OSINT: LEADING THE INVESTIGATION REVOLUTION IN A NEW AGE OF DIGITAL CRIME

SOCIAL LINKS

INTRODUCTION

SOCIAL LINKS

A SOCIAL LINKS STUDY

This analytical paper has been put together by Social Links, a leading provider of OSINT software.

Our products service the needs of multiple national security organizations from around the world. These include 35+ police services, 15+ defense ministries, 10+ ministries of internal affairs, and 105 law enforcement agencies.

WHAT IS OSINT?

An acronym standing for 'open-source intelligence', **OSINT refers to the extraction and analysis of open-data—information which is in the public domain and legally accessible to all.** While the name evokes espionage, the publicly open nature of its sources gives OSINT broader and less secretive modes of application, setting it apart from what we might think of as traditional intelligence.

Although open-source intelligence has now spilled over to commercial sectors, where it is leveraged in various ways, its importance for law enforcement agencies (LEAs) and intelligence bureaus has become ever more profound. **With 80-90%** of crucial modern intelligence data rumoured to come from open sources, **OSINT is now a cornerstone of modern reconnaissance and investigation processes.**

A CONCISE HISTORY OF OSINT

The use of OSINT to inform military decision-making emerged during WWII when the US government began amassing intelligence on their adversaries through fastidiously studying newspapers, magazines, radio broadcasts, photos and other media, in an attempt to discern enemy strategies and objectives.

This practice was referred to as Research and Analysis, and the department which carried out such operations formed a branch of the Office of Strategic Services (OSS)—later to be known as the CIA.

In the advent of the internet and the colossal rise of social media, OSINT took on a new meaning and nature. The sheer profusion of open data that became available for analysis transformed OSINT from a little-known reconnaissance method into a full-blown international industry spanning both public and private sectors.

INTRODUCTION

CRIME IN THE DIGITAL AGE

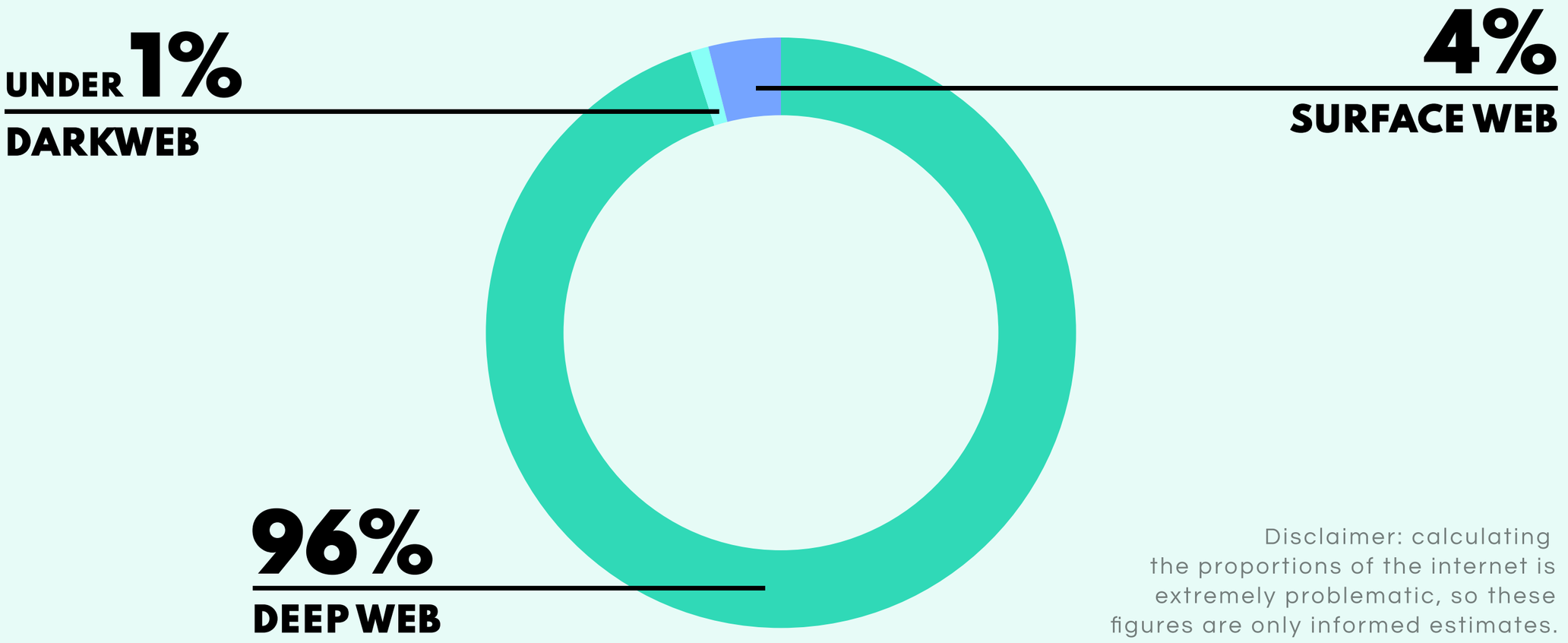
With so many aspects of human interaction having migrated to the online realm, criminal activity has also become proportionally digitized. Whether it's for illicit trade, radicalization, fraud, money laundering or theft, modern criminal actors are inevitably interfacing with the internet to achieve their ends.

In many ways, the data trails and traces connected to crime provide a range of opportunities for investigation units, but there is an inherent sticking point as well. The digital environment is so vast and complicated that traditional reconnaissance techniques are chronically ineffective when transposed to the online sphere.

If ill-equipped, analysts face unmanageable challenges in trying to conduct digital investigations. The Surface Web alone is host to more than 1.9 billion websites, not to mention the multitude of social media profiles. And, **according to estimates**, that only amounts to 4% of the internet's data, with the Deep Web accounting for the remaining 96%. The Dark Web is only a small fraction of the whole—well under 1%.

Meanwhile, internet crime is skyrocketing. The FBI has reported that in 2021 alone, people lost about $7B through ransomware, scams, and extortion, with over 6.5M crime reports recorded by the bureau overall. Furthermore, **according to Statista**, the global cost of cybercrime increased by just under a factor of 10 between 2016 and 2021, from $0.61T to $5.99, and is forecast to exceed $20T by 2026.

INTERNET DOMAINS BY PROPORTION (ESTIMATED)



Disclaimer: calculating the proportions of the internet is extremely problematic, so these figures are only informed estimates.

However, **open data is proving to be highly effective in closing criminal cases and providing evidence**. For instance, the exercise tracking app Strava can provide geopositioning data in real time, allowing analysts to reconstruct the location, movement, and timelines of a given subject.

This is just one example from a wide gamut of OSINT techniques at an investigator's disposal, whereby analysts can build a comprehensive picture of a person of interest, so that criminal activity can be identified, or even anticipated. Such techniques allow analysts to study a subject's objectives and tactics, as well as establish the their wider contextual network.

But, this is a complex process for which specialized tools are absolutely essential. With criminals employing increasingly sophisticated techniques and the Dark Web to retain anonymity and cover their tracks, only advanced technologies can zero in on the necessary information.

In addressing a range of challenges, open-source intelligence has become a widespread and versatile player in the law enforcement sector, being used in the fight against all kinds of illicit activity including fraud, money-laundering, illegal trade, extremism, and many other criminal cases besides.

INTRODUCTION

AREAS OF FOCUS

Alongside the far-reaching possibilities that the law enforcement sector has gained through the digital revolution, it has also inherited some complex challenges. For the purposes of this whitepaper, we have grouped the foremost issues into three overarching topics:

CYBERCRIME AND DIGITAL FORENSICS

The rapid evolution of the internet has largely been driven by the vast social and commercial opportunities it has provided its users. A major upshot of all this has been a large-scale transition of personal and professional life into cyberspace. And this, in turn, has given criminals an expansive new playing field to operate in, combining both the physical and the digital realms.

THE MISUSE OF SOCIAL MEDIA

In many ways, social media has been embraced as a digital surrogate for interpersonal life. But beyond this, it can have a hugely formative impact on the way people see the world. Whatsmore, the news, adverts, and political sentiment that circulates in someone's digital environment can be cynically manipulated, giving power to fraudsters, extremists, and bullies of various kinds.

ANONYMIZATION AND THE DIGITAL UNDERGROUND

For every advanced, new method or tool that LEAs adopt to trace lawbreakers and their activities, the criminals develop a more sophisticated form of anonymization to elude tracking. The chase is a constant battle of wits. Some of the most popular instruments currently in use are cryptocurrencies, and anonymization tools —such as the TOR browser—which are employed when using the Dark Web.

CYBERCRIME AND DIGITAL FORENSICS

THE CORONAVIRUS PANDEMIC: A CYBERCRIME CATALYST

The outbreak of the COVID-19 pandemic triggered an unprecedented migration from office-based to remote work. And for most organizations, this was an operational necessity. But with IT departments struggling to adapt to the new reality, the scale and nature of the shift opened the floodgates for all manner of security breaches.

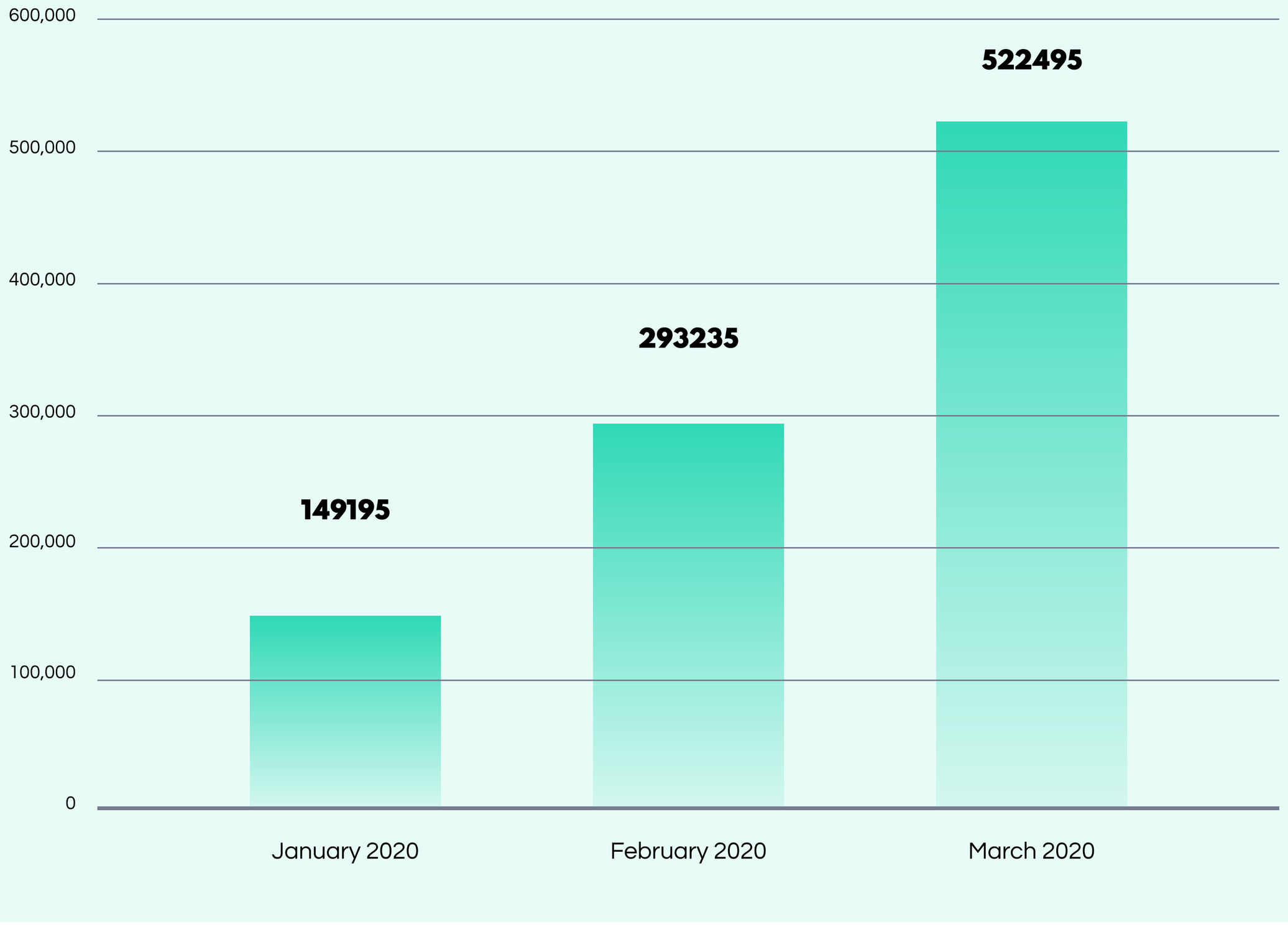
Where once were secure networks, set up and monitored by IT teams, there was suddenly a jumble of different routers and networks, each manned by a non-specialist remote worker. Furthermore, collaboration tools and conferencing platforms brought another layer of vulnerability, with even established companies such as Microsoft and Zoom hard pushed to patch up all the bugs allowing opportunities for infiltration.

On top of this, there has been the adoption of home equipment. According to a **study by Kaspersky**, 80% of remote workers accessed their corporate IT infrastructure via their personal computers even though the majority had been provided with a company alternative. With home internet usage often including torrent downloads and content streaming from unreliable sites, the increased susceptibilities to cyber threats have been clear.

A remarkable spike in the generation of malicious sites reflected these spiraling cybersecurity dynamics. In the first three months of the pandemic, Google **registered a 250% rise** in the number of phishing sites, as scammers and hackers of every kind sought to capitalize on the new situation that was shaking the stability of global cybersecurity.

NUMBER OF MALICIOUS SITES DURING THE FIRST 3 MONTHS OF THE PANDEMIC

Source: Google



CYBERCRIME AND DIGITAL FORENSICS

DIGITAL FORENSICS: AN OVERVIEW

There has long a been strong interconnection between offline actions and their counterparts in cyberspace. Forensics has therefore been at work in the digital realm for **well over 20 years**, with the International Organization on Computer Evidence founded in 1995, followed by the FBI's Regional Computer Forensic Laboratory in 2000.

Typically, the majority of digital forensic work has been carried out by centralized departments. However, such units have become increasingly **overwhelmed** by the huge amount of incoming tasks. This observation is also consistent with the **report** that digital evidence now plays a role in more than 90% of criminal investigations.

The central objective of digital forensics is to provide law enforcement with the insights and evidence needed to successfully proceed with a criminal investigation. However, the sources of data that feed into this process are many, varied, and vast. In such a climate, forensic analysts require a modern, inclusive approach towards the inspection of digital information.

THE CHALLENGES OF DIGITAL FORENSICS

THE LIMITED SCOPE OF 'TRADITIONAL' FORENSICS

The way people manage their data is seeing a paradigmatic shift. While some private data is still stored on premises as 'hard' copies, or offline backups, the vast majority resides on the cloud. With so much information sitting on a server somewhere as opposed to people's hard drives, offline data extracted from devices may only represent the tip of the iceberg.

INSUFFICIENT DATA RELIABILITY

Extracted data has to be proven reliable and comprehensible if it is to be accepted in court. Sometimes, it can be extremely difficult to present data as a coherent and unified picture of a subject's actions. Furthermore, in order to validate hypotheses, investigators often need to cross-check data via multiple sources—isolated fragments are frequently insufficient.

DATA OVERLOAD

With masses of data stored both online and on hardware devices, analysts can no longer filter and study it manually. The gathering process is complex, involving the identification, collection, and organization of vast reams of information. This then needs to be thoroughly filtered and subtly analyzed to deliver actionable intelligence.

LENGTHY PROCEDURES AND TIME CONSTRAINTS

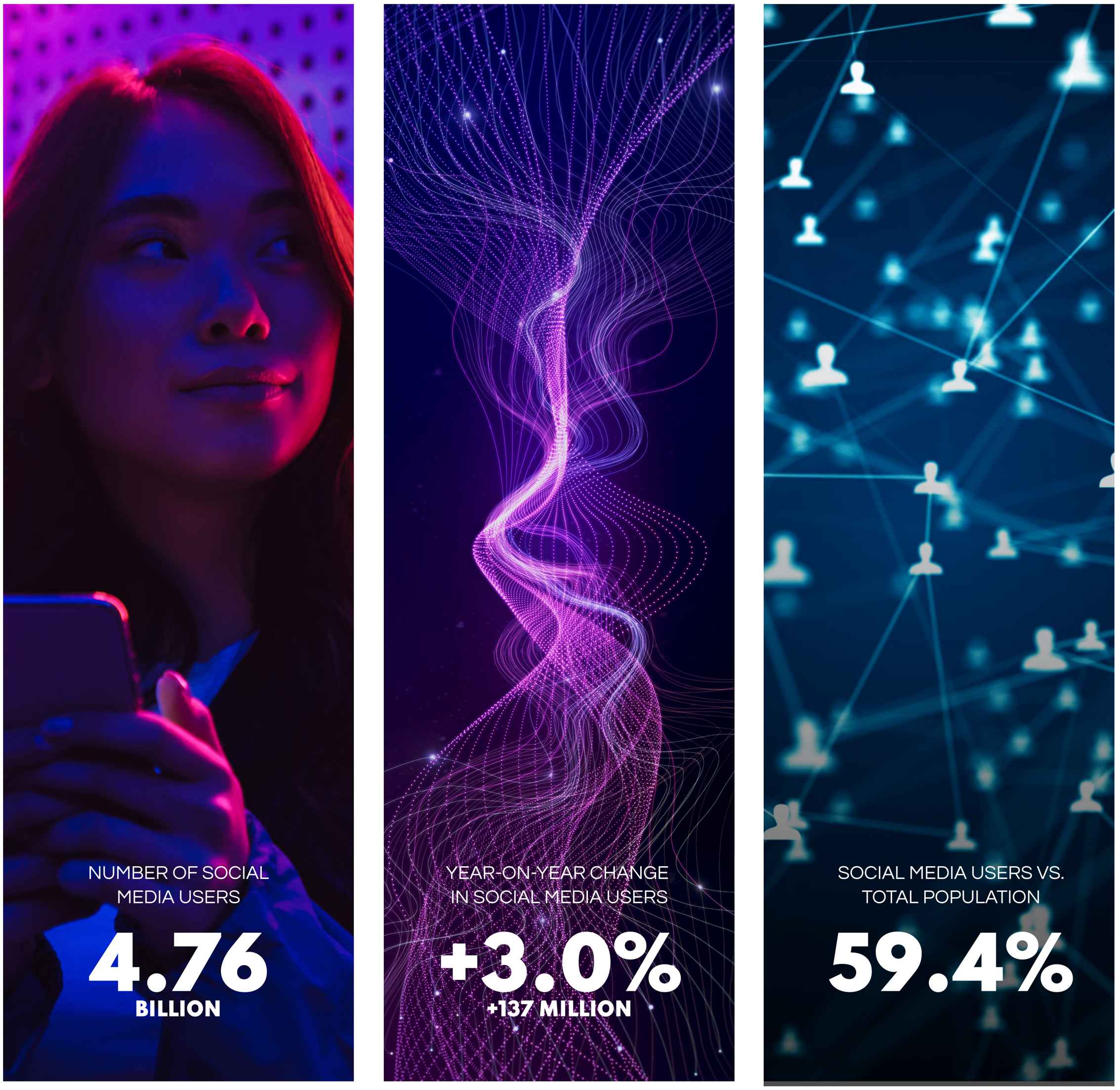
A full-cycle forensics study takes more time to conduct than investigators have at their disposal. Consequently, detectives become uninclined to turn to digital forensics experts, knowing that it could cause a bottleneck in the investigation process and seriously hamper the progress of the entire case.

THE MISUSE OF SOCIAL MEDIA

NETWORKING PLATFORMS: A CYBERCRIME PLAYING FIELD

The restrictions accompanying the COVID-19 pandemic gave a significant impetus to the adoption of social media for communication, and it has now become a truly dominant global phenomenon. There are currently 4.74B social media users around the world, with Facebook accounting for more than half of these.

Remarkably, this amounts to 59.3% of the entire global population. And with 137M users signing up every year—or 4 every second—social media enjoys an **annual growth rate of 4.2%**.



THE MISUSE OF SOCIAL MEDIA

NETWORKING PLATFORMS: A CYBERCRIME PLAYING FIELD

Of course, such an immense pool of human activity is bound to have some negative aspects. While social media allows friends and family to stay in touch, it can also be used for a range of more nefarious purposes. Many people engage with social media without really understanding the amount of sensitive data they are making public, and which can lead to many kinds of data breaches and compromises.

At the same time, the open channels of communication that social networks allow also make them a hotbed for scams and disinformation campaigns. A plethora of illicit activities take place on social media. Some of the most common include:

IMPERSONATION

Posing as someone else by creating a fake profile. Such puppet accounts can be used to defraud or conduct slur campaigns against individuals and companies.

SEVERITY: 1

ONLINE HARASSMENT

Stalking, bullying, verbal abuse, and threats are all forms, and can cause severe emotional distress to those on the receiving end.

SEVERITY: 3

ASTROTURFING

Fake grassroots online activity, aimed at influencing lawmakers, politicians, or social groups, which can lead to civil unrest.

SEVERITY: 2

FAKE NEWS DISSEMINATION

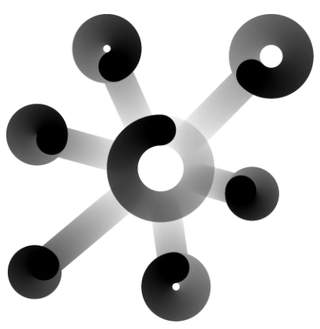
The manual or automated distribution of disinformation, aimed at influencing public opinion or sentiment.

SEVERITY: 1

SCAMMING

Scams are designed to defraud people through various ploys such as fake investment deals, job offers, romance, etc.

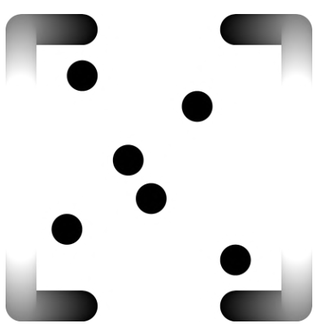
SEVERITY: 2



RADICALIZATION

Increasing acceptance of adopting undemocratic or violent means in attempting to bring about a political or ideological objective.

SEVERITY: 5



VIOLENT DISORDER PROPAGATION

Inciting public disorder to intimidate an ethnic or political group within the community, or effect political change.

SEVERITY: 5

HATE SPEECH

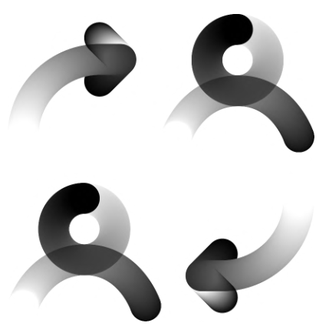
Offensive or threatening language that targets a particular group.

SEVERITY: 3

ILLEGAL TRADE

Selling illegal drugs, weapons, or other illicit goods via social media.

SEVERITY: 5



SOCIAL ENGINEERING

Manipulating someone through communication, so that they disclose sensitive data, smuggle contraband, etc.

SEVERITY: 1

THE MISUSE OF SOCIAL MEDIA

CHALLENGES

THE LARGE NUMBER OF SMALL OFFENSES

Minor offenses may seem relatively negligible, but viewed globally, they take on a different appearance. Petty cyber crimes such as cyberbullying, intimidation, and impersonation are currently so commonplace that victims rarely turn to the police. However, the social impact of such activities is tremendous. **Studies have found** that up to 35% of young adults have been persecuted online, and that, statistically, cyberbullying increases suicide rates by 8.7%.

Meanwhile, impersonation methods are mostly aimed at defrauding people and brands, and therefore have a financial impact. While each individual case may not seem to cost so much in the grander scheme of things, the cumulative expense is astronomical. With the annual cost of cybercrime expected to reach $10.5T by 2025, the socio-economic consequences should not be overlooked.

ANONYMIZATION

Those who conduct subversive information campaigns—for instance with violent disorder propagation or astroturfing goals in mind—use any tools and methods they can in order to anonymize their operations. In most cases, they use identity misappropriation to cover their tracks, alongside more technical anonymization tools such as TOR cloaking methods. Furthermore, due to their transactional anonymity, cryptos are the currency of choice in conducting financial operations.

Yet, social outreach may be considered the most important aspect of incitement campaigns. Therefore, countering sock puppet accounts on social media platforms remains a central objective in the fight against civil disruption. But how can analysts separate all the genuine profiles from the fake, when they are often indistinguishable at a cursory glance? And how can such tasks even be achieved in realistic timeframes?

LACK OF CONSUMER AWARENESS

While many understand the damage that fake news and astroturfing can do, a truly effective way to fight the issue remains as elusive as ever. According to a **2021 study**, 27% of radicals state that the internet was a primary catalyst for their extremist views and activities.

And the issue is compounded by its subtlety. Most people are simply unaware of how valid the information they consume is. **Research** shows that 80% of American adults have at some point digested fake news, while only 26% believe that they can identify false information.

ANONYMIZATION AND THE DIGITAL UNDERGROUND

THE DARKNET LANDSCAPE

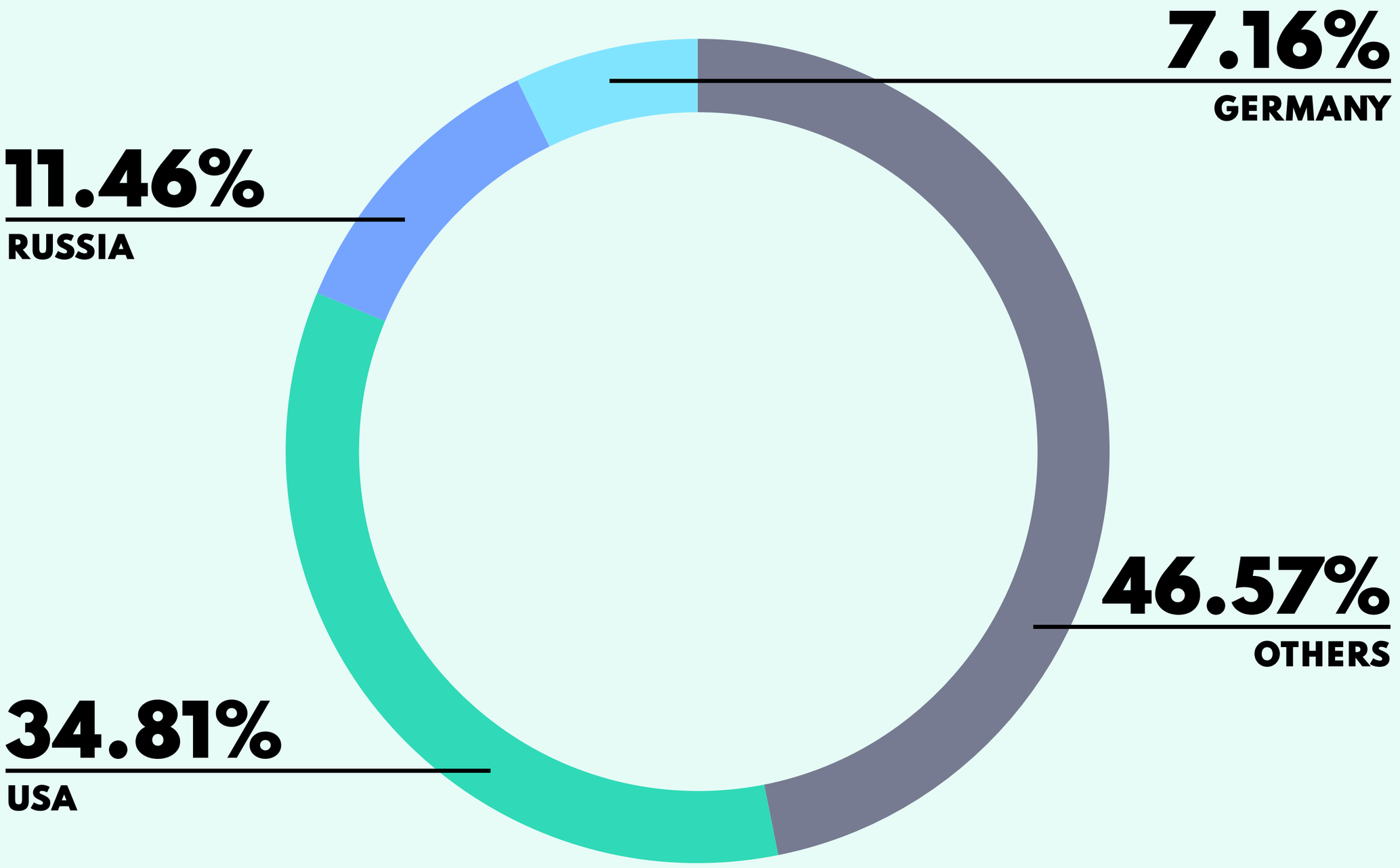
Widely thought of as the underbelly of the internet, and a safe haven for criminals, the Dark Web has earned itself a notorious reputation—and one that unfortunately holds a degree of truth. While plenty of legal activity unfolds on the Dark Web, a great deal is indeed illicit, and the reason for such disproportionate shadiness is simple: anonymity.

The Dark Web is navigated through specialized browsers—the most popular being TOR (The Onion Router)—that afford users a high degree of cloaking, or "virtual traffic tunnels". This makes user activity extremely difficult to track, which, in turn, draws illicit dealings. **Studies show** that 62% of people who use TOR, do so to utilize its anonymity features.

While this ill-famed domain only accounts for a fraction of the entire web—no more than 1%—it should be remembered that the Surface Web only **makes up 4%**, so the Dark Web is not insignificantly small. And it's growing fast, showing a **threefold expansion since 2017**, with the worldwide usership reaching 2M in 2022.

In terms of territories, the United States is home to the largest user base, representing 34.81% of the global demographic, with Russia coming in second at 11.46%, then Germany at 7.16%. Meanwhile, a total of 6.7% users harness the Dark Web for malicious purposes such as selling and buying illegal goods or services, and exchanging illicit data or content.

THE THREE LARGEST DARKNET USER BASES BY GLOBAL PERCENTAGE



Investigators who ignore the Dark Web are missing a crucial information source, while those who don't, face challenges in harnessing the data.

Dark Web users tend to be well-educated individuals, who are computer proficient and know how to mask their identity and cover their tracks. **58.8% of Tor users** have postgraduate degrees, and a further 17.7% have other qualifications from higher education.

ANONYMIZATION AND THE DIGITAL UNDERGROUND

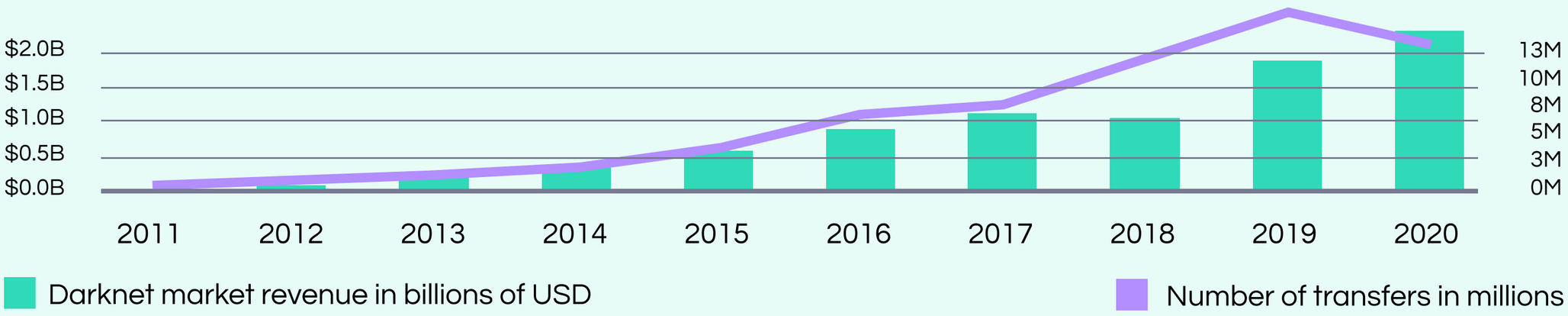
ILLEGAL TRADE ON DARKNET MARKETPLACES

Of all the illicit activity that is fostered by the Dark Web, by far the most abundant concerns the buying and selling of illegal goods and services. With the advent of Bitcoin in 2009, darknet marketplaces exploded.

A cryptographically obscured platform combined with an anonymous digital payment system drew both vendors and customers in their droves. In 2020, revenue from darknet markets hit an **all-time high of $1.7B**.

DARKNET MARKETS: REVENUE VS TRANSFERS RECEIVED

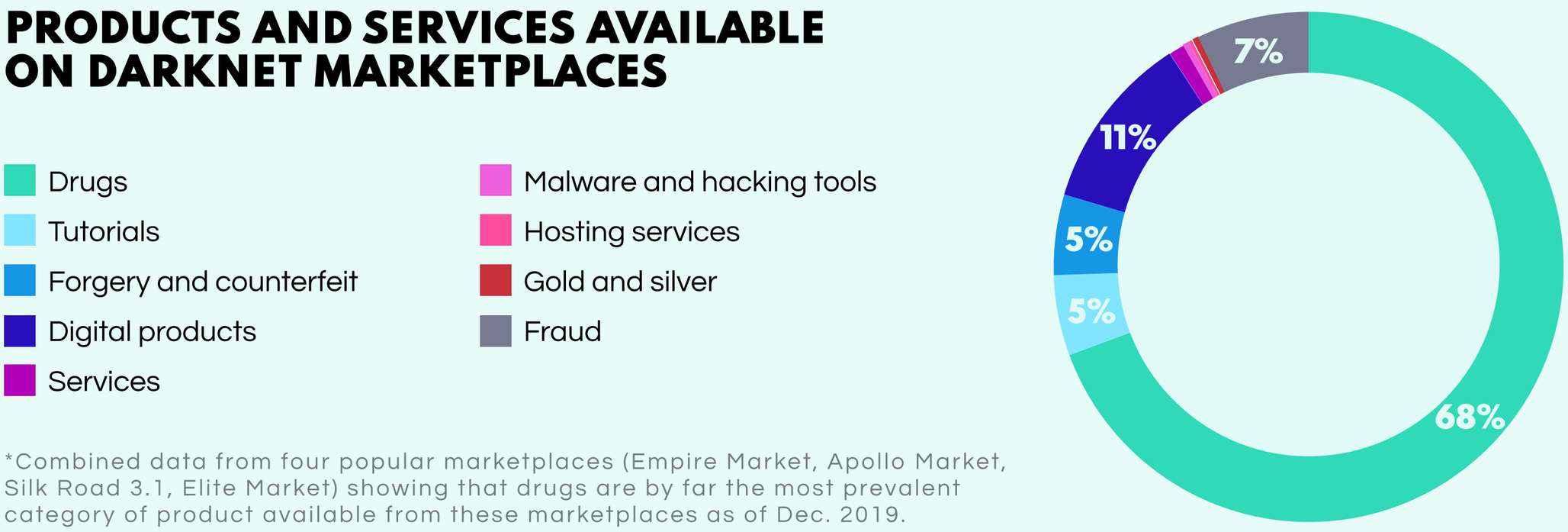
Source: Chainalysis 2021 Crypto Crime Report



Considering that these marketplaces are the go-to platforms for illicit trade, the type of wares being bought and sold are limited only by human imagination. Illegal items such as drugs, weapons, and counterfeit documents are par for the course. Drugs actually account for 68% of all illicit listings, while $80k-worth of firearms are sold every month.

Leaked data is also big business. A 2021 **SpyCloud study** reported 25.9M Fortune 1000 business accounts were doing the rounds. Hacked Facebook accounts can be bought for $65 and active bank details for $120. On top of this, all kinds of cybercriminal services can be readily procured. Distributed Denial-of-Service (DDoS) attacks are particularly popular, going for as little as $15 per hour.

PRODUCTS AND SERVICES AVAILABLE ON DARKNET MARKETPLACES



*Combined data from four popular marketplaces (Empire Market, Apollo Market, Silk Road 3.1, Elite Market) showing that drugs are by far the most prevalent category of product available from these marketplaces as of Dec. 2019.

As the foremost platform for conducting illicit trade, darknet marketplaces are clearly the online areas where investigators need to be looking to find peddlers of illegal goods and services.

However, with criminal actors taking care to conceal their activities behind layer upon layer of anonymization methods, law enforcement agencies need specialized technologies to overcome these hurdles.

ANONYMIZATION AND THE DIGITAL UNDERGROUND

THE ADOPTION OF CRYPTOCURRENCIES

Among the criminal classes of today, cryptocurrencies have unquestionably become the payment method of choice. Cryptos invariably provide a payment basis for cyber rackets such as the deployment of ransomware. **According to a Chainalysis report, the total cryptocurrency value received by ransomware addresses more than quadrupled between 2019 and 2020**, jumping from approximately $93M to $406M.

Yet, the criminal use of crypto is certainly not restricted to cybercrime—fraudulent investment schemes, illegal transborder money transactions, and payment for illegal goods and services are among the most common criminal motivations for adopting cryptos, not to mention terrorism and extremism financing. In short, almost any criminal activity that involves the transmission of monetary value can now be related to crypto transactions in some form.

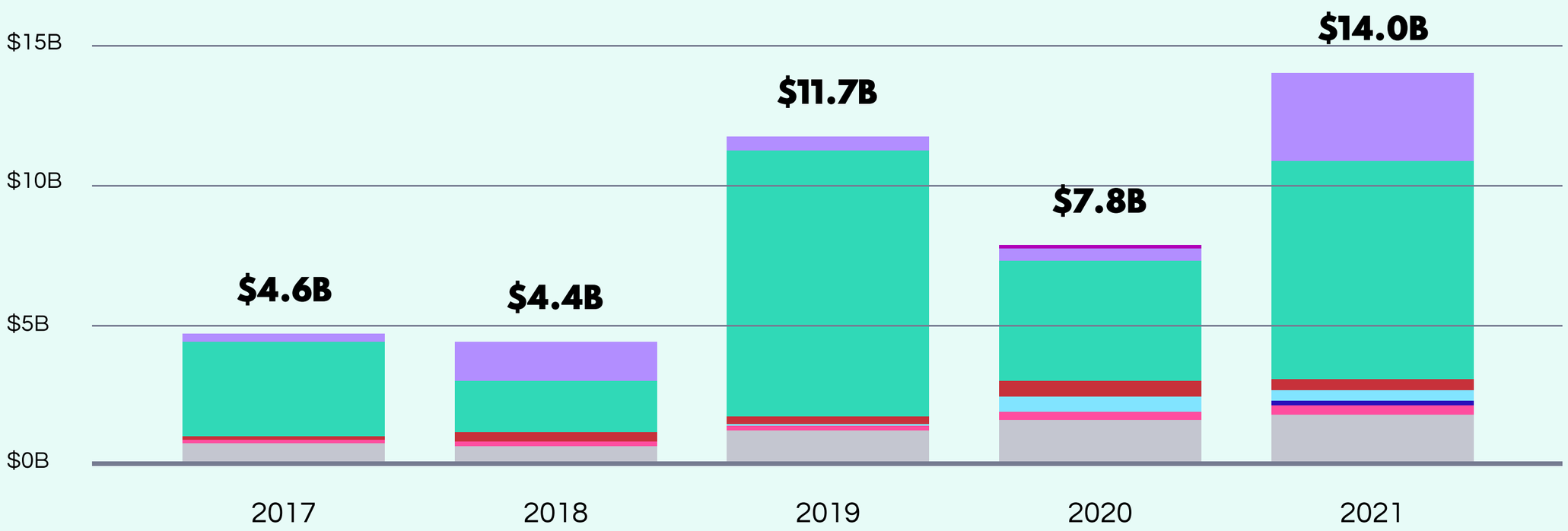
ESTIMATING CRIME-RELATED CRYPTO TRANSACTIONS

Due to its decentralized nature and **pervasive anonymity**, there is no conclusive figure on the proportion of crypto transfers currently being transacted for criminal purposes. In fact, conflicting estimates range dramatically between **0.15% and 46%** painting a somewhat vague picture of the situation.

The lowest point of this range comes from a **study** by the crypto investigation firm Chainanalysis, while the upper bound represents the findings of peer reviewed academic **research**. At the same time, the Financial Action Task Force (FATF) has **called into question** a narrower proposed range of 0.15%–15.4%, stating that the real percentage rate should be considerably higher.

TOTAL CRYPTOCURRENCY VALUE RECEIVED BY ILLICIT ADDRESSES, 2017–2021

Source: Chainalysis



However, even though such estimates are quite probably tentatively low, they still translate to huge amounts of money. Chainalysis estimated the monetary value of illicit crypto transactions at **$14B in 2021**.

And this figure is **deemed by some** as a significant underestimate since many illicit addresses have since come to light, modifying the estimate to $32B.

ANONYMIZATION AND THE DIGITAL UNDERGROUND

CRYPTOCURRENCIES AND MONEY LAUNDERING

While the anonymity offered by cryptocurrencies makes them an attractive payment method for illicit dealings, they also provide a raft of opportunities for a financial process that is essential for the majority of criminal actors—money laundering. After all, illegal assets and revenues are practically worthless if they cannot be legitimized or redeemed in some way.

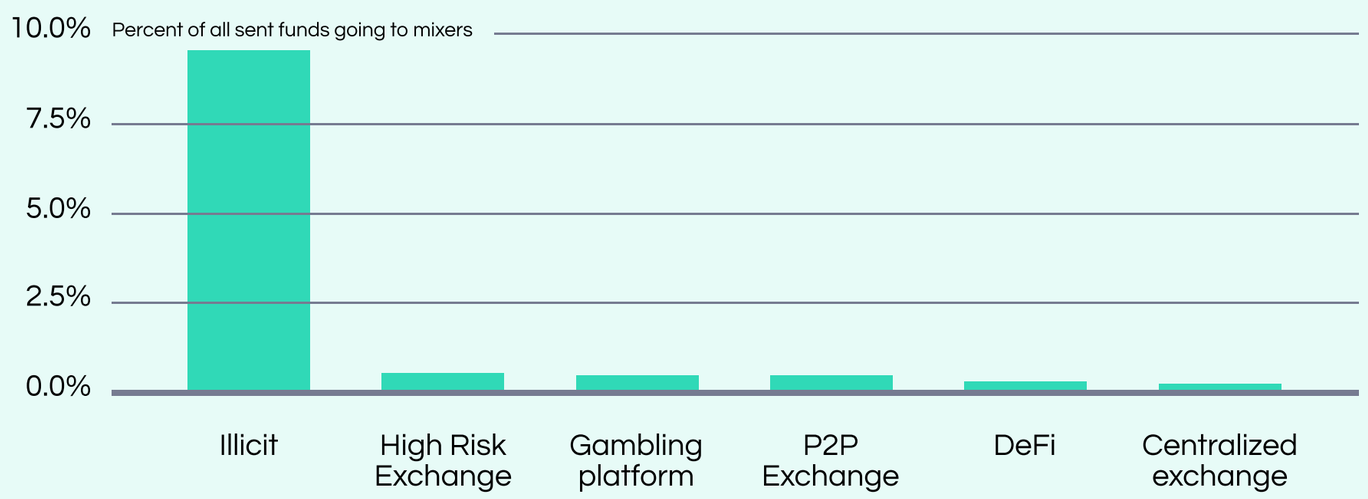
Blockchains consist of open data and are thereby transparent. In concept, they are distinctly lacking in privacy, because all transactions can be theoretically exposed to public scrutiny and traced back to the wallets. Why then, are they renowned for harboring anonymity, and how do they facilitate laundering?

MIXERS

Blockchain data can be thoroughly scrambled in order to obscure transactions. And this is precisely the service that cryptocurrency mixers offer. By blending together the cryptocurrency of multiple users, the blockchain is rendered indecipherable in these areas, making the tracing of transactions a very tall order indeed.

SHARE OF ALL SENT FUNDS GOING TO MIXERS BY SENDING ADDRESS TYPE, 2022

Source: Chainalysis



In this manner, criminals who fear being traced back to an illicit asset can pass the funds through a mixer then access the money with their tracks covered. In July, 2022, **Chainalysis reported** that 10% of illicitly held cryptocurrency entities had been washed via a mixer. This is in stark contrast to regulated entities such as centralized exchanges, of which only 0.01% had seen this process.

OVER-THE-COUNTER PEER-TO-PEER PLATFORMS

Although most of the centralized crypto exchanges have adopted stringent anti-money laundering (AML) policies, alternative trading options exist where this is most certainly not the case. Exchanges such as over-the-counter peer-to-peer (OTC P2P) trade platforms require minimal personal data and exercise virtually no control over the money flows. The lax regulations have attracted a significant user base to these platforms, which also enjoy popularity through trading flexibility—aside from crypto-to-crypto, users can also exchange crypto-for-fiat or crypto-to-goods.

MONEY-LAUNDERING-AS-A-SERVICE

For those who want to wash their crypto but don't have good technical knowledge of how to use mixers or alternative exchange platforms, there are plenty of services out there who will do it for them, in exchange for a commission or fee. And such options are proving popular. In the **QQAAZZ seizure case**, the laundering service operated in 20 countries, charging a huge 50% commission, yet their services were in high demand.

THE SOLUTIONS OF OSINT

ENHANCING DIGITAL FORENSICS

Used in: FORENSIC WORK, ORGANIZED CRIME CASES, COUNTER-TERRORISM AND RADICALISM

A large part of digital forensics concerns data extracted from devices—the physical artifacts collected in the course of a criminal investigation, such as computers, smartphones, USB sticks, external hard drives, and so on. Forensic experts then thoroughly draw out all data using **specialized extraction tools** before the analysts get busy, combing through the information for all manner of patterns, leads, and insights.

This process has long been a staple of digital forensics, but to consider hardware as the be-all and end-all of data sources would seriously limit the investigative scope. Placing hardware-based and online data into two separate camps is not just unnecessary, it is erroneous, and could even be counterproductive.

OSINT tools and techniques can significantly broaden the horizons of digital forensics. With automated open data processing tools, analysts can combine device data with the oceans of information available in the online realm. This can greatly enrich the evolution of a case, and provide investigators with leads which would be otherwise inconceivable.

HARDWARE FORENSICS →	COLLECTED DATA →	DATA ENRICHED WITH OSINT	
Mobile devices	Photo, audio and video materials	Social media profiles identification with image (photo) search	Information from 3rd party servers (sports apps, streaming services, etc.)
Computer hard drives	Chats	Information enrichment from the web and social media	Dark web activity identification
Thumb drives	Logs	Geo identification by photos and social media data	Data leaks on the person of interest collection
	Search history	Friends network reconstruction	

DIGITAL LOCATION TIMECODING

Used in: FORENSIC WORK, ORGANIZED CRIME CASES, COUNTER-TERRORISM AND RADICALISM, FRAUD CASES

Providing there is enough available data, timecode correlation is a simple and reliable way of proving an investigative hypothesis. For example, analysts can match information taken from surveillance cameras or witness statements with open data that validates the original source or acts independently. By harnessing locations from social media posts and tags, or geo data from apps such as Strava, investigators can reconstruct a subject's movements to corroborate extant evidence or deductive theories.

DNA ANALYSIS

Used in: FORENSIC WORK

OSINT solutions can even help the investigators with DNA matching. By connecting to the governmental or public DNA database, investigators can correlate genetic data with real-world identities and map out genealogical backgrounds, which can be essential in expanding the subject's social, professional, and geographical footprint.

Note: While DNA analysis mode is available on Social Links Professional, to harness your internal databases, Social Links Private Platform offers the most secure and powerful options for combining in-house and open data.

THE SOLUTIONS OF OSINT

SURVEILLANCE FOOTAGE AND BIOMETRICS

Used in: FORENSIC WORK, COUNTER-TERRORISM AND RADICALISM

CCTV footage from municipal public safety programs are a hugely important source for investigators. However, it is often the case that images are too noisy to be submitted as evidence or even recognized by witnesses. Advanced OSINT systems have the ability to extrapolate biometric data from even grainy footage, then run facial recognition searches that can locate matching images of the same person of interest from open sources. This can lead to the discovery of a subject's social media profiles, allowing the investigation to be considerably advanced.

HOLISTIC ANALYSIS

Used in: ALL CRIMINAL INVESTIGATIONS

Investigators are often confronted with data pictures that are fragmentary and incomplete. OSINT tools enable analysts to use the vast and varied resource of open data to interconnect points of information of disparate origin, cross-check and substantiate data and inferences, and fill gaps in the overarching structure of the case. The ability to view all related data globally can often suggest leads that would otherwise be too obscure to notice.

BACKGROUND CHECKS AND PROFILING

Used in: FORENSIC WORK, ORGANIZED CRIME CASES, COUNTER-TERRORISM AND RADICALISM, FRAUD AND LAUNDERING CASES

Investigative analysts utilize OSINT tools to create a highly detailed picture of the person of interest. Profiling and background checks sufficiently enhance the investigative process by helping analysts identify the current gaps in a criminal case, highlight patterns, and define further investigative steps. By enabling investigators to harvest all open data surrounding a given individual, OSINT tools provide the opportunity to discover more about a subject's lifestyle, connections, and even establish a psychological portrait. Furthermore, OSINT profiling techniques can be used to extract essential information such as a subject's name, location, communication sources, photos, videos, voice messages, vehicle information, financial details, and more.

PUBLIC RISK ASSESSMENT

Used in: COUNTER-TERRORISM AND RADICALISM

Operational researchers conduct online and offline intelligence searches for law enforcement officers on a daily basis. However, most of these studies are based on specific tasks and are often conducted 'ex post'—after the fact. OSINT tools provide analysts with the opportunity to assess public threats 'ex ante'—preemptively. Most criminals leave sizable digital trails, some of which include clear signals of the risk that they pose to society. AI-based gun detection modules, for example, can help investigators keep close tabs on those who haven't officially committed a crime yet, but may potentially do so individually or as a member of a criminal gang.

SENTIMENT ANALYSIS AND RIOT CONTROL

Used in: COUNTER-TERRORISM AND RADICALISM

Uprisings may seem to emerge spontaneously and unexpectedly. However, in most cases there are a plethora of weak indicators surfacing on the internet that forms of civil disorder were possible—or even imminent—due to changes in local public sentiment.

Sentiment analysis was once an expensive, time-consuming operation, conducted by specially trained sociologists. But the OSINT systems of today can not only conduct such analytical processes automatically, they can continually monitor the situation in real time so that authorities receive prior knowledge of potential unrest and the locales in which they are likely to play out. Furthermore, through the application of machine learning algorithms, OSINT tools can define sentiment changes around a particular topic, detecting hate speech and any given key themes or words.

THE SOLUTIONS OF OSINT

GROUP STRUCTURE IDENTIFICATION

Used in: ORGANIZED CRIME CASES, COUNTER-TERRORISM AND RADICALISM, MONEY LAUNDERING CASES

The internet has become a hub for modern terrorism and extremism, with many of the related activities taking place online. While social media is fostering radical indoctrination and recruitment processes, the rise of cryptocurrencies is facilitating fundraising for terrorist plots, arms trade is proliferating on darknet marketplaces, and the Surface Web is being used for target reconnaissance. Furthermore, decentralized network structures are enabling radicals to stay under the radar of law enforcement agencies.

The complex and nebulous threat posed by modern extremist and terrorist organizations is difficult to overestimate, and requires a host of techniques and technologies to effectively tackle. OSINT tools can significantly help investigators identify, map, and detail extremist groups and networks in various ways.

Firstly, by bringing together and consolidating massive volumes of data from a wide range of sources, OSINT tools can define even weak interconnections between people, and automatically elaborate possible group structures, complete with hierarchies including ring-leader and lieutenants, down to on-the-ground operatives.

Secondly, radical ideas can spread virally, having a wide-scale impact on impressionable demographics such as the young or marginalized. And like many viral ideas, radicalism has its own dynamic, language, symbology, and mottos, etc. OSINT technologies help analysts pick up on such signs, map out the communities where they are prevalent, and identify profiles which are actively engaged within the network, thereby flagging up people of interest for law enforcement agencies.

CRYPTO TRACKING FOR ILLICIT STREAMS AND ASSETS

Used in: CYBERCRIME CASES, FRAUD AND LAUNDERING CASES

Cryptocurrencies have fast become the most convenient way for criminals to transfer money. While some cryptos use highly sophisticated algorithms to cloak transactions, for the most popular currencies such as Bitcoin or Ethereum, felons can use mixer tools to effectively cover their tracks. Whatsmore, there is no single institution that can monitor these financial flows, yet they operate on a global scale, which is a propitious condition for laundering.

Specialized OSINT tools allow analysts to trace crypto transactions, including their recipients and senders, as well as the Dark-Web marketplaces and forums where the payments were made. Advanced OSINT systems also have the ability to unravel mixed cryptocurrencies to expose laundered assets and their owners. This enables investigators not only to uncover illegal trade and assets, but discover offshore schemes and other illicit financial activities.

Although the Dark Web only comprises a tiny fraction of the whole datasphere, it is the place to where most criminal activity can be traced. As a case in point, a Dark-Web marketplace that was seized by Europol in 2020 had 500k users, 2400 sellers, and 320k transactions amounting to $140M—the equivalent of 4650 bitcoins and 12800 moneros (a popular cryptocurrency among criminals).

COVERT INVESTIGATION

Used in: FORENSIC WORK, COUNTER-TERRORISM AND RADICALISM

Most online investigative activities are conducted in a passive form. This means that investigators do not directly reach out to people for the purposes of gathering information. Rather, they scour the internet and analyze publicly accessible data from which meaningful insights can be derived. However, this process is practically impossible without the use of specialized tools, since investigators cannot engage directly without giving themselves away. Furthermore, sock puppet accounts are simply not capable of gathering as much data as OSINT crawlers, which can automatically scan information from personal profiles across multiple online platforms without leaving any digital traces such as inclusion on a social media page's 'viewed by' list.

AREAS OF APPLICATION

OSINT: A MAJOR FORCE FOR FIGHTING CRIME

Digital forensics, reconnaissance, and footprinting, have become central methods in the majority of modern criminal cases.

LEAs and investigation bureaus increasingly depend on open data for verifying information, collecting evidence, and finding new leads across various types of inquiry.

CYBERCRIME CASES

OSINT tools have substantial utility in incident response (IR) and threat intelligence by bringing together vast amounts of open data to quickly and accurately detect breaches, and mitigate the impact of hacking instances. Furthermore, open data can be essential in conducting comprehensive analyses of cyberattacks to inform security measures and strengthen systems against future breaches.

FORENSIC WORK

Forensics specialists can derive vast amounts of additional information from crime-scene evidence through OSINT processes. By combining traditional and digital forensic methods, investigators can feed the OSINT system with the information retrieved from crime scenes to obtain a digital footprint of the person of interest, identify the actors involved, restore personal historical activities including geolocations, and find relevant social connections for further investigation.

ORGANIZED CRIME CASES

Criminal organizations make significant use of modern communication platforms including social media, messengers, as well as the Dark Web, in conducting their operations. OSINT tools empower investigators to quickly map and analyze the make-up, structure, and activities of crime syndicates including their affiliations, member profiles, financial transactions, and connections to illegal operations.

ILLEGAL TRADING CASES

Largely regarded as anonymous, the Dark Web has become host to a number of illicit markets including arms trafficking, drug dealing, and endangered animal trading among others. By connecting Surface Web accounts with counterparts in the Deep or Dark Web such as PGP keys, usernames, and cryptocurrency addresses, investigators can gain deep insights into criminal activities and actors, and make breakthroughs in various cases relating to black markets.

FRAUD CASES

LEAs are faced with the challenge of investigating a huge amount of fraud, from tax evasion and asset or property concealment, to corporate attacks that result in a significant yearly revenue losses. OSINT sweeps establish digital connections between individuals and organizations which the subjects were unaware even existed, unearthing fraudulent operations and corrupt allegiances.

MONEY LAUNDERING CASES

By analyzing blockchain data with OSINT tools, investigators can unpack money laundering systems to uncover their entire transactional structures, and connect addresses to stolen assets. Also, because malicious addresses tend to appear in scam reports, ongoing investigations, and social media discussions within the crypto community, OSINT tools can quickly flag up suspect crypto entities.

COUNTER-TERRORISM AND RADICALISM

Although it is of huge importance to preempt and neutralize terrorist and radicalist actions before they are realized, identifying plans and perpetrators within decentralized criminal groups is a complex challenge. Even determining the very existence of these networks can pose significant difficulties to security specialists. OSINT monitoring and automated group structuring technologies help law enforcement officers detect suspicious discussions and internet activity early on so that such organizations can be de-anonymized and neutralized before harmful acts take place.

THE ADVANTAGES OF OSINT TOOLS

GREATER ACCURACY AND SPEED

With a wide array of powerful search methods at their disposal, investigators have far greater control over the way information is extracted—relevant data can be focused in on, while superfluous material can be filtered away. Accurate, detailed digital profiling often depends on the range of parameters at the analyst's disposal. The ability to manipulate search methods for greater focus significantly accelerates investigative processes and often leads to a higher success rate.

AUTOMATION AND AI

In the field of OSINT, machine learning frequently plays a crucial role in the extraction and sorting of data. For example, neural networks are especially helpful in generating automated methods for image recognition. To find images that contain an object of focus—for instance a weapon—an extensive amount of open data may need to be trawled through. Such work would be time-consuming and laborious, but **search methods powered by AI can do the job much more effectively than a human, and in a fraction of the time**.

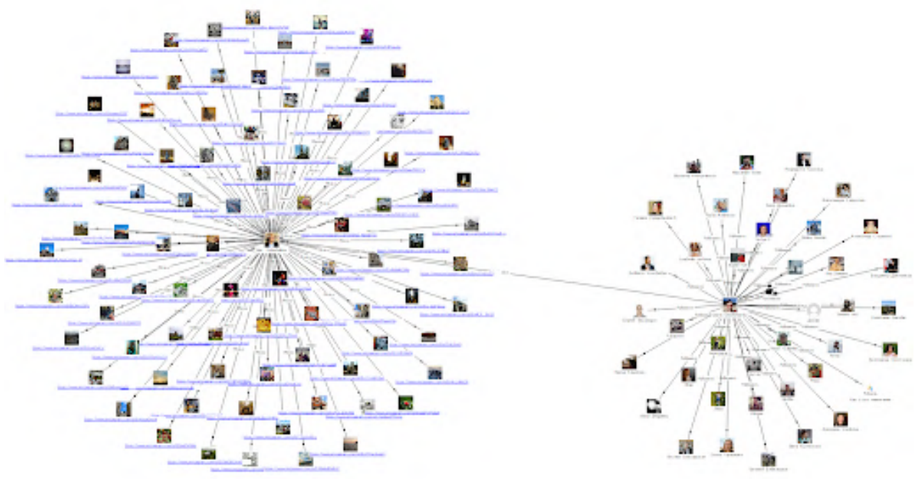
DATA TIME RELEVANCE

The immense amount of data pouring into the online sphere means that information can become out-of-date within a very short time-span. This is a continual problem for analysts who think they have found a crucial connection, only to subsequently learn that the key information is no longer relevant.

Modern OSINT tools have the ability to collect and analyze information in real time, allowing subjects to be monitored, and investigators kept entirely up-to-date. The investigative decision-making is consequently based on current, valid and relevant information, driving cases forward more effectively.

DATA VISUALIZATION

Making sense of reams of open data is a formidable task for the OSINT analyst. To facilitate the process, visualization tools are used, helping the analysts to create a comprehensible picture from the extant data. By viewing data as visual reference points on a graph, investigators can use vertices to piece together immense networks mapping out all the connections, affiliations, acquaintances, geolocations, subscriptions, etc. which are relevant to a particular investigation.



From this vantage point, threat actors or questionable activities can be quickly traced and identified, and data can be readily cross-checked and verified. This type of link analysis can give investigators the crucial insights they need to make significant breakthroughs in a wide range of cases, and can also embody evidence.