⁷⁹ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in Africa', public version, *INTERPOL*, 2018.
- ¹⁸⁰ 'The Online Trade of Light Weapons in Libya', *Small Arms Survey*, April 2016, <http://www.smallarmssurvey.org/fileadmin/docs/R-SANA/SANA-Dispatch6-Online-trade.pdf> (accessed 15 March 2020).
- ¹⁸¹ N. R. Jenzen-Jones & I. McCollum, 'Web Trafficking: Analysing the Online Trade of Small Arms and Light Weapons in Libya', *Small Arms Survey*, April 2017, <http://www.smallarmssurvey.org/fileadmin/docs/F-Working-papers/SAS-SANA-WP26-Libya-web-trafficking.pdf> (accessed 15 March 2020).
- ¹⁸² E. Dubuis, 'Le trafic d'armes se développe sur Facebook', *Le Temps*, 08 April 2016, <https://www.letemps.ch/monde/trafic-darmes-se-developpe-facebook> (accessed 01 May 2020).
- ¹⁸³ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in Africa', public version, *INTERPOL*, 2018.
- ¹⁸⁴ *ibid.*, p. 79.
- ¹⁸⁵ J. Eligh, 'The Evolution of Illicit Drug Markets and Drug Policy in Africa Continental Report', *ENACT*, 03 June 2019, <https://enact-africa.s3.amazonaws.com/site/uploads/2019-06-30-continental-report-3-3.pdf> (accessed 10 May 2020).
- ¹⁸⁶ 'État de la menace liée au numérique en 2019', *Ministère de l'intérieur*, 2019, <https://www.interieur.gouv.fr/content/download/117535/942891/file/Rapport-Cybermenaces2019-HD-web-modif%C3%A9.pdf> (accessed 10 May 2020).
- ¹⁸⁷ 'EU Drug Markets Report 2019', *Europol and EU Drug Agency (EMCDDA)*, 26 November 2020, https://www.europol.europa.eu/sites/default/files/documents/drug_markets_report_2019_pdf.pdf (accessed 18 June 2020).
- ¹⁸⁸ In Western Africa, Senegal for example has integrated the fight of online illicit drug trafficking in a national strategic paper for the period 2016-2020.
- ¹⁸⁹ C. Nwannennaya and TF. Abiodun, 'Illicit Drug Trafficking in Nigeria: Obstacle to National Development and Security', *Journal of Political Sciences & Public Affairs*, Vol. 5, Issue 1, 2017, <https://www.longdom.org/open-access/illicit-drug-trafficking-in-nigeria-obstacle-to-national-development-andsecurity-2332-0761-1000230.pdf> (accessed 10 May 2020).
- ¹⁹⁰ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Southern African Region', public version, *INTERPOL*, 2018.
- ¹⁹¹ 'Trafic de stupéfiants : un couple d'Éthiopiens en détention', *Ouest France*, January 2020, <https://www.ouest-france.fr/normandie/flers-61100/flers-trafic-de-stupefiants-un-couple-d-ethiopiens-en-detention-6710559> (accessed 10 May 2020).
- ¹⁹² 'Sur les chemins globalisés du khat, cette « amphétamine » de la Corne de l'Afrique', *Le Monde Afrique*, 21 June 2019, https://www.lemonde.fr/afrique/article/2019/06/21/sur-les-chemins-globalises-du-khat-cette-amphetamine-de-la-corne-de-l-afrique_5479842_3212.html (accessed 10 May 2020).
- ¹⁹³ 'La propagation du khat dans un marché mondialisé', *France Info*, 23 June 2019, https://www.francetvinfo.fr/monde/afrique/kenya/la-propagation-du-khat-dans-un-marche-mondialise_3500521.html (accessed 10 May 2020).
- ¹⁹⁴ R. Chelin, 'Drug Trafficking /Synthetic Drugs on the Rise Despite Mauritius's Best Efforts', *ENACT*, 20 April 2020, <https://enactafrica.org/enact-observer/synthetic-drugs-on-the-rise-despite-mauritiuss-best-efforts> (accessed 10 May 2020).
- ¹⁹⁵ 'Project ENACT: Serious and Organized Crime in the Northern Africa Region', public version, *INTERPOL*, 2018..
- ¹⁹⁶ 'Counterfeiting', *UNICRI website*, <http://www.unicri.it/topics/counterfeiting/> (accessed 14 May 2020).
- ¹⁹⁷ 'Global Impacts of Counterfeiting and Piracy to Reach US\$ 4.2 Trillion By 2022', *International Chamber of Commerce*, 6 February 2017, <https://iccwbo.org/media-wall/news-speeches/global-impacts-counterfeiting-piracy-reach-us4-2-trillion-2022/> (accessed 10 May 2020).
- ¹⁹⁸ D. Akoth, 'The Complexity of Counterfeiting and Piracy in Africa', *Institute of Security Studies*, <https://issafrica.org/amp/iss-today/the-complexity-of-counterfeiting-and-piracy-in-africa> (accessed 10 May 2020).
- ¹⁹⁹ 'L'Afrique peine à traquer le faux', *Jeune Afrique*, 16 June 2009, <https://www.jeuneafrique.com/202860/archives-thematique/l-afrique-peine-traquer-le-faux/> (accessed 10 May 2020).

- ²⁰⁰ 'Counterfeiting a Global Spread a Global Threat', *UNICRI*, 2011, pp. 58-59
http://www.unicri.it/topics/counterfeiting/organized_crime/reports/CTF_2011_Unedited_Edition_Final.pdf (accessed 12 May 2020).
- ²⁰¹ P. Jacquemot, 'L'Afrique des possibles : Les défis de l'émergence', *Karthala*, 2016 p. 207 (accessed 10 May 2020).
- ²⁰² P. Ramara, 'South Africa: High Online Counterfeit Goods Risk', *Mondaq*, 22 January 2019, <https://www.mondaq.com/southafrica/dodd-frank-consumer-protection-act/773528/high-online-counterfeit-goods-risk-says-survey> (accessed 10 May 2020).
- ²⁰³ R. Cartwright, A. Baric, 'The Rise of Counterfeit Pharmaceuticals in Africa', *ENACT*, 2018, <https://enact-africa.s3.amazonaws.com/site/uploads/2018-11-12-counterfeit-medicines-policy-brief.pdf> (accessed 10 May 2020).
- ²⁰⁴ 'Africa Steps up Fight against Counterfeits', *Managing Intellectual Property*, March 2017, <https://www.spoor.com/docs/4549/Feature%20Africa.pdf> (accessed 10 May 2020).
- ²⁰⁵ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in Africa', public version, *INTERPOL*, 2018.
- ²⁰⁶ 'Counterfeit Medicines and Organized Crime', *UNICRI*, 2013, p. 64, http://www.unicri.it/topics/counterfeiting/medicines/report/Ctf_medicines_and_oc_advance_unedited2013.pdf (accessed 12 May 2020).
- ²⁰⁷ *ibid*, p. 58-59
- ²⁰⁸ *ibid*, p. 111.
- ²⁰⁹ E. Przyswa, 'Contrefaçon de médicaments, et organisations criminelles', *IRACM*, 2013 p.58 (accessed 12 May 2020).
- ²¹⁰ *ibid*, p. 58-59
- ²¹¹ *ibid*.
- ²¹² *ibid*. p.33.
- ²¹³ 'Lutter contre la falsification des médicaments en Afrique', *Sanofi*, 13 July 2018, <https://www.sanofi.com/fr/media-room/articles/2018/lutter-contre-la-falsification-des-medicaments-en-afrique> (accessed 12 May 2020).
- ²¹⁴ Countries include : Angola, Benin, Burkina Faso, Cameroun, Cape Verde, Djibouti, Democratic Republic of Congo, Gambia, Côte d'Ivoire, Kenya, Malawi, Maurice, Morocco, Namibia, Rwanda, Senegal, Seychelles, South Africa, Swaziland, Tunisia, Zambia and Zimbabwe.
- ²¹⁵ G. F. Adandé, '84 tonnes de faux médicaments saisis au Bénin', *Voa Afrique*, 02 March 2017, <https://www.voaafricain.com/a/i-84-tonnes-de-feux-medicaments-saisis-au-benin-dans-la-lutte-contre-la-vente-illegale/3746807.html> (accessed 12 May 2020).
- ²¹⁶ 'Opération PANGEA X : des millions de faux médicaments saisis dans les pharmacies en ligne', *Contrefaçon riposte*, 26 September 2017, <https://www.contrefacon-riposte.info/international/5547-operation-pangea-x-des-millions-de-faux-medicaments-saisis-dans-les-pharmacies-en-ligne> (accessed 12 May 2020).
- ²¹⁷ 'Operation Pangea - Shining a Light on Pharmaceutical Crime', *INTERPOL*, 21 November 2019, <https://www.interpol.int/en/News-and-Events/News/2019/Operation-Pangea-shining-a-light-on-pharmaceutical-crime> (accessed 12 May 2020).
- ²¹⁸ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Central African Region, public version, *INTERPOL*, 2018.
- ²¹⁹ Stolen Motor Vehicle, *INTERPOL*, retrieved at <https://www.interpol.int/en/Crimes/Vehicle-crime> (accessed 11 May 2020).
- ²²⁰ S. Bridge, 'How Thieves Use Electronic Devices to Steal Cars', *CBC News*, 01 April 2016, <https://www.cbc.ca/news/business/marketplace-electronic-car-theft-1.3515106> (accessed 11 May 2020).
- ²²¹ J.Colombain, 'Nouveau monde. Qu'est-ce que le vol de voiture par "mouse jacking" ?', *France24*, 08 November 2017, https://www.france24.com/fr/replay-radio/nouveau-monde/nouveau-monde-quest-ce-que-le-vol-de-voiture-par-mouse-jacking_2435579.html (accessed 31 May 2020).
- ²²² Stolen Motor Vehicle, *INTERPOL*, retrieved at <https://www.interpol.int/en/Crimes/Vehicle-crime> (accessed 11 May 2020).
- ²²³ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Western African Region, public version, *INTERPOL*, 2018.
- ²²⁴ Information retrieved from the Southern Africa Regional Police Chiefs Cooperation Organization website: <https://sarpcoco.com/vehicle-crimes/> (accessed 11 May 2020).
- ²²⁵ 'Project ENACT Strategic Assessment: Overview of Serious and Organized Crime in the Southern African Region', public version, *INTERPOL*, 2018.
- ²²⁶ Students from the Stanford University Artificial Intelligence Laboratory and Massachusetts Institute of Technology.
- ²²⁷ Storing system for unregulated data.
- ²²⁸ Freenet was described as a "revolutionary software that offers anonymous passage into the darkest reaches of the web, where one can access everything from child pornography to instructions on how to build explosives". Source: T. McCormick, 'The Dark net: A Short History', *Foreign Policy*, 9 December 2013, <https://foreignpolicy.com/2013/12/09/the-dark-net-a-short-history/> (accessed 30 January 2020).
- ²²⁹ The Gawker exposé, published by a Gawker-affiliated blog.
- ²³⁰ The name "Silk Road" derives from the historical trade routes between Europe, India, China and other countries in 206 BC – 220 AD.
- ²³¹ The pseudonymous Dread Pirate Roberts refers to a fictional character known for its liberalist ideas and criticism of regulations. He operated the market along with two other individuals, Smedley and Variety Jones.
- ²³² Joint law enforcement operation that took down online illegal markets and arrested their vendors and administrators. The operation led to the arrest of 17 individuals and the seizure of approximately USD 1 million in Bitcoins as well as drugs, silver and gold.
- ²³³ An exit scam is a fraudulent act where a seller/promoter vanishes with the money of users.
- ²³⁴ In March 2015, Evolution moderators shut down the market and disappeared with around 12 billion dollars in customer Bitcoins.
- ²³⁵ The biggest Bitcoin exchange, Mt. Gox, went offline and its owners disappeared with 850 000 Bitcoins.
- ²³⁶ At the time of writing the report, the total number of cryptocurrencies is around 3474 with a market cap of USD 259,416,920,648. Retrieved from <https://coinmarketcap.com/all/views/all/> (accessed 15 May 2020).
- ²³⁷ Information gathered from the following sources: M. Power, 'Online Highs are Old as the Net: The First E-Commerce Was a Drugs Deal', *The Guardian*, <https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal>, 19 April 2013 (accessed 29 January 2020); J. Breeding, 'The Origin And History Of The Dark Web', *The Ranker*, 11 December 2018, <https://www.ranker.com/list/history-of-the-dark-web/jordan-breeding> (accessed 29-30 January 2020); 'TOR History', *The TOR Project*, <https://www.torproject.org/about/history/> (accessed 29 January 2020); T. McCormick, 'The Dark net: A Short History', *Foreign Policy*, 09 December 2013, <https://foreignpolicy.com/2013/12/09/the-dark-net-a-short-history/> (accessed 29-30 January 2020); 'The Dark Web: A History Lesson', *The Hacker News*, 18 May 2019, <https://hackwarenews.com/the-dark-web-a-history-lesson/> (accessed 29 January 2020); Tor .onion URLs directories, *The Hidden Wiki*, <https://thehiddenwiki.org/> (accessed 29 January 2020); B. Marr, 'A Short History of Bitcoin and Crypto Currency Everyone Should Read', *Forbes*, 06 December 2017, <https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#124366983f27> (accessed 30 January 2020); A. Rosburgh, 'A Short History of Dark net

Markets and the Impact of Disruptions Along the Way', *National Drug & Alcohol Research Center*, 18 February 2016, <https://ndarc.med.unsw.edu.au/blog/short-history-dark-net-markets-and-impact-disruptions-along-way> (accessed 30 January 2020); R. Bigmore, 'A Decade of Cryptocurrency: from Bitcoin to Mining Chips', *The Telegraph*, 25 May 2018, <https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/> (accessed 30 January 2020).

²³⁸ 'What is a VPN?', *Norton*, <https://us.norton.com/Internetsecurity-privacy-what-is-a-vpn.html> (accessed 31 January 2020).

²³⁹ 'How to Access the Dark Web / Dark net in a Secure Way?', *The Best VPN*, 6 December 2019, <https://thebestvpn.com/access-the-dark-web/> (accessed 03 February 2020).

²⁴⁰ 'TOR History', *The TOR Project*, <https://www.torproject.org/about/history/> (accessed 03 February 2020)

²⁴¹ 'Investigating Biological and Chemical Terrorism on the Dark net: Operational Manual', *INTERPOL*, 2019 (accessed 03 February 2020).

²⁴² Website retrieved at <https://duckduckgo.com/> (accessed 03 February 2020).

²⁴³ 'What's the Dark Web & How to Access It in 3 Easy Steps – 2020', *VPN Monitor*, <https://www.vpnmentor.com/blog/whats-the-dark-web-how-to-access-it-in-3-easy-steps/> (accessed 03 February 2020).

²⁴⁴ Information retrieved from Google Trends Service, term searched 'dark web' (accessed 20 February 2020).

²⁴⁵ Information gathered from the following sources: R. Joseph, 'Tech Solutions for Rhino Trade', *Oxpeckers*, August 2019, <https://oxpeckers.org/2019/08/tech-solutions/> (accessed 26 February 2020); F. Thomaz, 'Illicit Wildlife Markets and the Dark Web a Scenario of the Changing Dynamics', *The Global Initiative Against Transnational Organized Crime*, November 2018, <https://globalinitiative.net/wp-content/uploads/2018/11/TGIATOC-Dark-webReport-Web.pdf> (accessed 26 February 2020).

²⁴⁶ M. R. Fuentes, 'Digital Souks: A Glimpse into the Middle Eastern and North African Underground', *Trend Micro*, 2017, p. 37, https://documents.trendmicro.com/assets/white_papers/wp-middle-eastern-north-african-underground.pdf (accessed 26 February 2020).

²⁴⁷ 'Cybercrime in West Africa Poised for an Underground Market', *Trend Micro & INTERPOL*, 2017, p. 30-31, <https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf> (accessed 26 February 2020).

²⁴⁸ 'Illegal Wildlife Trade in the Dark net', *INTERPOL*, 2017, <https://www.interpol.int/en/News-and-Events/News/2017/Research-identifies-illegal-wildlife-trade-on-the-Darknet> (accessed 20 March 2020).

²⁴⁹ 'How the 'Dark Web' Worsens Ghana's Human Trafficking Crisis', *Small Voice Human Trafficking*, September 2018, <http://www.humantrafficking.co.za/index.php/news/2235-how-the-dark-web-worsens-ghana-s-human-trafficking-crisis-18-september-2018> (accessed 27 February 2020).

²⁵⁰ 'The Evolution of Cryptocurrency', *Euro Staff*, <https://www.eurostaffgroup.com/cryptocurrency/> (accessed 11 February 2020).

²⁵¹ P. Rao, 'Africa could be the Next Frontier for Cryptocurrency', *Africa Renewal*, April 2018 - July 2018, <https://www.un.org/africarenewal/magazine/april-2018-july-2018/africa-could-be-next-frontier-cryptocurrency> (accessed 11 February 2020).

²⁵² C. Blenkinsop, 'Crypto in Africa: Opportunities and Challenges, Explained', *Coin Telegraph*, 02 December 2019, <https://cointelegraph.com/explained/crypto-in-africa-opportunities-and-challenges-explained> (accessed 12 February 2020).

²⁵³ Ibid.

²⁵⁴ Ibid.

²⁵⁵ T. Karombo, 'Why Africa Is Fertile Ground for Bitcoin Adoption', *CCN*, 15 June 2018, <https://www.ccn.com/why-africa-is-fertile-ground-for-bitcoin-adoption/> (accessed 12 February 2020).

²⁵⁶ M. Russon, 'Crypto-currencies Gaining Popularity in Kenya', *BBC News*, 22 February 2019, <https://www.bbc.com/news/business-47307575> (accessed 12 February 2020).

²⁵⁷ Such as Abra in Malawi and Morocco, GeoPay operating in South Africa, the Kobocoin based in London and launched by a Nigerian entrepreneur, BitMari service operating in Zimbabwe, etc.

²⁵⁸ P. Rao, 'Africa could be the Next Frontier for Cryptocurrency', *Africa Renewal*, April 2018 - July 2018, <https://www.un.org/africarenewal/magazine/april-2018-july-2018/africa-could-be-next-frontier-cryptocurrency> (accessed 12 February 2020).

²⁵⁹ C. Blenkinsop, 'Crypto in Africa: Opportunities and Challenges, Explained', *Coin Telegraph*, 02 December 2019, <https://cointelegraph.com/explained/crypto-in-africa-opportunities-and-challenges-explained> (accessed 12 February 2020)

²⁶⁰ 'The Pros & Cons of Cryptocurrency', *Wall Street*, 18 September 2018, <https://wall-street.com/the-pros-cons-of-cryptocurrency/> (accessed 11 February 2020).

²⁶¹ 'The Positives, Negatives and Risks of Cryptocurrencies', *CBIZ*, 15 July 2019, <https://www.cbiz.com/insights-resources/details/articleid/7517/the-positives-negatives-and-risks-of-cryptocurrencies> (accessed 11 February 2020).

²⁶² K. Rooney, 'Crime Still Plagues Cryptocurrencies, as \$1.7 Billion as Stolen from Investors Last Year', *CNBC*, 29 January 2019, <https://www.cnbc.com/2019/01/29/crime-still-plague-cryptocurrencies-as-1point7-billion-was-stolen-last-year.html> (accessed 11 February 2020).

²⁶³ 'The Pros & Cons of Cryptocurrency', *Wall Street*, 18 September 2018, <https://wall-street.com/the-pros-cons-of-cryptocurrency/> (accessed 11 February 2020).

²⁶⁴ Conducted by the researchers at the University of Sydney and the University of Technology Sydney.

²⁶⁵ A. Sulleyman, 'Bitcoin Price is so High because Criminals are Using it for Illegal Trades', *Independent*, 24 January 2018, <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-fall-criminals-blockchain-anonymous-cryptocurrency-zcash-monero-dash-a8174716.html> (accessed 11 February 2020).

²⁶⁶ Ibid.

²⁶⁷ 'Bitcoin ATMs in Africa – Where to Find them and How They Work [2019]', *Block News Africa*, 26 November 2019, <https://blocknewsafrica.com/bitcoin-atms-in-africa/> (accessed 12 February 2020).

²⁶⁸ F. Anusionwu, 'Bitcoin ATM, Definitions, Processes and Places in Africa where you can Find a Bitcoin ATM', *Blockchain Africa*, 08 June 2019, <https://www.blockchainafrica.io/bitcoin-atm-definitions-processes-and-places-in-africa-where-you-can-find-a-bitcoin-atm/> (accessed 12 February 2020).

²⁶⁹ 'Cryptocurrency Laundering as a Service: Members of a Criminal Organization Arrested in Spain', *EUROPOL*, 08 May 2019 (accessed 12 February 2020).

²⁷⁰ For more information on the relevant taxonomy developed and used by INTERPOL's Innovation Center, please refer to <https://interpol-innovation-centre.github.io/DW-VA-Taxonomy/taxonomies/entities>.

²⁷¹ Countries such as China, Iran and Vietnam have previously tried to block access to BBC News websites. Source: 'BBC News launches 'Dark Web' Tor Mirror', *BBC News*, 23 October 2019 <https://www.bbc.com/news/technology-50150981> (accessed 30 January 2020).

- ²⁷² 'BBC News launches 'Dark Web' Tor Mirror', *BBC News*, 23 October 2019 <https://www.bbc.com/news/technology-50150981> (accessed 30 January 2020).
- ²⁷³ J. E. Dunn, 'New BBC 'Dark Web' Tor Mirror Site Aims to Beat Censorship', *Naked Security by Sophos*, 28 October 2019, <https://nakedsecurity.sophos.com/2019/10/28/new-bbc-dark-web-tor-mirror-site-aims-to-beat-censorship/> (accessed 30 January 2020).
- ²⁷⁴ 'What's the Dark Web & How to Access It in 3 Easy Steps – 2020', *VPN Monitor*, <https://www.vpnmentor.com/blog/whats-the-dark-web-how-to-access-it-in-3-easy-steps/> (accessed 04 February 2020).
- ²⁷⁵ T. McCormick, 'The Dark net: A Short History', *Foreign Policy*, 9 December 2013, <https://foreignpolicy.com/2013/12/09/the-dark-net-a-short-history/> (accessed 30 January 2020).
- ²⁷⁶ Screenshot provided by the S2W LAB.
- ²⁷⁷ Thread: each new discussion started.
- ²⁷⁸ Screenshot provided by the S2W LAB.
- ²⁷⁹ Information based on data gathered from search on the surface web.
- ²⁸⁰ Screenshot taken from dark web site.
- ²⁸¹ At the time of conducting the Trend Micro study, the aforementioned dark web markets were still online.
- ²⁸² M. R. Fuentes, 'Digital Souks: A Glimpse into the Middle Eastern and North African Underground', *Trend Micro*, 2017, p. 37, https://documents.trendmicro.com/assets/white_papers/wp-middle-eastern-north-african-underground.pdf (accessed 26 February 2020).
- ²⁸³ 'Illegal Wildlife Trade in the Dark net', *INTERPOL*, 2017, <https://www.interpol.int/en/News-and-Events/News/2017/Research-identifies-illegal-wildlife-trade-on-the-Darknet> (accessed 20 March 2020).
- ²⁸⁴ Information retrieved through the dark web crawler developed by the S2W LAB.
- ²⁸⁵ Screenshots provided by the S2W LAB.
- ²⁸⁶ Information retrieved through the dark web crawler developed by the S2W LAB.
- ²⁸⁷ Screenshot provided by the S2W LAB.
- ²⁸⁸ *ibid.*
- ²⁸⁹ Screenshot provided by the S2W LAB.
- ²⁹⁰ *ibid.*
- ²⁹¹ *ibid.*
- ²⁹² 'Firearms in Dark net: Empowering the Lone Wolf', *INTERPOL*, February 2015.
- ²⁹³ G. P. Paoli; J. Aldridge; N. Ryan; R. Warnes, 'Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web', *Rand Corporation*, 2017, p. 54, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf (accessed 27 February 2020).
- ²⁹⁴ Screenshot provided by the S2W LAB.
- ²⁹⁵ Screenshot provided by the S2W LAB.
- ²⁹⁶ *ibid.*
- ²⁹⁷ *ibid.*
- ²⁹⁸ Screenshot provided by the S2W LAB.
- ²⁹⁹ Information retrieved through the dark web crawler developed by the S2W LAB (accessed 18 March 2020).
- ³⁰⁰ Screenshot provided by the S2W LAB.
- ³⁰¹ *ibid.*
- ³⁰² M. R. Fuentes, 'Digital Souks: A Glimpse into the Middle Eastern and North African Underground', *Trend Micro*, 2017, p. 37, https://documents.trendmicro.com/assets/white_papers/wp-middle-eastern-north-african-underground.pdf (accessed 26 February 2020).
- ³⁰³ R. Joseph, 'Tech Solutions for Rhino Trade', *Oxpeckers*, August 2019, <https://oxpeckers.org/2019/08/tech-solutions/> (accessed 26 February 2020).
- ³⁰⁴ Screenshot provided by the S2W LAB.
- ³⁰⁵ Information retrieved from dark weblinks.com between October and December 2019 (accessed 25 March 2020).
- ³⁰⁶ Information retrieved through the dark web Monitor Tool developed by TNO (accessed 10 February 2020).
- ³⁰⁷ Screenshot provided by the S2W LAB.
- ³⁰⁸ Screenshot provided by the S2W LAB.
- ³⁰⁹ Information retrieved through the Dark web crawler developed by the S2W LAB.
- ³¹⁰ *VPN Usage Statistics*, GeoSurf, <https://www.geosurf.com/blog/vpn-Usage-statistics/> (accessed 18 February 2020).
- ³¹¹ 'VPNs Are Primarily Used to Access Entertainment', *Global Web Index*, 06 July 2018, <https://blog.globalwebindex.com/chart-of-the-day/vpns-are-primarily-used-to-access-entertainment/> (accessed 18 February 2020).
- ³¹² 'VPN Use and Data Privacy Stats for 2020', *VPN Monitor*, April 2020, <https://www.vpnmentor.com/blog/vpn-use-data-privacy-stats/> (accessed 18 February 2020).
- ³¹³ Information retrieved from Google Trends Service, term searched 'Virtual Private Network' (accessed 31 January 2020).
- ³¹⁴ 'Who Uses TOR?', *The TOR Project*, <https://2019.www.torproject.org/about/torusers.html.en> (accessed 26 July 2019).
- ³¹⁵ W. Nicol, 'A Beginner's Guide to Tor: How to Navigate through the Underground Internet', *Digital Trends*, <https://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-Internet/> (accessed 26 July 2019).
- ³¹⁶ Retrieved from the TOR project official website, <https://www.torproject.org/>.
- ³¹⁷ 'Organized Crime Index Africa 2019', *ENACT GIATOC*, 2019, p. 22.
- ³¹⁸ *ibid.*
- ³¹⁹ *ibid.*, p. 99.
- ³²⁰ 'Organized Crime Index Africa 2019', *ENACT GIATOC*, 2019, p. 34.
- ³²¹ INTERPOL Innovation Centre runs many initiatives related to dark web and virtual assets. More on these initiatives can be found on the following link, <https://www.interpol.int/How-we-work/Innovation/Darknet-and-Cryptocurrencies>.

► **ABOUT INTERPOL**

INTERPOL is the world's largest international police organization. Our role is to assist law enforcement agencies in our 194 member countries to combat all forms of transnational crime. We work to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. Our services include targeted training, expert investigative support, and specialized databases and secure police communications channels.

► **OUR VISION: "CONNECTING POLICE FOR A SAFER WORLD"**

Our vision is that of a world where each and every law enforcement professional will be able through INTERPOL to securely communicate, share and access vital police information whenever and wherever needed, ensuring the safety of the world's citizens. We constantly provide and promote innovative and cutting-edge solutions to global challenges in policing and security.



INTERPOL
