# Cybercrime and dark web in Africa[1]

Attila Gulyás[2]

**Abstract:**

The widespread availability of smart devices and internet access has radically transformed the continent's cybersecurity landscape. However, this sudden technological change was not accompanied by the development of a robust cybersecurity infrastructure. State actors, economic operators, and the population were unprepared for the risks associated with new technology. Criminals have taken advantage of this situation, resulting in various types of cyberattacks against actors in economic life, state institutions, critical infrastructures, and the population. The author hypothesized that there is a correlation between cybercrime rates and dark web usage in African countries. To test this hypothesis, quantitative data was collected on internet penetration, cybercrime statistics, and dark web usage. The analysis of the collected data confirmed the hypothesis that there is a correlation between a country's use of the dark web and the severity of cybercrime.

**Keywords:**
Dark web; TOR; cybercrime; ransomware; Africa.

[1] DOI: https://doi.org/10.12700/jceeas.2024.4.3-4.278

[2] Ret. Lt. Colonel, Doctoral Student, Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary; ORCID: 0000-0001-5645-144X; gulyas.attila@phd.uni-obuda.hu.

## Introduction

Thanks to the digital technical revolution that took place in the last decade, the Internet has become part of everyday life on the African continent. Social media and various internet services quickly became popular among users. The wide spread of the Internet also increased the competitiveness of economic actors, which was accompanied by an increase in international interest.

Unfortunately, the explosive spread of the Internet has not been followed by the development of cyber security. The lack of training of users, the lack of professionals and the need for financial resources, combined with the lack of legal background, led to the formation of a significant gap between the spread of Internet services and the construction of the necessary cyber security systems.

Cybercriminals quickly recognized the gap and Africa soon became an attractive target for cybercrime. Parallel to the development of internet services, cybercriminals are also developing their tools and methods. They use increasingly sophisticated procedures that cause significant financial damage to the population and businesses and also put more and more pressure on cybersecurity organizations.

At the same time, organized criminals and terrorist organizations have also recognized the potential of cybercrime and use the special knowledge of cybercriminals in their operations related to cryptocurrencies and the dark web. Organized criminals on the dark web typically engage in activities like trading with false identities, drug sales, human trafficking, organ trafficking, and child pornography. (Interpol, 2023, pp.3-4)

In this research, the author examined the correlation between the countries most affected by cybercrime on the African continent and their population's use of the dark web.

## The most typical cybercrimes on the continent

First of all, we need to clarify what is the cybercrime itself. According to Kaspersky (Kaspersky, 2019) cybercrime is an activity in which the target or the device is a computer or a computer network. Typically, cybercrime is committed by cyber criminals or hackers to make money. However, in some cases, the aim is to cause damage to computers or computer networks for some reason instead of making money. The motivation behind the profit-free attacks can be political, or personal.

The perpetrators are highly skilled individuals, or organizations but it is not a rarity when novice hackers or so-called script kiddies are behind the attacks.

According to the Interpol report on African Cyber Threat Assessment 2024, (Interpol, 2024, pp. 11-22) ransomware and digital extortion are on the rise in the continent. This phenomenon is characterized by the continuous evolution as cybercriminals hone on their business models and extortion techniques.

The most common attack vector for ransomware attacks are phishing emails.

## *Ransomware and digital extortion*

These two types of cyber threats have the heaviest financial impact and besides, they can disrupt or paralyze the critical infrastructures and essential services in the continent. According to Check Point on average (Check Point Research, 2023) 1 out of every 15 organizations in Africa experienced a ransomware attack attempt every week in the first quarter of 2023 while the global average is 1 out of 31 attack attempts. Even more worrying are attacks on critical infrastructure. Nearly half of the countries reported ransomware attacks against business actors, hospitals, internet service providers, and power grids.

These type of attacks in most cases require some kind of human activity. The most typical example of this is phishing emails or messages as the most common attack vectors.

## *Phishing emails*

A phishing campaign is when specially crafted emails or other types of communication messages are sent with the intention of tricking recipients into doing something that compromises their security.

These emails or messages can contain links to malicious sites, malware-infected attachments, or attackers ask the receiver to answer with confidential information.

We can distinguish two types of phishing campaigns. The first one is mass phishing in which there is no dedicated target. The attackers send emails or messages in bulk to many recipients with the content for many people so for the attackers, it is not important who swallows their bait.

Unlike mass phishing in the case of spear phishing the target is designated and the message is specially crafted to trick him into undermining the security of the organization he is working for.

## *Other infection vectors*

Besides phishing campaigns, other vectors are also common among African ransomware groups.

The groups with preference use poorly secured RDP (Remote Desktop) connections, fake web applications, fake mobile applications especially fake mobile bank applications and unsecured networks where the administrators failing regularly update and patch their systems.

## *Tactics of digital extortion*

Once the ransomware operators have gained access to the system they explore it and its vulnerabilities and elevate their privilege on the system. After that, they deploy the malware that encrypts the data on the target system. The next step is demanding ransom in exchange for restoring the encrypted data. To increase the pressure on the victim they

threaten by leaking the sensitive information. Another tactic is the disruption of reluctant victim's service to paralyze the target.

Some ransomware groups simply exfiltrate the sensitive data and threaten to leak it unless the victim pays a ransom. Victims tend to pay because the reputational damage poses a bigger risk for their business than paying a significant amount of money. The ransom payment can reach millions of dollars, but there is no guarantee for not leaking the stolen data. Exfiltration is a growing business because the stolen data can be sold many times. Ransomware and hacker groups are trading with this kind of data. They split it into smaller parts, repack them, and sell them many times.

## *Ransomware affiliate program*

Besides evolving ransomware techniques the ransomware groups elaborated a new „affiliate" program. They develop ransomware programs and platforms and offer their ransomware software as a service for others who pay them a part of their income comes from the ransom. The ransomware owners provide the software, the infrastructure, and the user manual for their „affiliates". This model has many advantages. The owners get more income than they would if they ran the software alone. They don't have to waste time for the target- related information collection, the malware deployment, and the contact with the victims. This model has many advantages. First of all, the owners stay behind the scenes. The owners get more income than they would if they ran the software alone. They don't have to waste time for the target-related information collection, and the malware installation. The spare time enables them to elaborate more sophisticated and more aggressive ransomware solutions. This affiliate program is known as ransomware- as- a- service (RAAS) program that is very common among cybercriminals. The core members of ransomware groups recruit professionals, pen-testers, cryptocurrency specialists, and software developers. Besides, they involve in their projects bulletproof hosting services and money laundering specialists just to name a few.

## *Online Scams*

In addition to ransomware, online scams are significant threats in Africa. An online scam is a fraudulent act carried out via the Internet or computer technology intending to steal money, personal or business information from people or organizations. Criminals achieve their aims by the use of a combination of malware components and social engineering techniques. Behind the epidemic-like spread of online scams across the continent is the explosive increase in digital technology. Africans spend significant time online communicating through social media, net banking, and gaming exposing themselves to cybercriminals seeking victims in the cyber realm. Estimating the real size of losses resulting from online scams is difficult. However, according to criminal professionals, all age groups and genders are involved. Any citizen or organization can be a victim, there is no exception.

African member countries reported different categories of online fraud to Interpol in 2023. These are the following in order of later discussion in detail:

- romance scams
- pig butchering
- mobile phone scams
- business email compromise (BEC)

## *Romance scams*

Romance scams has a variety of forms but they have a common feature. Criminals (often with fake identities) get in contact with the victims under the guise of fake romantic or intimate relationships for financial gain. The criminals use social media, messaging apps, or online dating sites and apps as communication platforms to approach their victims. The second phase involves building a trusted relationship by exploiting their vulnerabilities and weaknesses. The duration of this phase varies, depending on the victim. Once the scammers have succeeded, they start manipulating the victim to steal their money. Nowadays, the most common type of romance scam is catfishing. In this scheme, the perpetrator creates a fake online identity to deceive their victims. Generally, they steal profile pictures or complete accounts to make themselves more attractive and in addition to hide their real persona. After building the trusted relationship they come up with different wide variety of reasons to gain their sympathy, or support (sick close relatives, money to meet in person, etc.). This type of scam can be a hit-and-run action or a long-lasting process. After accomplishing their aims, they disappear leaving the victim both financially and emotionally ripped off.

## *Sextortion*

The modus operandi of this crime is similar to a romance scam but has some minor differences. After building the trusted relationship the scammer asks for intimate pictures from the victim. Once has succeeded, the perpetrator starts to blackmail the victim by threatening to publish the intimate pictures on social media. To increase the pressure on the victim the perpetrator in some cases publishes some samples and demands payment in exchange for taking the content down.

Another type of sextortion is when the perpetrator unlawfully gains access to the victim's hidden social media profile often by use of malware and blackmails the victim by publishing their private contents. Sometimes the hit-and-run blackmail turns into a recurring monthly payment. Undoubtedly romance scam has a huge financial impact on victims but the emotional impact is inestimable. These types of scams often result in continuous feelings of terror, psychological disorders, and suicide.

## *Pig butchering*

In a pig butchering scam, criminals contact targets out of the blue, gain their trust, and manipulate them into making phony investments. Once successful, the criminals disappear with the funds, leaving no trace behind. In the majority of instances, cryptocurrency is utilized in this kind of crime. According to Finra (Finra, n.d.) the scam has three stages:

## *1. A slow build*

A stranger gets in contact with the subject from the out of the blue. They have different explanations for why they contacted, such as having found their names on message lists, or social media. Of course, they use fake profiles and fake identities. Step by step they get closer and try to make friendship while they map the victim's personality. The duration of this stage varies, between days to months. Occasionally, they pretend to desire a romantic relationship. Until gain trust, they don't send investment-related messages.

## *2. Sharpening the knife*

The second phase has two goals. First, make the victim believe they will make money by following the „friend" advice and the second is to make sure of that the victim has enough capital to make a bigger investment.

The scammer makes the victim believe that he has a connection to a reputable financial institution from which he can receive confidential lucrative investment advice. To gain the victim's trust criminals can forge fake brokerage dashboards with attractive investment profits. Following this, the criminal surges the victim to make a smaller investment to ensure that the investment works. The victim makes his investment on the criminal's brokerage dashboard where he gets „profit" according to his user account balance. This trick usually dispels his suspicions.

## *3. The slaughter*

After having convinced the victims, criminals switch into high gear and urge victims to make a bigger investment or a series of investments. Once the victims do it they leave them with devastating losses and disappear without any trace or they express their sympathy over victims' losses and offer their help and suggest another investment to gain back the losses. But usually, it only helps them rip off the victims to their bones. When they succeed they disappear leaving no trace behind.

This relatively new type of crime affects especially Western and Southern African countries. (Interpol, 2024b, p. 5, 13, 14, 16) There is a close relationship between the increasing use of mobile bank services and the rise of smartphone scams across the continent.

The most common smartphone scams are mobile phishing and banking trojans.

The first one is a slightly modified version of a type of attack discussed previously, while the second involves malware like banking trojans. These are designed to steal sensitive financial information like banking credentials, account balances, and credit card data from infected phones. The trojans can be deployed through different vectors. The malware spread via phishing emails, fake applications, illegal or cracked software, etc. The trojan horses disguise themselves as legitimate program to gain access to the system. On top of that they act as remote access trojans (RATs) enabling the attacker to control the infected system. The malware can collect keystrokes, sensitive information, screenshot, some of them can control microphone, built-in cams, and eavesdrops the victim phone conversations.

In the last few years Africa witnessed the explosive growth of smartphones and in parallel to this increasing scams targeting smartphone users relying on their smartphones. The stakeholders of financial sectors and law enforcement agencies face big challenges due to this increasing scam wave across the continent.

## *Business Email Compromise (BEC)*

BEC is a type of cybercrime which involves different forms of email fraud to attack financial and business organizations or individuals. Cybercriminals compromise legitimate business or private email accounts by using social engineering and/or exploiting vulnerabilities and attempt to trick organizations or persons into completing funds transfers or divulging confidential or personal information.

According to Interpol report the BEC attacks are increasing both in their volumes and their impacts. BEC can result in loss of reputation and also have an emotional, and psychological impact on victims.

Mostly financial institutions and companies with active foreign business connections together with under-developed security controls are in the crosshairs of cyber criminals. The phishing emails were the attack vectors in 80 % of BEC in African countries in 2023. The reason for the popularity of phishing emails is their hard-to-detect feature. This type of email doesn't contain malicious links, malware, or attachments so they are not flagged as spam (Interpol, 2024a, p.23).

BEC can be classified into five categories:

1. Data theft: the criminal crafts a role-specific email (HR manager, or bookkeeper) to obtain personnel or TAX-related information. The stolen data can be used to launch further BEC attacks against the target.

2. Account or system breach: the attacker hacks an employee's or accountant's email account and from the compromised email to send requests for invoice payments to multiple partners, but the receiver bank account is controlled by the attacker.

3. CEO impersonation: after extensive reconnaissance of the targeted organization, the attackers impersonate high-level executives to initiate payment to an account under their control. This scheme of scam is also known as business executive scam.

4. Government, law enforcement or attorney impersonation: the attackers under the guise of officials such as TAX officers, government officials, or lawyers use various methods to put under pressure their targets to transfer funds to their accounts.

5. Bogus invoice: The attackers try to exploit the relationship between their target and its suppliers. Pretending to be one of the suppliers they issue a forged invoice or payment notice to targets asking them to transfer funds to their account.

BEC techniques are continuously evolving. The actors carry out extensive target-related reconnaissance by extensive use of all of the available OSINT tools and techniques. This reconnaissance involves social media and organization-related websites, events, conferences, financial information collection, and leaked databases both on the open and dark web. A new tendency the involve AI in the information collection phase.

## *Cyber espionage*

Cyber espionage (cyber spying) is a type of attack committed by malicious hackers against mostly governmental or significant business entities or universities and research & development centres to obtain information that provides attackers with advantages over the enemy or rival company (Gillis, 2023).

Cyber espionage often refers to a nation-state-launched attack with the aim to obtain political gain against the counterpart. In contrast, when the motive is financial gain the cyber-attack is economic espionage.

Of course, it goes without saying that the actors strive to remain undetected in the IT environment for as long as possible, making these types of attacks very complex.

The cyber espionage actors use the wide scale of attack vectors and tactics (Thomas, 2018). The most frequent are the following:

- Exploiting vulnerabilities in websites, web browsers
- Spear phishing emails designed to elevate the attacker's privileges
- Attack the supply chain including the closest partners
- Different malware, trojans, and worms
- Infection of commonly used third party software applications or free software components (libraries, header files)

According to the Africa Center for Studies as for the cyber espionage in the continent, China is the most concerning country (Africa Center for Strategic Studies, n.d.; Allen and van der Waag-Cowling .N, 2021).

Tilouine and Kadiri, the journalists from Le Monde (Tilouine and Kadiri, 2018) published an article on 26. January 2018 alleging that China had been spying on the African Union in the Chinese-built Center in Addis-Ababa, Ethiopia. It was claimed that the servers in the centre every night between midnight and 2 a.m. uploaded the new content to another server located in Shanghai. AU initially declined to comment on allegations but later changed its stance and declared that China doesn't spy on AU.

## *The most cybercrime-affected countries in Africa*

Africa is susceptible to new technologies due to its population of which more than 60 percent is under 25 years old. The key economic sectors such as finance, education, agriculture, security, and telecommunication are trying to leverage the advantages of online platforms.

However, the widespread use of new technologies together with the insufficient cybersecurity architecture, the lack of cyber hygiene, and inadequate legislation foster favourable soil for cybercriminals. At the same time, many African countries are facing with economic problems making it difficult to allocate resources for cybersecurity. Africa experienced a 23% increase in cyberattacks per organization per week in the second quarter of 2023 compared to the same period in 2022. Cyberattacks face governments, and businesses overwhelming challenges (Allen and van der Waag-Cowling. N, 2021). In Africa the insufficient cyber security infrastructure costs countries 10% of their GDP, which is a significant burden on their budgets. According to Interpol survey about 90 % of African businesses operate without cybersecurity protocols (Economic Commission for Africa, 2022).

## *The main targets of attackers*

According to Positive Technologies survey (Positive Technologies, 2023) as it can be seen in figure 1. The most targeted sectors of economy were: finance (18%), Telecom (12%), government (12%), and retail (12%).

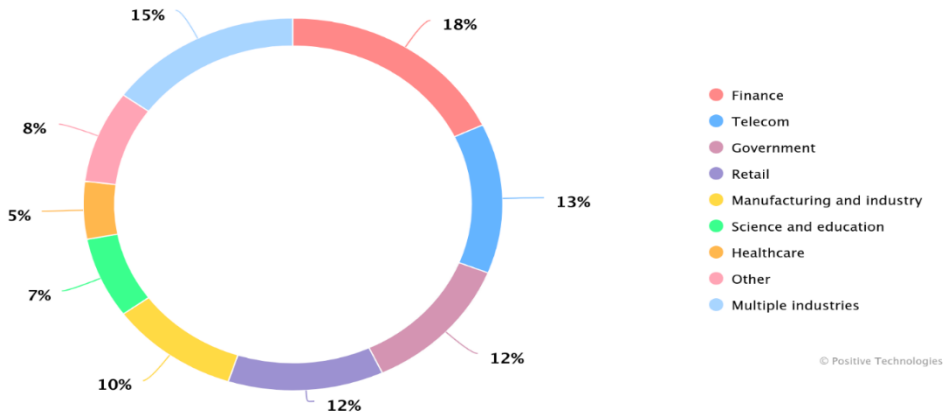


*Figure 1: Categories of victim organizations. Source: https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/.*

The targeted attacks accounted for 68% of successful attacks of which individual targeted attacks accounted for 15%. Among the targeted victims we can find the Flottenwave, TransUnion, Eskom, and government institutions like the Bank of Zambia, and ministries in Uganda, just to name a few.

## *Consequences of attacks*

Mostly, criminals obtained confidential information from companies (38%). Presumably, they multiple times can make money from this kind of information because it can be sold on markets and also can be used for further attacks. In some cases, the attacks can lead to functional disruption of the target organization (35%) while 7% of attacks cause direct financial losses. The consequences of attacks can be seen in the figure 2.

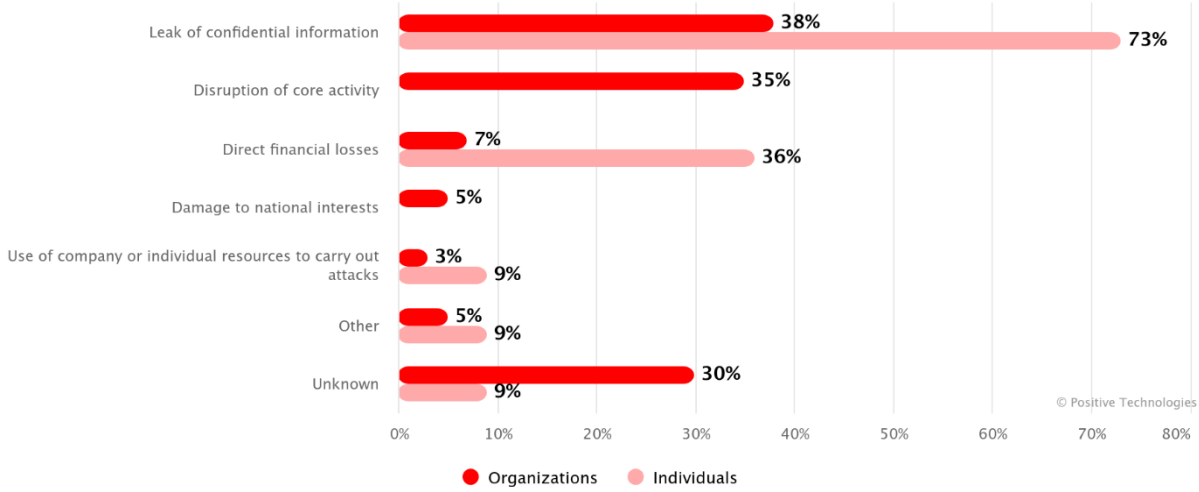


*Figure 2: Consequences of attacks (percentage of successful attacks). Source: https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/.*

The consequences of attacks may vary from minor damages (annoying incidents) to non-tolerable events. Non-tolerable events are events that are the results of cyberattacks and prevent the achieving the operational goals of the organization or have prolonged harmful effects on the organization's activity.

## *Finance sector*

The finance sector is the most favourable target of cybercriminals. First of all, they are interested in financial gain, and besides, this sector stores large amounts of customer data allowing attackers to plan further attacks against the customers (Positive Technologies, 2023).

The OPERA1ER group was responsible for 35 successful attacks between 2018 and 2022 in Africa. They attacked banks and telecom companies of which they managed to steal more than 30 million USD.

## *Telecommunications*

This sector is the second most attractive to cybercriminals in the continent. The reason is their huge dataset. They have customer payment information, and the customer's connections which can be sold and used for further attack planning last but not least, attackers can disrupt their operations and restore in exchange for ransom.

Criminals attacked the RSAWEB South African Internet service provider in February 2023, encrypted the company's database and demanded ransom in exchange for restoring the service leaving some customers without Internet access for several days.

## *Government institutions*

The reason why government institutions are in the crosshairs of cybercriminals is their significant functions and their databases on citizens. These two features make them ideal targets for cybercriminals to launch ransomware campaigns threatening service disruption and steal databases that also can be sold on markets and used for planning further attacks.

The BlackCat group (also known as the ALPHV group) attacked the African Union's computer network leaving paralyzed the headquarters and infecting 200 computers with malware. Luckily, the attack happened after ten days after the closure of the summit of the organization. The system restoration required the help of Interpol, Afripol, and African Bank.

## *Retail*

In the trade industry, the attackers focus on stealing customers' and partners' data, especially payment and personal data. Cybercriminals succeeded in stealing confidential data in 86% of successful attacks in the African continent.

Attacker in 2022 stole about 3, 7 million customer records from a pharmacy retailer company. The criminals accessed the data by compromising a third-party service provider's system. As researches show today common method is compromising one member of the supply chain's system to get into the target's network. Two-thirds of successful attacks started by compromising a trusted supply chain resulted in data leakage and 4 in every 10 attacks led to service disruption.

## *Manufacturing and industry*

Cybercriminals attack the industrial sector owing to their role in technological processes and their impact on entire industries and regions or even the whole country. The sector relies more and more on interconnected computer networks, robotization, and digitalization enabling attackers to find vulnerabilities, and security flaws.

Successful attacks can have even a country-wide effect. The attack on Ghana Grid Company Limited (GRIDCo) caused five days of country-wide outages earlier in 2021.

## *Dark web and cybercrime*

The Internet, or World Wide Web, can be divided into three different parts. The first part is the clear web or open web, which is accessible to everyone. Users can visit open websites using a simple browser without needing any special tools or authentication. These websites are free for all and are indexed by search engines to improve users' search experiences.

The second part is known as the deep web. It is accessible to everyone but requires authentication. Examples of deep websites are online bank accounts, personal medical records, or email accounts. These pages are not accessible to search engines. Both the clear web and the Deep Web are traceable, meaning site owners, visitors, and practically everyone who uses these can be tracked down by their IP addresses.

The third component is the dark web. It is a special domain that provides anonymity, geographical anonymity, and freedom from censorship to its users. Accessing the dark web requires special software solutions and, in some cases, above-average IT knowledge. Privacy-savvy users can feel safe on the dark web as it is free from IT giants, from surveillance, and from censorship.

At first sight, it seems that the dark web is a unitary part of the World Wide Web, but it is not. This domain is categorized into different segments based on the specific software solutions, as each creates its own segment. The most popular software packages are "The Onion Router" (TOR), the "Invisible to the Internet" (I2P), and the "Freenet".

Beyond question, the TOR is the most popular solution. Besides the wide range of TOR services, it is easy to install, and use. It has an extra function compared to other solutions because it enables access to open websites with the full scale of anonymity.

This study will only cover TOR-related dark web content due to space limitations. Additionally, the TOR system is the primary choice for cybercriminals, while the other solutions have no significant role in cybercrime.

## *TOR*

The Onion Router (TOR) is an overlay network protocol implemented as an open-source software solution that operates on a worldwide decentralized network run by volunteers. It offers users anonymity, geographic anonymity, and censorship-free communication by using encrypted layers over network connections. The system routes the information through multiple routers in multi-layered encrypted packages, preventing observers from eavesdropping on the communication and revealing the identity and location of participants. The layers of encryption resemble an onion that is where its name comes from, and its top-level domains end with „. onion". (As for how TOR works please refer to my previous articles.).

The common opinion is that the TOR domain within the dark web is something diabolical dark place where drug dealers, pedophiles, money counterfeiters, fraudsters, and cybercriminals are playing their cruel games. For most people, the TOR is synonymous with crime. Unfortunately, it is partly true, however TOR has a white side as well, but it is not so interesting to get on headlines. Originally, the Tor system was designed to provide freedom of speech, and censorship-free communication for political dissidents, human rights activists, and believers persecuted for their religion.

Regrettably, privacy-focused features and the spread of cryptocurrency were precisely those circumstances that made this system attractive to criminals.

Next, let's shed some light on dark web-related crimes.

What crimes are typical on the dark web?
On dark web there are typical crime categories that are the following:

- illegal trading in all kinds of narcotics, drugs
- illegal trading in arms
- illegal trading in financial instruments
- illegal trading in stolen data
- cybercrime related software and knowledge trading
- child porn- related crimes

The first five types of crimes are typically conducted in dark marketplaces, but there are topic-dedicated sites as well.

Dark web markets are commercial websites on dark web that operate mainly on TOR system. They sell or broker typically illicit goods such as narcotics, drugs, weapons, counterfeit documents, currencies, stolen credit cards and payment information, stolen (leaked information), forged documents, stolen goods, hacking services, migrant routes, human organs, cyber-arms, malware, just to name a few.

To ensure secure transactions, sellers and buyers can utilize cryptocurrencies in combination with escrow services. On markets' websites, the goods are grouped by searchable categories. Vendors have a reputation rating system where the buyers can rate both the vendor and their services.

The way dark markets operate is ideal for vendors allowing them to reach a broader customer base and hide their activity from law enforcement agencies.

Usually, dark markets don't require any special authentication from the buyers to enter their sites, more over their offer can be checked without any registration, only buying can be tied to registration. At the same time, they are keen on their reputation so they remove the scammer, or fraudster vendors from their sites.

The child pornography-related crime is an exception in this aspect because even the dark web market owners exclude such kind of activity from their markets.

Dark markets often have partner forums where the users can receive market-related „good to know" information, and exchange experiences concerning the services

available on the market. Such forums don't have an e-commerce function they were established only for knowledge and experience sharing.

Independent forums (specialized shops) are for wisdom-sharing, and some of them have an e-commerce function. These forums pose a more significant threat because the partners and the details of the transactions are less traceable than in dark markets. Such forums are topic-specific, which means they are only dedicated to one category such as hacking, cybercrime, stolen information trading, arms trading, etc.

In contrast with the simple dark markets entering such forums is tied to the offer of a reference person or registration fee. On top of that, the hard-core forums require evidence from the applicants that proves their skills. Applicants are supposed to commit topic-related crimes such as intrusion into websites or web services.

Cybercrime or cyber security related forum members have access to vulnerabilities, tactics, techniques, procedures, zero-day exploits, tutorials, experiences, malware, etc. Some of the offers are free while others are paid services. Besides they can find partners (accomplices) for further actions. Membership of such forums can be very useful for cyber security experts.

The specialized shops or forums serve more sophisticated, more targeted, and higher-priced cybercriminal data and products, and their offers are for the experienced cybercrime buyers.

## *Cybercrime related pricelist*

The Flashpoint private intelligence company surveyed prices of stolen data (Flashpoint, 2020), exploit kits, and ransomware-as-a-services on dark markets on the dark web in 2020. The report contains aggregated pricing information for a wide range of dark web data and service types found on criminal marketplaces.

In this paper, the author will only present an extraction from the report concerning cybercrime-related prices to highlight how easy and cheap to buy tools, techniques, and procedures for a successful campaign on the dark web.

Exploit Kits: phishing, ransomware, and others

| Item | Price (USD) |
|---|---|
| Ransomware exploit kit | $9 |
| Legacy ransomware, bundle of 9 types | $12 |
| Tailored phishing page with tutorial | $35 |
| Office365 exploit kit | $125 |

*Figure 3: Pricing of exploit kits. Source: Flashpoint pricing analysis, 2020.*

## *1. RDP server access*

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft to allow system administrators to remotely connect to other corporate machines and

servers. This connection is used for tasks such as pushing updates, performing maintenance, and facilitating help desk support. RDP clients and RDP server software are available for most common operating systems, including Windows, Linux, Unix, Mac OS X, iOS, and Android.

RDP is also a popular target for cybercriminals who exploit RDP access to carry out various attacks, including account takeover attacks, carding, payment fraud, and conducting reconnaissance. The use of RDP is increasing in popularity within the cybercriminal ecosystem.

| Item | Price (USD) |
|---|---|
| RDP with global admin access | $10 |
| RDP, country-specific | $26 |
| Hacked RDP | $35 |
| Bank drop RDP via PayPal | $575 |

*Figure 4: RDP server access. Source: Flashpoint pricing analysis, 2020.*

## 2. Bank logs and routing numbers

Access to online bank accounts, also known as "bank logs", is a popular dark web product and is priced accordingly. The price of bank accounts on dark markets depends on the balance available and the institution from which it originates.

| Item | Price (USD) |
|---|---|
| US bank log - $100 USD balance | $25 |
| US bank log - $4,000 USD balance | $55 |
| US bank drop (account number, routing number, linked accounts) | $530 |
| UK bank log - £3,000 GBP balance | $50 |
| Germany bank log - €3,500 EUR balance | $300 |
| Japan bank log - ¥400,000 JPY balance | $350 |

*Figure 5: Bank Logs and Routing Numbers. Source: Flashpoint pricing analysis, 2020.*

## 3. Fullz (i.e., All-in-One Packages)

Fullz" is slang for a full package of personal information that is comprehensive enough for cybercriminals to impersonate the victim and profit off of identity fraud schemes. Personal information contains name, social security number, date of birth, account specific credential data. Personal information with financial data is more expensive while the price of a typical data package ranges from 4 to 10 USD.

| Item | Price (USD) |
|---|---|
| US fullz identity data (incl SSN and DOB) | $125 |
| UK fullz identity data | $50 |
| EU fullz identity data | $25 |
| Japan fullz identity data | $45 |

*Figure 6: "Fullz" pricing. Source: Flashpoint pricing analysis, 2020.*

The Flashpoint report gave us a glimpse of cybercrime-related dark web business showing that such type campaign doesn't require significant investment to acquire the software solutions. In light of this, it becomes understandable what is the reason for the explosive spread of cybercrime.

## *Correspondence between country crime index and the number of TOR users in Africa*

Author assumes there is a correspondence between the country crime index (especially cybercrime) and the number of TOR users in African countries.

In the comparison, the following data sources were used: statistical data on population and internet users per country (Worldometers, Statista), Global Cyber Safety Index (GCSI), Global Cybercrime Index (GCI), and European Union-funded Organized Crime Index (OCI).

A researcher can access a wide range of usage data of the TOR ecosystem by visiting the TOR metrics site (https://metrics.torproject.org). The service collects data from the TOR network and provides archive historical data preserving the users' privacy. TOR metrics includes data on users, servers, traffic, bridges, onion services, etc. In this paper, we analyse user-related data to determine the number of users connecting to the network in each African country.

TOR metrics gave us statistics on 45 countries of the 54 African countries. The author collected the number of TOR users per country into a database between 02.15.2024 and 05.15.2024. During this period the user number varied between 5 and 7900. Most users were from South Africa, totalling 7500, while the smallest number came from Eritrea, totalling 5. The average number of users is 1093, and the median number of users is 426.

The OCI ranks countries based on the frequency of occurrence of different types of crime. In this study, the African countries were investigated based on the frequency of cyber-dependent crimes (The Organized Crime Index, 2024).

To prove or refute the hypothesis concerning correspondence between the number of TOR users and the frequency of occurrence of cyber-dependent per country the number of TOR users and the ranking of cybercrime-dependent countries' rank list in Africa were compared.

The author examined the countries ranked below ten in the list of the most cyber-dependent affected countries. Due to identical rankings, 16 countries with an index below 10 are highlighted. Following rank 8, the subsequent rank is 18, resulting in the absence of ranks 9 and 10. To provide users with a clearer perspective, table 6 includes the number of Internet users per country and the proportion of TOR users in relation to Internet users per country.

Taking a closer look at the number of TOR users, we can determine that the average number of users is 1117, but a more realistic number is obtained if we consider the median number of users, which is 443. Comparing the cybercrime –dependent rank and

the median of TOR users we can conclude that there is a correspondence with the number of TOR users. There is three exception Burkina Faso Botswana and Mali.

| | Country | Population | Internet Users | TOR Users | TOR per Internet Users | Cyber-Crime Rank in Africa |
|---|---|---|---|---|---|---|
| 1. | Kenya | 55100586 | 22481039 | 3634 | 0,0162% | 1 |
| 2. | Nigeria | 223804632 | 101831108 | 2650 | 0,0026% | 1 |
| 3. | South Africa | 60414495 | 45129628 | 7900 | 0,0175% | 3 |
| 4. | Uganda | 49933884 | 13482149 | 815 | 0,0060% | 4 |
| 5. | Ghana | 34121985 | 23817146 | 1772 | 0,0074% | 4 |
| 6. | Burkina Faso | 23251485 | 4627046 | 253 | 0,0055% | 6 |
| 7. | Cote D'Ivoire | 29608534 | 11369677 | 896 | 0,0079% | 6 |
| 8. | Angola | 36684202 | 14416891 | 904 | 0,0063% | 8 |
| 9. | Tanzania | 67438106 | 21512756 | 1045 | 0,0049% | 8 |
| 10. | Togo | 9262347 | 3482642 | 463 | 0,0133% | 8 |
| 11. | Senegal | 17763163 | 10657898 | 1365 | 0,0128% | 8 |
| 12. | Cameroon | 28647293 | 12576162 | 642 | 0,0051% | 8 |
| 13. | Botswana | 2675352 | 2068047 | 357 | 0,0173% | 8 |
| 14. | Ethiopia | 126527060 | 24546250 | 2348 | 0,0096% | 8 |
| 15. | Namibia | 2604172 | 1619795 | 460 | 0,0284% | 8 |
| 16. | Mali | 23293698 | 7710214 | 151 | 0,0020% | 8 |

*Figure 7: OCI cybercrime rank in Africa (2023) and the number of Tor users in Africa between 02.15.2024-05.15.2024. Source: TOR metrics, Worldometers, Statista, and European Union-funded Organized Crime Index, composed by the author.*

Concerning Burkina Faso, according to the OCI report foreign hackers from China, Indonesia, Albania, and Sudan are responsible for the high-ranking in the list in question. As for Botswana, the number of TOR users is below the median, but the proportion of TOR users is equal to that of South Africa.

Taking the third country, the OCI report paints an incomplete picture of Mali's cybercrime situation because it only reports rising of ransomware, and viruses resulting in data breaches.

To make it easier to understand, the data in the table have also been represented on Figure 8.

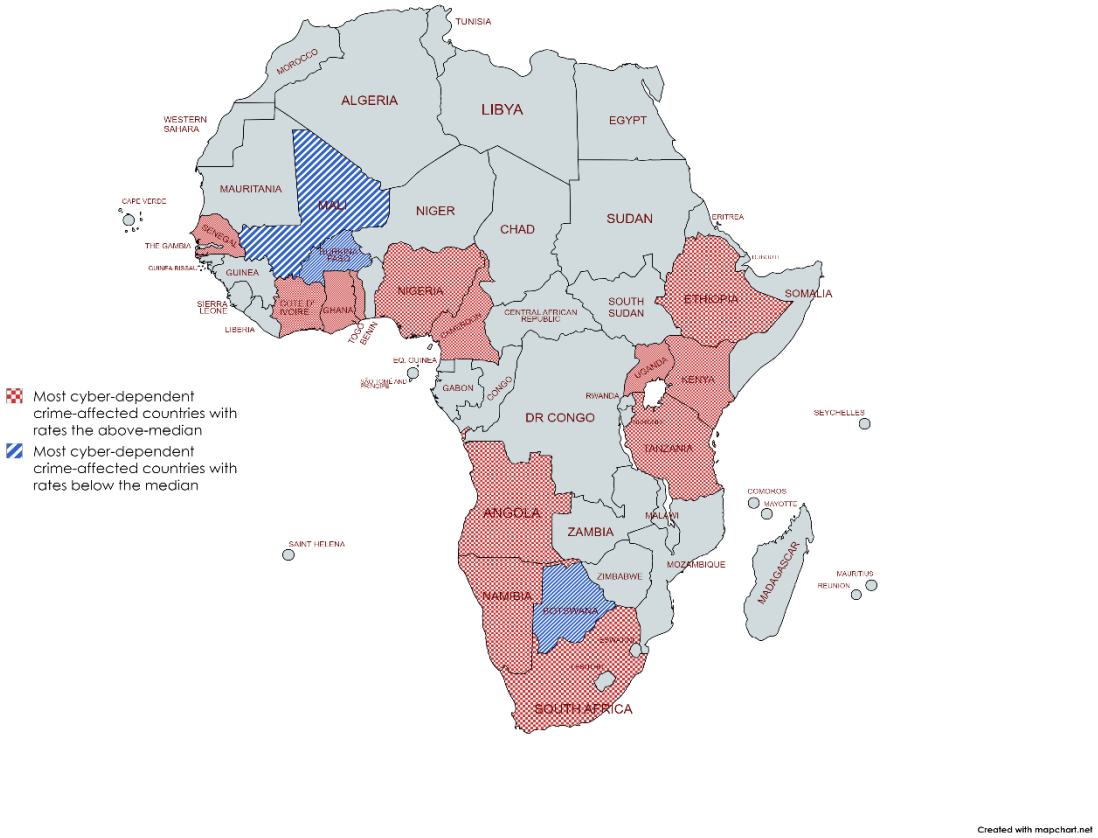


*Figure 8: Most cyber-dependent crime affected countries in Africa and their dark web usage.*

As a counter test, let's see where to locate the countries with the lowest number of Tor users in the African Cyber-dependent crime rank list that Figure 9. shows.

| | Country | Population | Internet Users | TOR Users | TOR per Internet Users | Cyber-Crime Rank in Africa |
|---|---|---|---|---|---|---|
| **1.** | Eritrea | 3748901 | 997208 | 5 | 0,0005% | 45 |
| **2.** | Central African Republic | 5742315 | 608685 | 9 | 0,0015% | 40 |
| **3.** | Guinea-Bissau | 2150842 | 679666 | 28 | 0,0041% | 40 |
| **4.** | Chad | 18278568 | 4112678 | 39 | 0,0009% | 29 |
| **5.** | Equatorial Guinea | 1714671 | 1145400 | 41 | 0,0036% | 45 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **6.** | Liberia | 5418377 | 1630931 | 49 | 0,0030% | 18 |
| **7.** | South Sudan | 11088796 | 1341744 | 51 | 0,0038% | 51 |
| **8.** | Leshoto | 29608534 | 13916011 | 54 | 0,0004% | 51 |
| **9.** | Niger | 27202843 | 4597280 | 68 | 0,0015% | 51 |
| **10.** | Sierra Leone | 8791092 | 2672492 | 75 | 0,0028% | 45 |
| **11.** | Gambia | 2773168 | 1503057 | 140 | 0,0093% | 29 |
| **12.** | Sudan | 48109006 | 13807285 | 141 | 0,0010% | 32 |
| **13.** | Guinea | 14190612 | 4810617 | 145 | 0,0030% | 40 |
| **14.** | Republic of the Congo | 6106869 | 1661068 | 150 | 0,0090% | 32 |

*Figure 9: Lowest number of TOR users and their ranks in African cyber-dependent list. Source: Composed by author.*

It seems, that the comparison of the two datasets based on the collected data confirms my hypothesis that there is a correspondence between the number of TOR users and the OCI cyber-dependent crime rank list.

## *Summary*

We are witnessing a rise in cybercrime worldwide, and the African continent is no exception to this trend. With the advent and spread of new technologies, new types of crimes emerged and what is more criminals have found new ways to commit old crimes. Cybersecurity has not kept up with technological advances, leaving a void for cybercriminals to fill.

Cybercrimes primarily affect the financial, industrial, and commercial sectors, but at the same time, all social strata are exposed to the threat of cybercriminals.

Computer-dependent crimes have a significant impact on national economies, causing damages exceeding 10% of the countries' GDP.

This paper presented the most typical cybercrimes and the possible connections between them and the dark web markets and dedicated websites. The importance of the dark web is unquestionable for cybercrimes because this domain hosts those markets, dedicated webpages, and forums where a significant part of criminals and future criminals can acquire the knowledge, tools, and techniques that are needed to commit cybercrimes. The Flashpoint's report gave us an insight how simple and cheap for cyber criminals to access tools, knowledge, and information.

The author hypothesized that based on its role in cybercrime, there is a correspondence between dark web usage in African countries and their cybercrime index. It seems that the analysis of collected data proved that the proportion of dark web usage correlates with the OCI cybercrime–dependent country index in Africa. The counter-test proved that countries with low-level dark web usage have a low rank in the cyber-dependent crime list.

Summing up, the hypothesis can be considered confirmed.

Africa is not only involved in cybercrime on the dark web. A search in the TOR system yielded a significant number of results specific to Africa. These results led to various illicit activities such as narcotics markets, illegal trading of flora and fauna, as well as sites involved in arms and human trafficking, among others. It's important to note that the research did not explore the connection between dark web usage and the aforementioned crimes.

This may be the subject of further research.

## *Conflict of Interest*

The author hereby declare that no competing financial interest exists for this manuscript.

## *Notes on Contributors*

Attila Gulyás ret. Lt. Colonel graduated from the Kossuth Lajos Military College as an infantry officer in 1988. After serving four years as a troop officer, he was transferred to the Military Security Office, where he served in different positions. He retired from the service as a head of a department and in the rank of Lieutenant Colonel in 2010. He has been interested in IT for a quarter-century. His hobby is computer programming (VB.net, Visual C++, and Python) and computer forensics on personal computers on MS Windows and Linux operating systems. He is a doctoral student at the Óbuda University, Doctoral School on Safety and Security Sciences, researching the connection between terrorism and the Dark Web. His research subject is terrorist activity in cyberspace: from social media to the Dark Web.

References

Africa Center for Strategic Studies. (n.d.). *Understanding Africa's Emerging Cyber Threats*. Retrieved June 20, 2024 from https://africacenter.org/programs/cyber/

Allen, N. (2021). *Africa's Evolving Cyber Threats*. Africa Center for Strategic Studies. Retrieved July 7, 2024 from https://africacenter.org/spotlight/africa-evolving-cyber-threats

Allen, N., & van der Waag-Cowling, N. (2021). *How African states can tackle state-backed cyber threats*. Brookings. Retrieved June 23, 2024 from https://www.brookings.edu/articles/how-african-states-can-tackle-state-backed-cyber-threats/

Check Point Research. (2023). *Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most*. Retrieved June 2021, 2024 from https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

Economic Commission for Africa. (2022). *ECA launches the Guideline for a Model Law on Cybersecurity during the 17th IGF*. United Nations Economic Commission for Africa. Retrieved June 14, 2023 from https://www.uneca.org/stories/eca-launches-the-guideline-for-a-model-law-on-cybersecurity-during-the-17th-igf

Finra. (n.d.). *Pig Butchering' Scams: What They Are and How to Avoid Them*. Retrieved June 19, 2024 from https://www.finra.org/investors/insights/pig-butchering-scams

Flashpoint. (2020). *Dark Web Marketplaces 2020*. Flashpoint-Intel. Retrieved December 12, 2024 from https://flashpoint.io/resources/research/flashpoint-pricing-analysis-dark-web-marketplaces-2020/

Gillis, A. (2023). *What is Cyber Espionage? How to Protect Against It*. Search Securit. Retrieved June 15, 2024 from https://www.techtarget.com/searchsecurity/definition/cyber-espionage

Interpol. (2023). *African Cyberthreat Assessment Report Cyberthreat Trends* file:///C:/Users/bened/Downloads/2023_03%20CYBER_African%20Cyberthreat%20Assessment%20Report%202022_EN.pdf

Interpol. (2024a). *Interpol African Cyberthreat Assessment Report 2024* file:///C:/Users/bened/Downloads/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

Interpol. (2024b). *Interpol Global Financial Fraud Assessment* file:///C:/Users/bened/Downloads/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03%20v2.pdf

Kaspersky. (2019). *Tips on How to Protect Yourself against Cybercrime*. Retrieved June 10, 2024 from https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Positive Technologies. (2023). *Cybersecurity threatscape of African countries 2022–2023.* Retrieved June 15, 2024 from https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023

The Organized Crime Index. (2024). *Countries with the Highest Cyber-dependent crimes rate in Africa - The Organized Crime Index*. Retrieved June 30, 2024 from https://africa.ocindex.net/rankings/cyber-dependent_crimes?f=rankings&view=List&group=Country&order=DESC&region=&criminality-range=0%2C10&state-range=0%2C10