TRENDS IN SERIOUS AND ORGANIZED CRIME:

A rising global & technological threat

Cognyte

Formerly a Verint company

Cognyte
Formerly a Verint company

TRENDS IN SERIOUS AND ORGANIZED CRIME:

A rising global & technological threat

TABLE OF CONTENTS

ABSTRACT

Far from diminishing in the current century, serious and organized crime has persisted and thrived, making use of the same trends in globalization and technology that in so many ways have made our lives simpler, faster, and even safer.

This report explores the dimensions of serious and organized crime and how it has changed over the past few years by exploiting globalization and technology to become more sophisticated and tech-savvy than ever. We will then delve into some of the ways technology can help you battle this evolving threat.

DIMENSIONS OF SERIOUS AND ORGANIZED CRIME

In March 2021, law enforcement agencies around the world announced they had infiltrated the Sky ECC encrypted phone network, which had operated out of the United States and Canada for over a decade.[1] The company had a user base of 170,000 individuals who relied on the security of its dedicated hardware and encryption, in part, to facilitate transnational crime networks.[2] The company originally denied the claims that their security had been hacked along with denying allegations that it had become the "platform of choice for criminals."[3] However, its website was later seized by the FBI and other international law enforcement agencies.

While the Sky ECC case is still pending as of this writing, an earlier encrypted phone network called EncroChat was cracked in 2020 and led to the UK's largest law enforcement operation, resulting in over 700 arrests,[4] followed by another 1,500 in early 2021.[5] The National Crime Agency had evidence that the EncroChat network was used to facilitate the "distribution of illicit goods, money laundering and plotting to kill rivals."[6] Police claimed that in the earlier raid, they had successfully mitigated over 200 "threats to life."

[1] https://www.europol.europa.eu/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks
[2] https://www.computerweekly.com/news/252497791/Arrest-warrants-for-Candians-behind-Sky-ECC-cryptophone-networks-used-by-organised-crime?vgnextfmt=print
[3] https://www.globenewswire.com/news-release/2021/03/10/2190026/0/en/SKY-ECC-platform-remains-secure-and-no-authorized-Sky-ECC-device-has-been-hacked.html
[4] https://edition.cnn.com/2020/07/02/uk/encrochat-crime-messaging-cracked-intl-gbr-scli/index.html
[5] https://www.thetimes.co.uk/article/1-500-arrested-in-swoop-on-drug-gangs-using-encrochat-7r7lnwcmv
[6] https://edition.cnn.com/2020/07/02/uk/encrochat-crime-messaging-cracked-intl-gbr-scli/index.html

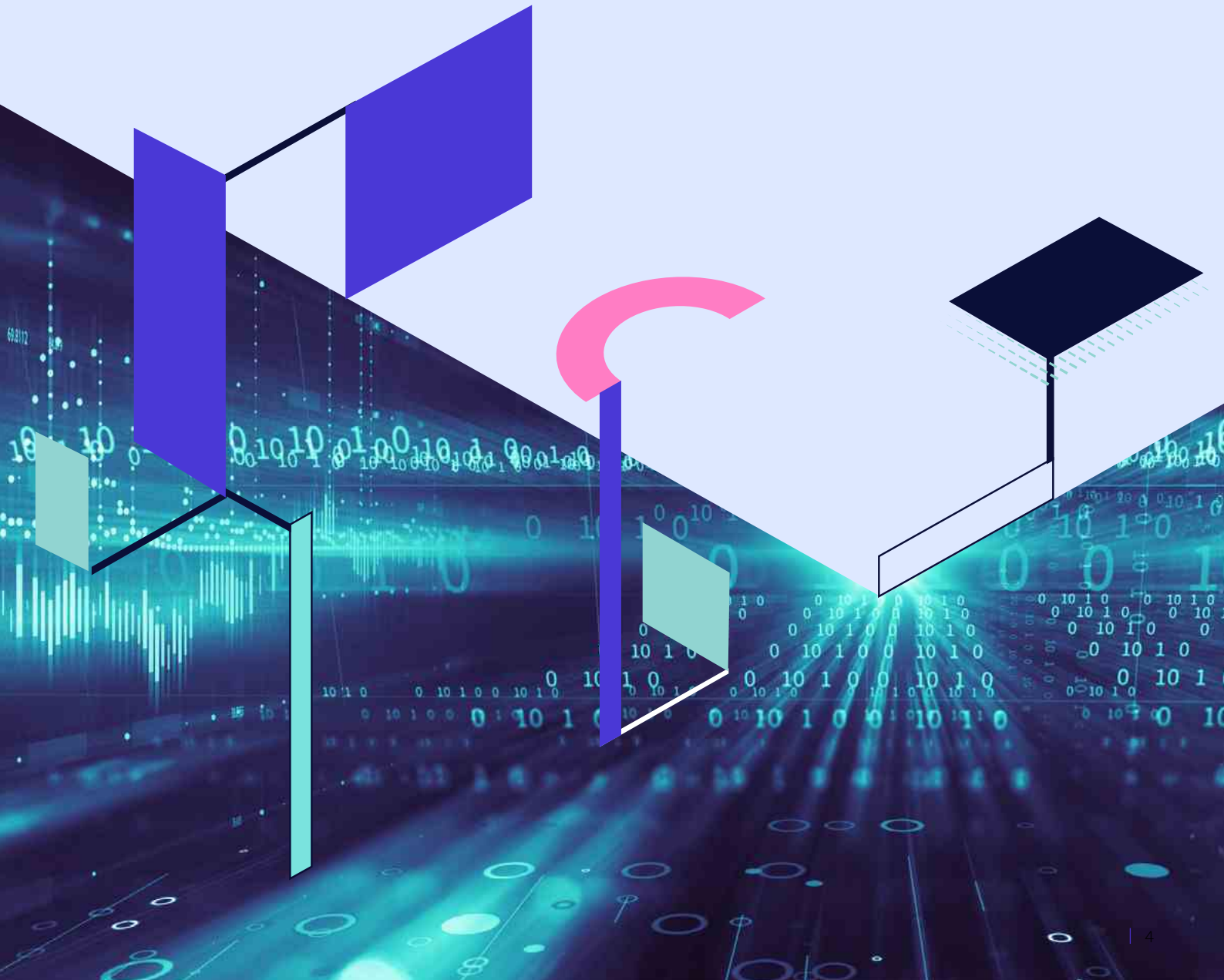
The magnitude of today's serious and organized crime often comes as a surprise to those who don't work in law enforcement, as it tends to fly under the radar until a major news item like the EncroChat raids makes headlines.

Most people only see the tip of the iceberg: A major crime leader is arrested in South America, an exposed kidnapping ring shocks the world, or another high-profile trial hits the courtroom where the scope of criminal activities is laid bare.

As with an iceberg, it can be hard to see just how extensive these crime networks are. What looks like a local phenomenon, confined to a single city, jurisdiction, or country, may in fact have grown to represent a far more insidious threat beneath the surface and under the cover of highly encrypted, secretive networks like Sky ECC, EncroChat, or the dark web.

For individuals in law enforcement and security, it's vital to recognize the true reach of serious and organized crime today, as it is redefining itself, expanding across borders, and broadening its scope.

Before we explore the modern dimensions of this threat and discuss concrete solutions that make use of cutting-edge technology, let's first briefly highlight what falls within the scope of serious and organized crime.



WHAT IS SERIOUS AND ORGANIZED CRIME?

Different organizations and government bodies use a range of names to describe the types of crime discussed in this report. Today, almost all serious crime falls into the broad category of transnational organized crime (TOC), a subcategory of which is organized crime groups (OCGs). TOC is also associated with terrorism.

Transnational crime represents a massive and lucrative underground economy that spans the entire world – and it is growing in size and scope. It is important to distinguish "transnational" crime from "international," which is recognized and governed by international law and includes crimes against humanity, such as genocide.

According to the FBI, "TOC poses a significant and growing threat to national and international security with dire implications for public safety, public health, democratic institutions, and economic stability across the globe."[7]

According to Europol's Serious and Organized Crime Threat Assessment (SOCTA),[8] major areas of activity for transnational crime organizations include cybercrime; drug production, trafficking, and distribution; migrant smuggling and human trafficking; property crimes including trade in illicit goods and services; and criminal finance and money laundering.

The reason serious and organized crime is growing is its extreme profitability. Although some transnational criminal activity is committed by nation-state actors with political goals or those who seek to unsettle international peace,[9] the most serious crime organizations are run like businesses.

[7] https://www.fbi.gov/investigate/organized-crime
[8] https://www.europol.europa.eu/socta-report
[9] https://core.ac.uk/download/pdf/35317222.pdf?repositoryId=894

THE CRIMINAL ECONOMY

Due to its very nature, there is no way to know exactly how profitable serious and organized crime really is, but current estimates are around $2.2 trillion—and growing.[10] Money laundering alone represents potentially up to half that figure, according to U.S. government estimates.

The amount of money involved is clear from recent headlines:

2021 Just months before being taken down, the encrypted phone network Sky ECC announced on its site, "We're so confident SKY ECC is unbeatable, we'll give US $5,000,000 to anyone who can beat our device and encryption."[11]

2019 With the capture of Fuminho, the head of Primeiro Comando da Capital (PCC), Brazil's largest OCG, "the São Paulo Attorney General's Office estimated the PCC's earnings stood at around 800 million reais ($145 million) a year."[12] (particularly dramatic given Brazil's GNI per capita is only $9,13013)

2021 The Rohingya crisis increased public awareness about the hundreds of people being trafficked for years on illegal ships, driving illegal migration, and adding to the overall financial cost of migrant smuggling in SE Asia, estimated to be $132-196M. Over half a million Rohingya migrants have paid $2,000-$3,000 to be smuggled illegally out of Myanmar so far. These dollar figures and major headlines, as already mentioned, are just the tip of the iceberg. But even these are substantial enough to convince anyone that the rest of the iceberg is overwhelmingly large.

"Serious and organized crime is estimated to be $2.2 trillion-and growing"

- Organized Crime and Corruption Reporting Project

There are multiple factors that hinder law enforcement agencies attempting to combat serious and organized crime using traditional means:

It often emerges from countries experiencing poverty, war, displacement, bureaucracy, and corruption, which may not have resources and personnel for law enforcement.

It is highly tech-savvy, with increasingly sophisticated tools to accomplish its goals and hide from law enforcement agencies.

It is expanding, both globally and into a broader range of criminal activities, making use of extensive hidden networks of connections (to individuals, groups, and governments worldwide).

In the following sections, we will explore the ways these criminal organizations are using technology and globalization to spread out, both horizontally into different types of criminal activities and vertically in terms of the scale of those activities.

[10] https://www.occrp.org/en/daily/6240-ngo-transnational-organized-crime-groups-make-us-2-2-trillion-a-year
[11] originally https://www.skyecc.com/challenge/ , cited in https://threatpost.com/europol-arrests-cracked-sky-ecc/164744/
[12] https://insightcrime.org/news/analysis/brazil-gang-finances-pcc/
[13] https://www.statista.com/statistics/1066745/gross-national-income-per-capita-brazil/

TECHNOLOGY IS ENABLING TODAY'S SERIOUS AND ORGANIZED CRIME GROUPS

Over the last two decades, serious crime has encountered the same massive geographic, economic, and technological shifts as the rest of the world. These include the adoption of widespread and massively networked technologies along with the use of advanced and covert communication methods.

A few alarming statistics emerge from the most recent 2021 Europol SOCTA report."[14] The report demonstrates the true scope of criminal activity happening throughout Europe, covering 5,000 international groups and over 180 nationalities. According to their report, 7 out of 10 organized crime groups are active in more than three countries. It goes on to warn that "Criminals will continue to rely on the use of new technologies and further expand their technical capabilities."[15] Facilitating all these transnational activities are the same global technologies the world is using for entertainment, business productivity, and financial transactions.

"The 2020 State of Crypto Crime Report" is similarly shocking,[16] revealing that darknet markets for cryptocurrencies reached a value of $790 million. Far from funding only cybercrime, cryptocurrencies are being used to fund darknet transactions related to drugs and other illicit goods, stolen data such as credit card information, and, perhaps most alarmingly, child abuse. At the same time, sophisticated money laundering services are enabling the exchange of crypto for fiat (standard) currency while disguising the true nature of criminal organizations' assets. The report also mentions that although the trend is still in its early stages, terrorist groups have been increasingly embracing a range of technologies, including cryptocurrency, in order to advance their agenda.

Today's serious and organized crime groups use technology in two basic ways: to commit criminal activities and as a countermeasure against law enforcement. Let's explore these two paths in more detail.

> *" **7 out of 10** organized crime groups are active in more than three countries. "*
> - Europol

[14] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment[8] https://www.europol.europa.eu/socta-report
[15] https://www.europol.europa.eu/sites/default/files/documents/socta2021_2.pdf
[16] https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf

USE OF TECHNOLOGY TO COMMIT CRIMINAL ACTIVITIES

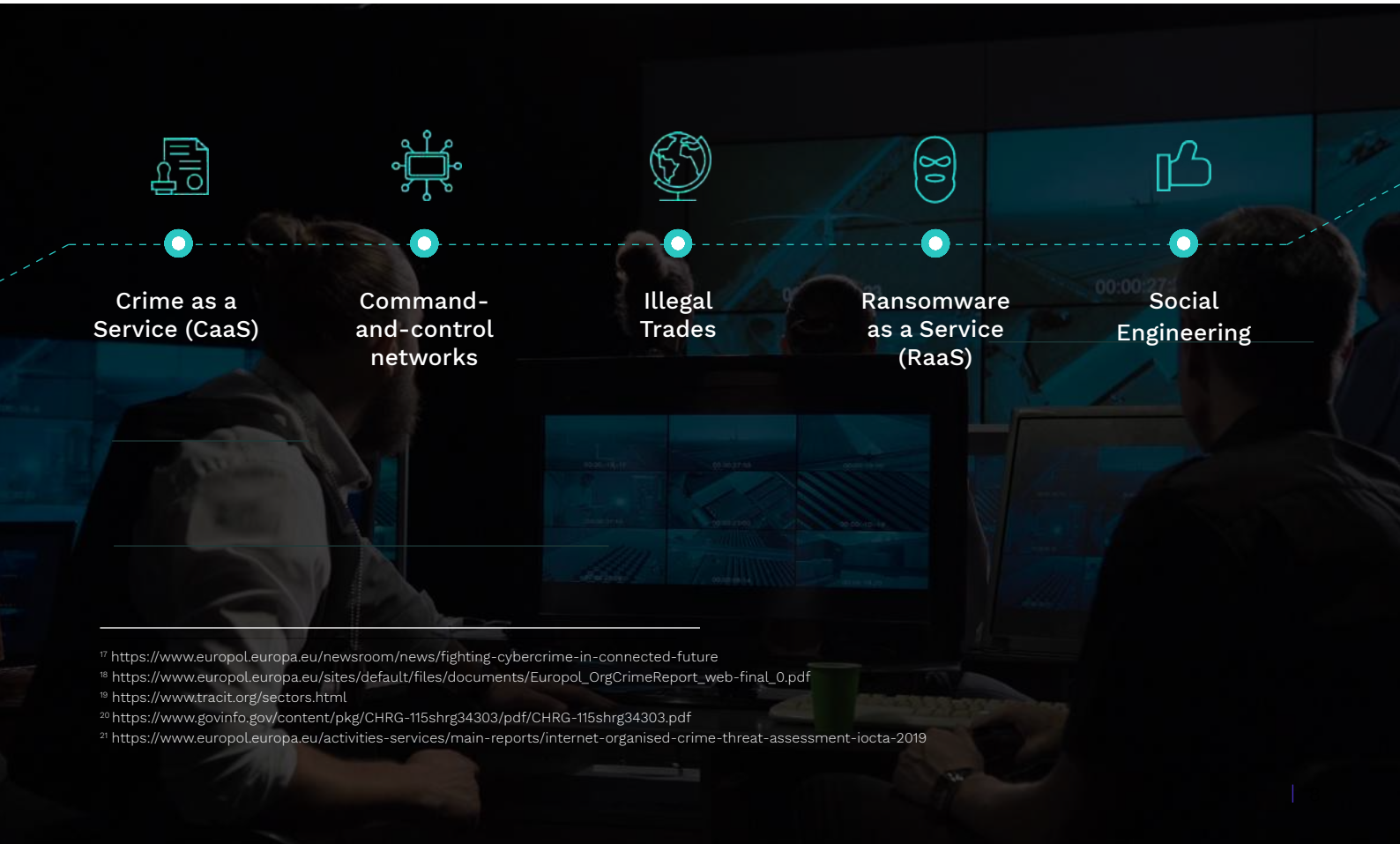
When it comes to committing technology-based crimes, the first thing that comes to mind is cybercrime. While a full discussion of cybercrime is outside the scope of this report, everyone involved in law enforcement and security must be aware that it is becoming more audacious, with highly focused, crafted attacks resulting in serious damage to major, profitable targets.[17]

One of the phenomena noted by the State of Crypto Crime report is the growth of the "Crime as a Service" business model, particularly seen in Ransomware as a Service (RaaS). Sophisticated hackers use the darknet to literally rent out easy-to-use malware to newcomers while taking a cut of the proceeds. This eliminates the need for the cybercrime expertise and infrastructures OCGs have needed in the past if they wanted to profit from ransomware; today, anyone can break into cybercrime with only minimal investment. In addition, according to Europol, Crime as a Service is harder for law enforcement to detect and carries lower penalties than traditional forms of criminal activity.[18]

Cybercrime represents a profitable market to traditional OCGs since the barriers to entry are so low. In other words, serious and organized crime is being transformed by the "integration of digital systems in many criminal activities and the expansion of the online trade in illicit goods and services."[19]

For example, social engineering is one high-tech strategy–using email or other online communication- that criminals are leveraging to perpetrate insurance fraud. As reported in a 2017 U.S. government hearing, "as technology improves, so are the fraudsters improving the ways that they get more sophisticated and commit these crimes."[20] The same social engineering techniques are also becoming prevalent in other highly lucrative areas, such as investment fraud.[21]

As many brick-and-mortar retailers have discovered over the last two decades, expanding into cyberspace makes sense because it allows them to access new markets and remain competitive, enabling them to stay in business when many other retailers haven't survived globalization. The same is true for OCGs moving their activities into cyberspace.



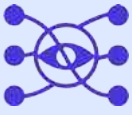
[17] https://www.europol.europa.eu/newsroom/news/fighting-cybercrime-in-connected-future
[18] https://www.europol.europa.eu/sites/default/files/documents/Europol_OrgCrimeReport_web-final_0.pdf
[19] https://www.tracit.org/sectors.html
[20] https://www.govinfo.gov/content/pkg/CHRG-115shrg34303/pdf/CHRG-115shrg34303.pdf
[21] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

But it is important to note that the use of technology doesn't only refer to cybercrime. In today's criminal spheres, many "real-world" crimes are facilitated in cyberspace. These are known as "cyber-enabled," as opposed to "cyber-dependent," crimes, which are those that take place entirely or almost entirely online.

For instance, in the 2013 Azov Films case, police raided the home of the owner of a website selling child pornography. That raid resulted in the investigation and arrest of hundreds of adults in more than 50 countries, along with the discovery of more than 300 children who had been exploited. While the internet was an essential factor in the operation of the business, this was an example of a cyber-enabled crime since it could theoretically have taken place entirely offline. The technology involved simply made the business more lucrative and enabled it to spread globally.

The leading technology for those engaged in cyber-enabled crime is social media platforms and applications, which are used by 46% of the world's population and are now also the "command-and-control" networks of choice—for both transnational organized crime and terrorism.

For criminals, technology assists in the same ways it does in most day-to-day activities: providing hassle-free communication across borders and thus allowing OCGs to move money around almost instantly, recruit personnel, keep teams informed, and implement plans on the ground. Two other factors are making business more efficient and lucrative:



The decline of face-to-face transactions and the use of cash in favor of the darknet, social media, apps, and cryptocurrency. For instance, a 2020 Europol report on drug markets indicated that dead drops, which used to be prevalent mainly in Eastern European countries like Moldova and Ukraine, are now being used by darknet drug vendors in countries like Spain and Finland.[22]

The rise of privacy-focused, decentralized marketplaces, as seen, in part, by the 27% rise in darknet cannabis sales in the early months of the COVID-19 crisis.[23]

[22] https://www.emcdda.europa.eu/system/files/publications/13097/EU-Drug-Markets_Covid19-impact_final.pdf
[23] https://www.europol.europa.eu/sites/default/files/documents/eu_drug_markets_covid19_impact_final.pdf

USE OF TECHNOLOGY TO THWART LAW ENFORCEMENT

Beyond facilitating crime with new tools to communicate and commit crime, technology advancements also give offenders increasingly sophisticated means to hide their crimes. Technological means used to thwart law enforcement include encrypted communication networks such as Sky ECC, advanced document forgery, underground payment methods, and alternative banking and trading platforms for money laundering.

Low-tech means to evade law enforcement, such as vehicle theft, have taken on high-tech dimensions. For instance, OCGs use advanced tools to steal vehicles and perform sophisticated document fraud via digital technologies to give stolen vehicles new identities.[24]

While law enforcement agencies and security organizations do have some sophisticated means of detection, it is hard to keep up with a highly motivated criminal organization attempting to evade detection or capture.

New payment methods and alternative banking platforms have also proven rich territory for criminal actors interested in hiding their activities, as mentioned above in the context of darknet exchanges and crypto money laundering. Beyond cryptocurrencies, these methods include prepaid cards, online payments, and internet vouchers, with new technologies popping up every day.

As new payment means and exchanges are introduced, these are often poorly regulated at first, as government regulatory bodies move very slowly to assess and fully understand the new offerings before attempting to adapt existing regulations or introduce new ones. International standards are poorly defined and inconsistent for the same reasons, making enforcement across borders particularly difficult if criminals move funds to a more “friendly” jurisdiction. This means criminals will be drawn to these methods either until they become mainstream or are shut down by law enforcement.

All of this means it’s harder than ever for law enforcement agencies to investigate crime, and resources including technological tools are needed to stay ahead of well-funded, well-organized, nimble criminals.

[24] https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pd

THE CURRENT SPREAD OF SERIOUS AND ORGANIZED CRIME

One of the biggest challenges in countering serious and organized crime is its fluid dimensions, which are increasingly shifting and expanding in scope. For many law enforcement and other security organizations, one leading concern right now is the massive spread of OCGs not only geographically, but also in terms of the types of crimes they commit.

GEOGRAPHIC SPREAD

Serious and organized crime previously limited to one area has spread into other areas of the world.

POLY-CRIMINALITY

Serious crime organizations are also spreading their activities into other types of crime, particularly cybercrime.

As an example of the severity of these combined threats, in 2018, Interpol held a conference dedicated to the spread of serious and organized crime in Africa. Criminal activities, the key findings noted, comprised a breathtaking range of goods and services, from malware to fake medications, from human trafficking to illegal logging, all facilitated by geographic spread to other parts of the world, notably South America and Europe.[25]

GEOGRAPHIC SPREAD

When Brazilian PCC boss Fuminho was captured in Mozambique, it was revealed that he was merely using that country as a pipeline to channel cocaine throughout southern Africa.[26] This expansion into other countries of operation is increasingly common, though it did slow somewhat with COVID-19. Over 70% of OCGs are typically active in more than three countries, according to Europol, with three areas of particular mobility in OCGs including:

East-West and Cross-Europe OCGs.

OCGs typically active in Eastern Europe are increasingly moving into Western Europe. For example, the UK, which has historically had a very low level of weapons violence, is now fighting against weapons smugglers from former Eastern Bloc countries and Russian money laundering.[27]

Latin American OCGs.

From the extensive network uncovered when PCC leader Fuminho was taken down, it is clear that Latin American OCGs, of which PCC is the largest, are working hand-in-hand with and through groups in other nations to conduct their activities.

Blue crime

Often overlooked when it comes to the geographic mobility of OCGs is transnational organized crime that takes place at sea, as seen with the illegal migration of the Rohingya people out of Myanmar; this also encompasses crimes against mobility, illicit flows, and environmental crimes.

Borders are no longer enough to contain these organizations. According to a 2021 report in Americas Quarterly, "[Transnational criminal organizations] respect no borders or rule of law and operate with agility and innovation."[28]

[25] https://www.interpol.int/en/News-and-Events/News/2018/Transnational-crime-converging-across-Africa-INTERPOL
[26] https://clubofmozambique.com/news/mozambique-fuminho-controlled-the-local-and-south-african-drug-market-carta-157588/
[27] https://www.bbc.com/news/uk-44102751
[28] https://americasquarterly.org/article/the-threat-that-cannot-be-addressed-alone/

POLY-CRIMINALITY

The term poly-criminality or multi-criminality, when applied to serious and organized crime, refers to crimes that are usually multidisciplinary, representing a hybrid of physical and cyber-criminal activities and often taking place across international borders.

This trend already existed before COVID-19 but became even more pronounced in the wake of the pandemic. Just as COVID-19 forced businesses to pivot quickly, organized crime groups were forced to expand their activities in ways that did not involve crossing physical borders or, in some cases, going out in public at all. Reports indicate that since COVID-19, for instance, PCC and other Latin American OCGs have expanded into cybercrime.[29]

As mentioned above, the move into cybercrime for a mainstream OCG no longer necessarily requires advanced technical expertise due to the expansion of such dark web offerings as Ransomware as a Service (RaaS) and the entire field of Crime as a Service.

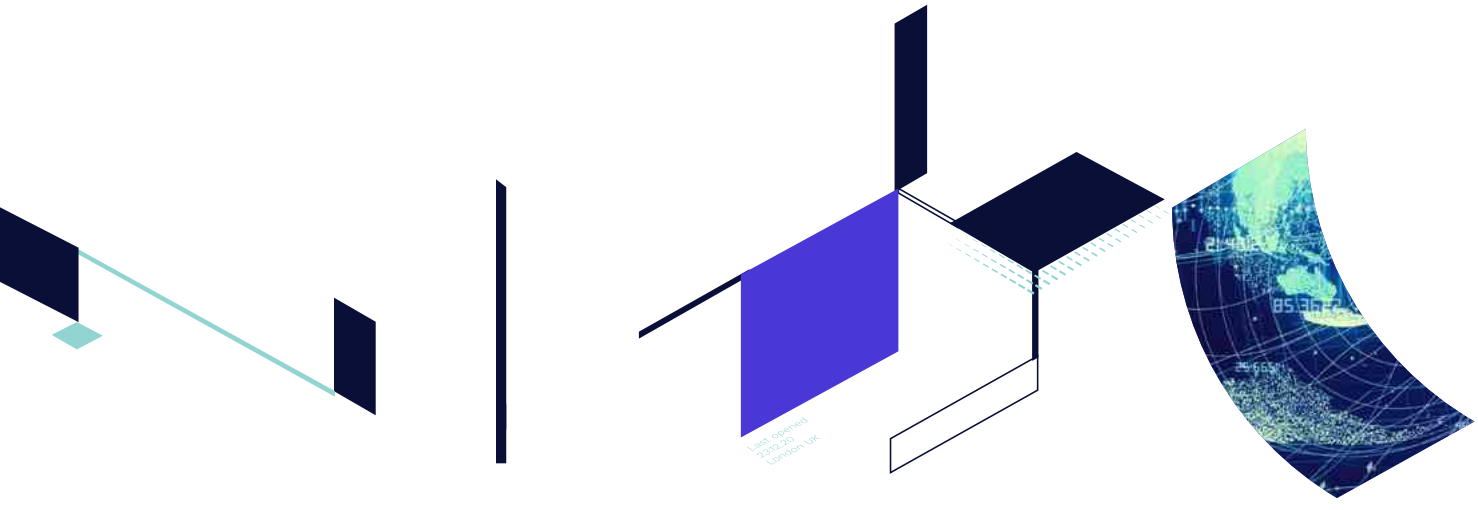
This should not be taken to mean that COVID has steered OCGs away from their original physical activities. Unfortunately, according to UNODC, it is anticipated that COVID-19 will actually create an uptick in human trafficking, for example, due to the resulting economic crisis, putting millions of men, women, and children at greater risk for exploitation.[30]

Instead of replacing their original criminal activities, OCGs see this forced diversification of serious and organized crime as a way of building resilience and eliminating risk wherever possible. In other words, they are running their organizations more and more as large enterprise-scale businesses and adopting technological solutions, just as all smart enterprises do.

As the UK-based defense and security think tank RUSI explains, “Where law enforcement agencies see a focus on firearms, drugs or tobacco smuggling, OCGs simply see a business opportunity. As highlighted by the Italian-based research center Transcrime, diversification of activity allows them to expand the economies of scale among illicit markets, reduce operational costs and, ultimately, increase their profit margins.”[31]

The RUSI report highlights this shift in OCGs’ operating model as a challenge for law enforcement. When an organization is spread out across continents and operates in drug trafficking, environmental crime, money laundering, and cybercrime, it’s not enough just to gather one type of information. Agencies and organizations fighting serious and organized crime must often adopt multiple methodologies to detect and disrupt these activities.

This demands flexibility along with solutions that can expand and scale to meet the demands of today’s law enforcement - just to stay a step ahead.



[29] https://americasquarterly.org/article/transnational-crime-pcc/

[30] https://www.unodc.org/unodc/frontpage/2021/February/share-of-children-among-trafficking-victims-increases--boys-five-times-covid-19-seen-worsening-overall-trend-in-human-trafficking--says-unodc-report.html

[31] https://rusi.org/commentary/it%E2%80%99s-who-you-know-not-what-you-know-why-we-need-focus-organised-crime-networks-and-not

COG8 SIDEBAR: BRAZILIAN ORGANIZED CRIME

Brazil's organized crime groups (OCGs) encapsulate today's trends in serious and organized crime. They are the main reason that Brazil, which borders three cocaine-producing nations,[32] has the world's highest homicide rate.

The leading OCG in Brazil is Primeiro Comando da Capital (First Capital Command, usually known as PCC), but there are numerous other large and active groups. These include Comando Vermelho (Red Command, or CV), which became a PCC rival in 2016 leading to bloody battles in Rio's slum districts, or favelas,[33] and Familia do Norte (Family of the North, or FDN).

PCC itself, which may have up to 30,000 members,[34] was founded in 1993 within Taubate Penitentiary[3] but has been particularly active since 2006, when it launched a series of lethal attacks against São Paulo's Military Police. Even though many members are in prison, poor prison discipline and easy access to cell phones allow leaders to mastermind activities from behind bars.

OCGs succeed in Brazil in part due to the belief that they take care of ordinary citizens in ways governments can't. During COVID-19, PCC oversaw curfews and price controls in the favelas to curb the spread of the disease.[36, 37] OCGs provide income in the face of massive unemployment and fight dangerous, unhealthy prison conditions.[38] Another factor fueling OCG dominance in Brazil is the rising middle class, which has led to a demand for commodities unavailable through legitimate means.[39]

PCC is run like a multinational corporation with leaders appointed for each of the organization's divisions, such as money laundering, drug sales, and bank robbery. This tight business model has let it grow to become the dominant force in South and Central America and has facilitated its global expansion. Other OCGs, like CV, are more loosely organized.

As with OCGs elsewhere, Brazilian OCGs are expanding both geographically and in the realm of poly-criminality.

Geographic expansion: Brazilian OCGs originated due to the country's central location to the cocaine trade. However, in recent years, beyond expanding into easy-access markets within South America, Brazilian OCGs have become more aggressive, expanding to control cocaine trade routes even in Africa and Europe.[40]

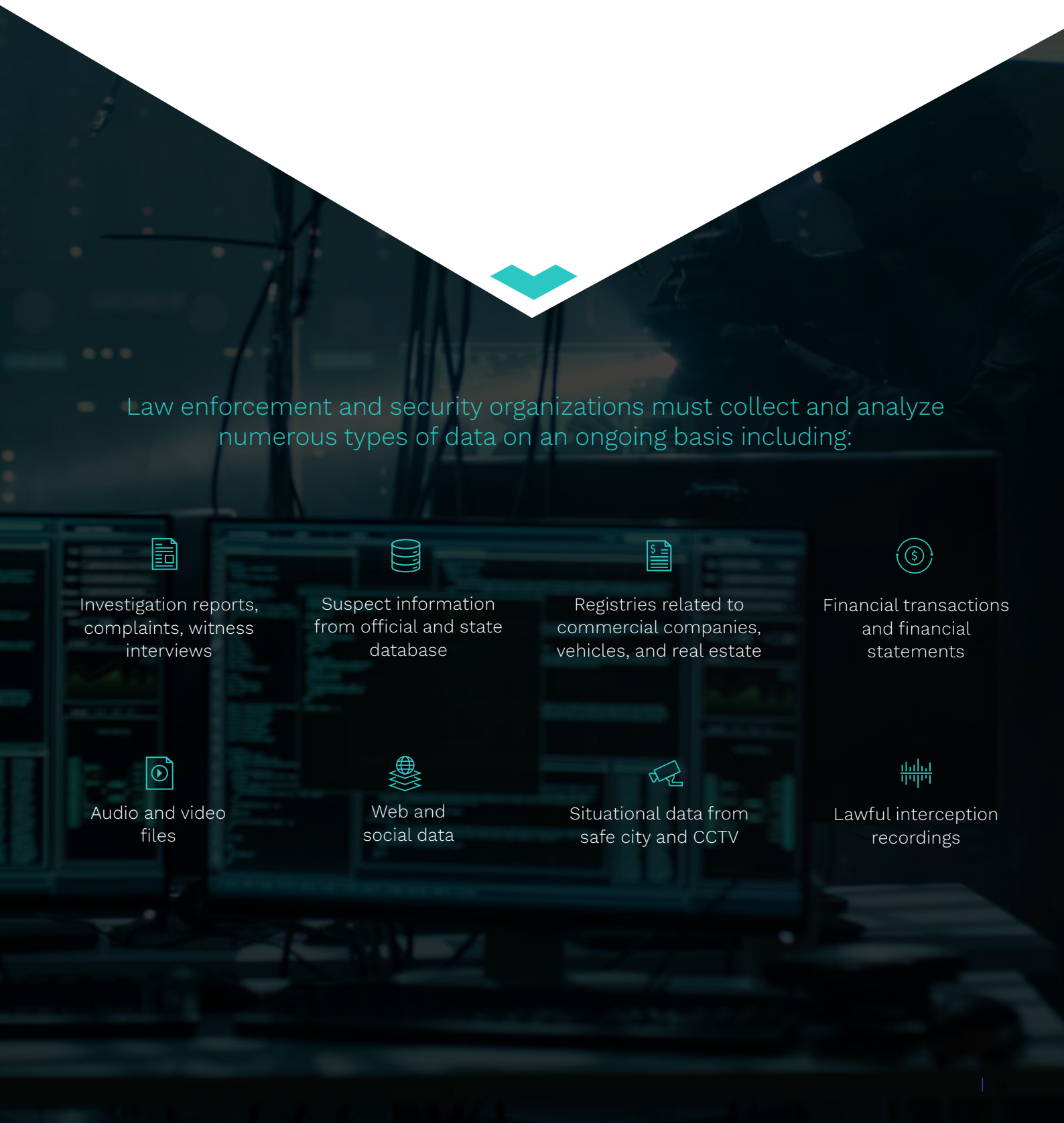
Multi-modal crime: Brazilian OCGs have shifted from their early focus on the drug trade. Today, they're involved in a wide range of criminal activities, including human trafficking, global cybercrime,[41, 42] and environmental crimes such as smuggling mercury,[43] an insidious environmental toxin used in refining gold.

[32] https://globalinitiative.net/analysis/lessons-from-organised-crime-task-forces-brazil-and-beyond/
[33] https://americasquarterly.org/article/red-command/
[34] https://americasquarterly.org/article/transnational-crime-pcc/
[35] https://www.researchgate.net/profile/Marcos-Alan-S-V-Ferreira-2/publication/328747324_Brazilian_criminal_organizations_as_transnational_violent_non-state_actors_a_case_36 study_of_the_Primeiro_Comando_da_Capital_PCC/links/5c335df9458515a4c713f034/Brazilian-criminal-organizations-as-transnational-violent-non-state-actors-a-case-study-of-the-Primeiro-Comando-da-Capital-PCC.pdf
[36] https://americasquarterly.org/article/new-aq-the-pandemics-big-winner-transnational-crime/
[37] https://www.unodc.org/documents/data-and-analysis/covid/RB_COVID_organized_crime_july13_web.pdf
[38] https://insightcrime.org/brazil-organized-crime-news/family-of-the-north-fdn/
[39] https://www.europol.europa.eu/sites/default/files/documents/Europol_OrgCrimeReport_web-final_0.pdf
[40] https://foreignpolicy.com/2019/08/08/brazilian-organized-crime-is-all-grown-up/
[41] https://www.osac.gov/Content/Report/e2e8a425-32bf-45f5-aa49-18aceb1e211e
[42] https://americasquarterly.org/article/the-other-mutating-virus-the-pandemic-and-organized-crime/
[43] https://insightcrime.org/news/dirty-business-smuggling-pipeline-carrying-mercury-amazon/

STAYING AHEAD OF SERIOUS AND ORGANIZED CRIME

It's always been up to law enforcement and security organizations to stay one step ahead of the criminals. In recent years, agencies have purchased a variety of solutions, each addressing a specific threat.

Today, the security landscape is changing, with the biggest shift being the growing challenge presented by big data. Essentially, current technology provides more data than ever before, but without the capacity to integrate and analyze that data and produce meaningful conclusions, the capabilities themselves are next to useless.



Law enforcement and security organizations must collect and analyze numerous types of data on an ongoing basis including:

- Investigation reports, complaints, witness interviews
- Suspect information from official and state database
- Registries related to commercial companies, vehicles, and real estate
- Financial transactions and financial statements
- Audio and video files
- Web and social data
- Situational data from safe city and CCTV
- Lawful interception recordings

When all this data is scaled massively and siloed or fragmented across different departments, the only coherent solution that can help these organizations keep up with the pace of technology is an open suite of software that not only addresses individual use cases but also works together to provide a comprehensive umbrella. Let's look at five important use cases where technology is aiding law enforcement and security organizations and giving them an edge over criminals.

LAWFUL INTERCEPTION

Gathering telecommunications and telephone evidence in compliance with lawful interception-capability requirements can give your organization a foot in the door. This type of interception can quickly yield an overwhelming amount of data. Therefore, along with tools that let you comply with court-compliant evidence collection, you will need the ability to analyze data you are collecting in real time, coupled with quick-to-grasp visualizations and actionable insights to help you move investigations forward fast.

WEB INTELLIGENCE

The information you need for your investigation is out there—with so many transnational crime organizations using social media, data is literally just waiting to be found. But manually tracking it all down and putting the pieces together to identify suspects and threats is time-consuming, if not completely impossible. Today, law enforcement and security organizations are using artificial intelligence and machine learning to surface critical insights across all media types and derive actionable intelligence from across the web. How? These tools use a sophisticated mixture of textual analytics, image and video analytics, face recognition, and grouping, along with speech-to-text transcriptions, providing more accurate and unparalleled intelligence from the open and dark web in just a fraction of the time agencies typically take to gather such data. With cutting-edge web intelligence, you can build suspect profiles, uncover links between criminal and terror networks, generate evidence, and detect threats; you can even engage targets securely and anonymously, turbo-charging your investigation.

CYBER THREAT INTELLIGENCE

Since so much crime today is cyber-enabled, obtaining tactical, operational, and strategic intelligence can help thwart crime as it's being planned or taking place. With threat actors moving quickly online, you need fast insights that let you respond quickly and build organizational resilience. Manually, it's almost impossible to know where the potential attackers are, what tools they use, and most importantly, what they're planning. Proactive and analytics-driven intelligence tools empower security teams, handing them the ability to analyze events as they take place across clear, deep, and dark web sites; closed forums; social networks; and messaging platforms. They can then accurately identify external threats with access to research capabilities, know-how, and threat-intelligence repositories and build a proactive cyber defense strategy with 24/7 monitoring that converts raw data into context-based and enriched actionable intelligence.

CRYPTOCURRENCY DE-ANONYMIZATION

With the rise in cryptocurrency use for illicit transactions around the globe, law enforcement and security teams need deeper intelligence. Especially when it comes to funding terror and organized crime, intelligence tools that apply advanced analytical techniques, such blockchain analytics, open sources (OSINT), and lawful interception (LI), can help de-anonymize these transactions, tame the “Wild West” factor, and help teams track and trace even these covert transactions. These tools help build intelligence over time by clustering and visualizing historical and future data based on neighboring and connected suspects or entities of interest.

ANALYTICS & DATA FUSION

In the real world, data isn’t always neat and tidy. With intelligence arriving in a wide variety of formats, ranging from text, video, and audio to maps and statistics, and from a massive range of sources, including financial records, cyber, WEBINT, forensics, government databases, and more, the data is surely out there—but is difficult to piece together meaningfully. In these situations, thinking out of the box is not just a nice-to-have—it’s a critical necessity to gain an edge. Releasing data from silos helps law enforcement and security teams make connections and identify factors they would probably overlook using conventional means.

SITUATIONAL INTELLIGENCE

When complex situations are emerging in real time, law enforcement and security organizations need insights that help them move as quickly and safely as possible. Data collection is the key to any intelligence-led law enforcement approach, and this is even more true with developing situations. A number of products are available today that are targeted to specific situations and needs, such as video command and control, real-time situational awareness, and incident management and response, all of which can be combined with AI and machine learning to quickly highlight crucial data and patterns.

TURNING DATA INTO INSIGHTS

When it comes to staying ahead of serious and organized crime, Cognyte provides a broad range of solutions tailor-made for law enforcement and security organizations, helping you turn data into insights.

Cognyte's open-architecture analytics platform scales to meet your needs and the demands of the big data at your fingertips.

In countries all over the world, over 1,000 customers at government and enterprise levels are using Cognyte to accelerate their investigations, successfully identifying, neutralizing, and preventing national, corporate, and cyber threats.

Cognyte's solutions integrate AI, offering up lightning-speed intelligence, with machine learning for increasingly accurate performance. With the ability to fuse data and identify patterns and connections across time and space, your team gains authentic insights that let you make the right move at the right time.

For a comprehensive security analytics solution that makes your team more effective, contact us

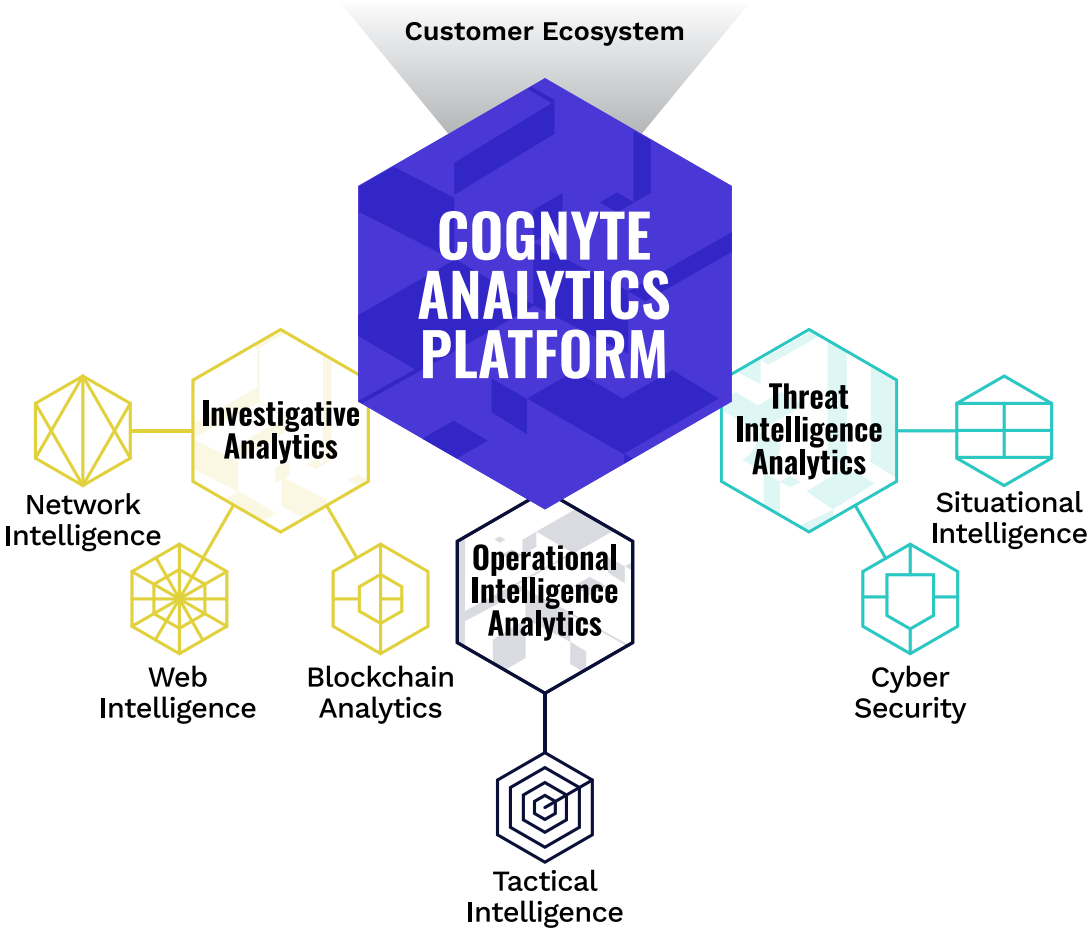
Cognyte

Formerly a Verint company

ABOUT COGNYTE SOFTWARE LTD.

Cognyte is a global leader in security analytics software that empowers governments and enterprises with Actionable Intelligence for a safer world. Our open software fuses, analyzes and visualizes disparate data sets at scale to help security organizations find the needles in the haystacks. Over 1,000 government and enterprise customers in more than 100 countries rely on Cognyte's solutions to accelerate security investigations and connect the dots to successfully identify, neutralize, and prevent threats to national security, business continuity and cyber security.

COGNYTE.COM



Click the diagram for more information.