VCIS Geo-Location Intelligence: A Dynamic Solution to Combat TBML and TBTF Schemes between Europe, West Africa and the Gulf Region

Intelligence de Géolocalisation VCIS: Une Solution Dynamique pour Lutter Contre les Schémas TBML et TBTF entre l'Europe, l'Afrique de l'Ouest et la Région du Golfe

Unlike traditional money laundering and terrorism financing, TBML and TBTF exploit global trade networks to move funds while appearing legitimate. These methods challenge law enforcement and regulators, requiring dynamic solutions to improve investigations and uncover links between criminals and trade companies.

The supervisory authorities and law enforcement agencies that are facing high risk TBML-TBTF schemes need to implement VCIS to increase the effectiveness of the investigations, face potential threats, and plug vulnerabilities.

Contrairement aux méthodes traditionnelles de blanchiment d'argent et de financement du terrorisme, le TBML et le TBTF exploitent la complexité des réseaux commerciaux mondiaux pour transférer des fonds tout en créant l'apparence d'activités légitimes, ce qui représente un défi majeur pour les forces de l'ordre et les régulateurs.

Face aux programmes TBML-TBTF à haut risque, les autorités de contrôle et les forces de l'ordre doivent déployer le VCIS pour renforcer l'efficacité des enquêtes, anticiper les menaces potentielles et identifier les vulnérabilités avec précision.

Table des Matières

What is Trade-Based Money Laundering (TBML)?

Trade-Based Money Laundering is a sophisticated and increasingly prevalent method used by criminal organizations and individuals to disguise illicit funds through international trade transactions in a way that avoids financial transparency regulations. The methods used to falsify trade documents and adjust pricing to benefit the criminal entity are often indirect. This makes TBML a preferred money laundering technique that is difficult to track.

It's estimated that up to $2 trillion of the annual $20 trillion in global trade is laundered money. This type of customs fraud can be conducted anywhere in the world. However, many laundered funds are routed through jurisdictions with weak financial regulations.

Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) initiatives have proven effective at decreasing the number of fraudulent financial transactions. However, this increased scrutiny may have funneled a certain portion of laundering activities through trading channels.

While it is an inherently difficult metric to measure, the Financial Action Task Force (FATF) and the International Monetary Fund (IMF) both estimate that the total

Qu'est-ce que le blanchiment d'argent basé sur le commerce (TBML) ?

Le blanchiment d'argent basé sur le commerce (TBML) est une méthode sophistiquée permettant aux organisations criminelles de dissimuler des fonds illicites via des transactions commerciales internationales. En falsifiant des documents et en manipulant les prix ou quantités déclarées, les criminels contournent les réglementations financières tout en créant une apparence de légitimité. Cette complexité rend le TBML difficile à détecter et à combattre pour les autorités de contrôle.

On estime que sur les 20 000 milliards de dollars du commerce mondial annuel, près de 2 000 milliards proviennent d'activités de blanchiment d'argent. Cette fraude douanière, omniprésente à l'échelle mondiale, est facilitée par le passage des fonds illicites à travers des juridictions aux régulations financières laxistes.

Les initiatives de lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CTF) ont permis de réduire les transactions financières frauduleuses. Cependant, cette surveillance renforcée semble avoir déplacé une partie des activités de blanchiment vers les circuits commerciaux.

Bien que difficile à quantifier précisément, le Groupe d'action financière (GAFI) et le Fonds monétaire international (FMI) estiment que le

value of money laundering in the world lies somewhere between 2% and 5% of the global GDP.

Due to the large volumes of global trade and vast geographic distances involved, TBML is often considered to be the most elusive form of converting illicit money into commercially acceptable cash.

Today, global customs authorities struggle to control the exploitation of international trade for laundering criminally gained money, mainly linked to narcotics, bribery, corruption, human trafficking, illegal weapon trade, and other societal malpractices.

Before delving into the Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) measures that regulators use to protect against TBML and TBTF, it is important to understand the common methodologies and risk indicators.

blanchiment d'argent représente entre 2 et 5 % du PIB mondial.

En raison des volumes élevés du commerce mondial et des distances géographiques impliquées, le blanchiment d'argent basé sur le commerce (TBML) est considéré comme l'une des méthodes les plus difficiles à détecter pour convertir des fonds illicites en ressources commercialement acceptées. Aujourd'hui, les autorités douanières mondiales rencontrent des défis majeurs pour contrôler l'utilisation du commerce international dans le blanchiment d'argent, particulièrement lié aux drogues, à la corruption, au trafic d'êtres humains, au commerce illégal d'armes et à d'autres pratiques criminelles.

Avant de discuter des mesures de lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CFT) mises en place par les régulateurs pour contrer le TBML et le TBTF, il est essentiel de comprendre les méthodologies et les principaux indicateurs de risque utilisés dans ce domaine.

The Common Economic Sectors & Products at Risk of TBML

The following information provides a brief overview of the common economic sectors and products that are vulnerable to Trade-Based Money Laundering (TBML). Please note that this list is not exhaustive and serves to give an overview of the current risk, highlighting the diverse sectors and products that criminals exploit. Private sector respondents have pointed out that criminals tend to target sectors, products, or businesses where there are gaps in customer due diligence and inconsistent application of know-your-customer processes across different jurisdictions. This risk is further exacerbated by a limited understanding of TBML.

TBML poses a threat to a wide range of economic sectors, including both high-value, low-volume sectors or products (e.g., precious metals) and low-value, high-volume sectors or products (e.g., second-hand textiles). Criminals use these sectors to launder the proceeds of their illegal activities. Certain common themes conducive to TBML exploitation have been identified, including:

- Goods with significant pricing margins.
- Goods with extended trade cycles involving shipping across multiple jurisdictions.
- Goods that are challenging for customs authorities to examine.

Les secteurs Économiques Communs et les Produits à Risque du TBML

Les informations suivantes offrent un aperçu des secteurs économiques et des produits couramment vulnérables au blanchiment d'argent basé sur le commerce (TBML). Cette liste, bien que non exhaustive, met en évidence les risques actuels et les secteurs ciblés par les criminels. Selon les observations des répondants du secteur privé, les criminels privilégient des secteurs, produits ou entreprises où des lacunes existent dans la diligence raisonnable et l'application des processus de connaissance de la clientèle, notamment dans des juridictions aux pratiques inégales. Ce risque est amplifié par une compréhension limitée du phénomène TBML.

Le TBML représente une menace pour divers secteurs économiques, englobant à la fois des secteurs à grande valeur et faible volume (par exemple, les métaux précieux) et des secteurs à faible valeur et volume élevé (par exemple, les textiles d'occasion). Les criminels exploitent ces secteurs pour dissimuler les produits de leurs activités illicites. Plusieurs thèmes communs favorisant l'exploitation du TBML ont été identifiés, notamment:

- Marchandises avec des marges de prix importantes.
- Marchandises avec des cycles étendus impliquant une expédition à travers plusieurs juridictions.
- Marchandises difficiles à examiner pour les autorités douanières.

Supply chains involving lower-value goods are particularly susceptible to full ownership by criminal organizations or PML (Professional Money Launderer) networks. The setup costs for such supply chains are lower, attracting less scrutiny from authorities throughout the chain. Criminals can also supply multiple markets across different jurisdictions, reducing the risk of arousing suspicion of market saturation. For instance, repeatedly shipping a lower-value product like clothing to the same destination might not raise suspicions.
These factors create an environment conducive to the use of common TBML techniques. Criminal organizations may carry out legitimate shipments of goods like cosmetic products, generating valid documentation that they later misuse for phantom shipments. In some cases, the transactions may appear entirely legitimate, but the shipped products have little to no value and are discarded upon arrival (e.g., second-hand textiles).

When higher-value products are targeted, criminal organizations, or PMLs, tend to penetrate and misuse established supply chains. They may leverage struggling companies by becoming silent partners, using the businesses and their supply chain contacts to launder the proceeds of their illicit activities.

Les chaînes d'approvisionnement impliquant des biens à faible valeur sont particulièrement vulnérables aux manipulations par des organisations criminelles ou des réseaux de blanchiment d'argent professionnels (PML). En raison de leurs coûts de mise en place relativement bas, ces chaînes attirent moins l'attention des autorités à chaque étape. De plus, les criminels peuvent approvisionner plusieurs marchés dans différentes juridictions, minimisant ainsi le risque d'éveiller des soupçons de saturation. Par exemple, l'expédition répétée de produits à faible valeur, tels que des vêtements, vers la même destination pourrait passer inaperçue.

Ces facteurs favorisent l'exploitation des techniques TBML classiques. Dans certains cas, bien que les transactions paraissent légitimes, les produits expédiés ont une valeur négligeable voire nulle, étant souvent jetés à leur arrivée, comme c'est le cas avec des textiles d'occasion.

Lorsqu'ils ciblent des produits de grande valeur, les organisations criminelles, ou PML, exploitent souvent les chaînes d'approvisionnement existantes. Elles prennent avantage des entreprises en difficulté en devenant des partenaires discrets, utilisant ces entreprises et leurs réseaux dans la chaîne pour dissimuler les fonds issus de leurs activités illicites.

Common Trade-Based Money Laundering Techniques

Below are some of the most common techniques criminals use to conduct trade-based money laundering activities.

- **Over-Invoicing & Under-Invoicing of Products and Services**

One of the most prevalent TBML techniques, over-invoicing or under-invoicing can transfer value between exporters and importers. If two parties are owned by the same corporation or agree to collaborate for economic benefit, they can adjust the price of goods or services to achieve unfair market advantages.
In over-invoicing, the exporter sets a price above the fair market rate to receive more money from the importer. Conversely, in under-invoicing, the exporter sets a price below the fair market rate so that the importer obtains a higher value upon selling the goods or services.

- **Issuing Multiple Bills for Goods and Services**

Money launderers sometimes operate by issuing multiple bills for the same commercial transaction. In addition, they may conduct the transactions through different financial institutions to disguise their activities.

Techniques Courantes de Blanchiment d'Argent Basées sur le Commerce

Voici les principales techniques utilisées par les criminels pour le blanchiment d'argent basé sur le commerce.

- **Surfacturation et sous-facturation des produits et services**

L'une des techniques les plus courantes du TBML, la surfacturation ou la sous-facturation, permet de transférer de la valeur entre exportateurs et importateurs. Si les deux parties appartiennent à la même entreprise ou s'entendent pour collaborer, elles peuvent ajuster le prix des biens ou des services pour obtenir des avantages commerciaux injustes. Dans le cas de la surfacturation, l'exportateur fixe un prix supérieur au taux du marché pour recevoir plus d'argent de l'importateur. À l'inverse, en cas de sous-facturation, l'exportateur fixe un prix inférieur au taux du marché, permettant ainsi à l'importateur d'obtenir une valeur plus élevée lors de la revente.

- **Émettre plusieurs factures pour des biens et des services**

Les blanchisseurs d'argent peuvent parfois émettre plusieurs factures pour une même transaction commerciale, ou effectuer des paiements via diverses institutions financières afin de dissimuler leurs activités. Bien qu'il puisse exister des raisons légitimes pour des paiements multiples concernant les mêmes

There are legitimate justifications for multiple payments for the same goods or services. So, it can be challenging to detect criminal enterprises using this technique.

- **Fraudulent Quantities of Shipped Products and Services**

Another common technique is changing the quantities of goods or services provided. Money launderers can conceal illegal payments and funds by inflating or deflating these numbers. In some cases, no goods are shipped at all.

- **False Descriptions of Goods and Services**

Descriptions of goods and services can be misconceived to falsify billing documents. Sometimes, money launderers misrepresent the quality or type of items provided. For example, fake goods may be billed as more expensive, genuine products.

Descriptions of goods and services can be misconceived to falsify billing documents. Sometimes, money launderers misrepresent the quality or type of items provided. For example, fake goods may be billed as more expensive, genuine products.

biens ou services, cette méthode rend la détection des pratiques criminelles plus complexe et nécessite une vigilance accrue pour identifier les transactions suspectes.

- **Quantités frauduleuses de produits et services expédiés**

Une autre technique courante consiste à modifier les quantités de biens ou services, permettant de masquer des paiements illicites, parfois sans expédition réelle de marchandise.

- **Fausses descriptions de biens et de services**

Les blanchisseurs d'argent manipulent fréquemment les descriptions de biens et de services pour falsifier les factures, en modifiant la qualité ou le type des produits. Par exemple, des articles contrefaits peuvent être facturés comme des produits authentiques et de plus grande valeur.

Les descriptions de biens et de services peuvent être intentionnellement modifiées pour altérer les documents de facturation. Les blanchisseurs d'argent ajustent souvent la qualité ou le type des articles, par exemple en facturant des produits contrefaits comme des biens authentiques et de valeur supérieure.

What is Trade-Based Terrorist Financing (TBTF)?

Trade-Based Terrorist Financing (TBTF) is a specific form of financial support used by terrorist organizations to fund their activities. It shares similarities with Trade-Based Money Laundering (TBML), but it has a crucial distinction: in TBTF, the funds or value moved can originate from both legitimate and illegitimate sources. This key difference adds complexity to the detection and disruption of TBTF.

In TBTF, the objective is to obscure the movement of funds by leveraging trade transactions. Just like in TBML, terrorists may use various techniques such as over or under-invoicing goods, misrepresenting the nature of the transactions, or employing multiple layers of trade to hide the origin of the funds. However, the funds involved in TBTF may be a combination of legitimately acquired money and money obtained through illegal or illicit activities.

The definition of TBTF, therefore, is the practice of concealing the movement of value through trade transactions with the intention of financing terrorism. It encompasses the use of both legitimate and illegitimate sources of funds, making it more challenging for authorities to

Qu'est-ce que Financement du Terrorisme Basé sur le Commerce (TBTF) ?

Le financement du terrorisme basé sur le commerce (TBTF) est une méthode spécifique utilisée par les organisations terroristes pour financer leurs activités, similaire au blanchiment d'argent basé sur le commerce (TBML). Cependant, une distinction majeure réside dans le fait que les fonds ou la valeur transférés dans le cadre du TBTF peuvent provenir à la fois de sources légitimes et illégitimes, ce qui rend sa détection et son interdiction particulièrement complexes.

Dans le cadre du financement du terrorisme basé sur le commerce (TBTF), l'objectif est de dissimuler les flux financiers en exploitant les transactions commerciales. À l'instar du blanchiment d'argent basé sur le commerce (TBML), les groupes terroristes recourent à des techniques telles que la surfacturation, la sous-facturation, la falsification de la nature des transactions ou l'utilisation de chaînes commerciales complexes pour dissimuler l'origine des fonds. Cependant, dans le TBTF, les fonds peuvent provenir à la fois de sources légitimes et de ressources issues d'activités illégales ou illicites.

Le financement du terrorisme basé sur le commerce (TBTF) désigne la pratique de dissimuler des mouvements de valeur à travers des transactions commerciales pour financer des activités terroristes.

identify and disrupt such financial activities.

By disguising the origin and movement of funds, TBTF allows terrorist organizations to finance their operations while evading detection and potentially using the cover of legitimate trade activities to facilitate their illicit financial operations.

Given the complexity and diversity of global trade, combating TBTF requires close cooperation and intelligence sharing among law enforcement agencies, financial institutions, and other stakeholders to effectively monitor and prevent the flow of funds to terrorist groups.

Cette méthode implique l'utilisation de fonds provenant de sources à la fois légitimes et illégitimes, compliquant ainsi la détection et l'interruption de ces activités par les autorités.

Le TBTF permet aux organisations terroristes de dissimuler l'origine et le flux des fonds, facilitant ainsi le financement de leurs opérations tout en évitant la détection. Cette pratique exploite souvent des activités commerciales légitimes comme couverture pour soutenir des transactions financières illicites.

Compte tenu de la complexité et de la diversité du commerce mondial, la lutte contre le TBTF nécessite une coopération étroite et un partage de renseignements entre les organismes chargés de l'application des lois, les institutions financières et les autres parties prenantes afin de surveiller et d'empêcher efficacement le flux de fonds vers les groupes terroristes.

Products commonly at risk of TBML

- **Gold, Precious Metals and Minerals**

Gold and other precious metals and minerals are frequently exploited in TBML schemes. They are used not only as commodities to move value but also as a proxy for cash within the money laundering process.

- **Auto Parts and Vehicles**

TBML schemes involve the exploitation of auto parts and vehicles, including the trade in second-hand cars or luxury vehicles. In some cases, damaged cars are transported from one jurisdiction to another and then sold in a legitimate market after repair. Criminal groups often declare a lower value at transshipment points to deceive law enforcement, using alternate networks of companies in different jurisdictions to route payments.

- **Agricultural Products and Foodstuffs**

Agricultural products, particularly highly perishable items like fresh fruits and vegetables, are exploited in TBML schemes. These low-value, high-volume products are not easily affected by market saturation due to their perishable nature. Criminal groups use legitimate supply chains to introduce illicit cash into the

Produits Couramment Exposés au Risque de TBML

- **Or, métaux précieux et minéraux**

L'or et d'autres métaux et minéraux précieux sont couramment utilisés dans les programmes TBML. Ces actifs servent à la fois à transférer de la valeur et à remplacer les liquidités dans le processus de blanchiment d'argent.

- **Pièces automobiles et véhicules**

Les programmes TBML exploitent les pièces automobiles et véhicules, y compris le commerce de voitures d'occasion et de luxe. Parfois, des voitures endommagées sont transportées, réparées, puis revendues sur des marchés légitimes. Les groupes criminels sous-déclarent la valeur lors des transbordements pour tromper les autorités, utilisant des réseaux d'entreprises dans différentes juridictions pour faciliter les paiements.

- **Produits agricoles et denrées alimentaires**

Les produits agricoles, notamment les fruits et légumes frais, sont utilisés dans les programmes TBML. Leur faible valeur et leur volume élevé les rendent moins vulnérables à la saturation du marché. Les groupes criminels exploitent les chaînes d'approvisionnement légitimes pour injecter des fonds illicites dans le système financier, contournant ainsi les méthodes classiques du TBML.

financial system, bypassing common TBML techniques.

- **Clothing and Second-Hand Textiles**

Similar to foodstuffs, clothing and second-hand textiles are attractive for TBML due to their low-value, high-volume nature, allowing for an extended supply chain. The significant price variability makes them appealing for misrepresenting prices to facilitate money laundering activities.

- **Portable Electronics (Mobile Phones, Laptops, etc.)**

Portable electronics, such as mobile phones and laptops, are also targeted in TBML schemes. Criminal groups deliberately misrepresent and undervalue these items, providing an opportunity to move substantial criminal proceeds discreetly.

In all these cases, TBML involves manipulating trade transactions to obscure the origins and true value of illicit funds, making it challenging for law enforcement authorities to detect and investigate the illicit activities.

- **Vêtements et textiles d'occasion**

Les vêtements et textiles d'occasion, similaires aux produits alimentaires, sont prisés dans le cadre du TBML en raison de leur faible valeur et de leurs volumes élevés, permettant ainsi une chaîne d'approvisionnement étendue. La grande variabilité des prix les rend également propices à la manipulation des prix pour faciliter les activités de blanchiment d'argent.

- **Appareils portables (téléphones mobiles, ordinateurs portables, etc.)**

Les appareils électroniques portables, tels que les téléphones mobiles et les ordinateurs portables, sont également utilisés dans les programmes TBML. Les groupes criminels manipulent et sous-évaluent intentionnellement ces produits, facilitant ainsi le transfert discret de fonds illicites.

Dans ces cas, le TBML consiste à falsifier les transactions commerciales pour dissimuler l'origine et la véritable valeur des fonds, rendant ainsi la détection et l'enquête par les autorités plus complexes.

How can geospatial data & location intelligence serve fighting TBML?

Geospatial data and location intelligence can play a significant role in fighting Trade-Based Money Laundering by providing valuable insights and enhancing the ability of authorities to detect and prevent illicit financial activities. Here are some ways in which geospatial data and location intelligence can be utilized:

- **Identifying High-Risk Areas**

Geospatial data can help identify regions or specific areas with a higher likelihood of being involved in TBML activities. By analyzing trade patterns, transaction flows, and historical data, authorities can pinpoint regions that are more vulnerable to TBML.

- **Tracking Trade Routes**

Location intelligence can assist in monitoring and analyzing trade routes, especially in regions known for illegal activities or financial secrecy. Suspicious trade corridors and routes can be closely monitored to detect anomalies or patterns indicative of TBML.

- **Integration with Other Data Sources**

Geospatial data can be integrated with other datasets, such as financial transactions, ownership records, and shipping data, to create a more comprehensive view of potential TBML

Comment les Données Géospatiales Aident-Elles à Lutter Contre le TBML?

Les données géospatiales et l'intelligence de localisation sont essentielles dans la lutte contre le blanchiment d'argent basé sur le commerce, en fournissant des informations clés pour améliorer la détection et la prévention des activités financières illicites. Voici quelques approches pour exploiter ces données efficacement:

- **Identifier les zones à haut risque**

Les données géospatiales permettent d'identifier les zones à risque accru de TBML. En analysant les modèles commerciaux, les flux transactionnels et les données historiques, les autorités peuvent cibler les régions les plus vulnérables au blanchiment d'argent basé sur le commerce.

- **Suivi des routes commerciales**

L'intelligence géographique permet de surveiller et d'analyser les routes commerciales, notamment dans les régions à risque élevé où la confidentialité financière prédomine. Elle facilite l'identification d'anomalies ou de schémas susceptibles de signaler des activités de TBML.

- **Intégration avec d'autres sources de données**

Les données géospatiales peuvent être combinées avec d'autres sources, telles que les transactions financières, les enregistrements de propriété et les données d'expédition, afin de fournir une vision

activities and help in conducting risk assessments.

- **Trade Discrepancies**

Geospatial data can help identify discrepancies in trade data, such as mismatched shipping routes, quantities, or values of goods. These discrepancies can be indicative of trade manipulation used in TBML schemes.

- **Cross-Border Transaction Analysis**

Geospatial data can aid in analyzing cross-border transactions and identifying transactions that might involve suspicious jurisdictions or entities. By tracking the movement of goods and funds across borders, authorities can uncover potential TBML schemes.

- **Visualization of Trade Networks and links with criminals**

Location intelligence tools can create visual representations of trade networks and financial flows, making it easier to identify complex trade relationships and potential money laundering activities within those networks.

- **Monitoring Ports and Free Trade Zones**

Geospatial data can be used to monitor activities in ports and free trade zones, which are known to be vulnerable to money laundering due to their cross-border nature and lower regulatory oversight.

complète des activités suspectes de TBML et de faciliter les évaluations des risques.

- **Écarts commerciaux**

Les données géospatiales permettent d'identifier des anomalies dans les itinéraires maritimes, les quantités ou les valeurs des marchandises, ce qui peut indiquer des manipulations commerciales associées au TBML.

- **Analyse des transactions transfrontalières**

Les données géospatiales permettent d'analyser les transactions transfrontalières et d'identifier les échanges impliquant des juridictions ou des entités à risque. En suivant les flux de biens et de fonds à travers les frontières, les autorités peuvent détecter d'éventuelles activités liées au TBML.

- **Visualisation des réseaux commerciaux et des liens avec les criminels**

Les outils de géolocalisation permettent de visualiser les réseaux commerciaux et les flux financiers, facilitant ainsi l'identification des relations complexes et des activités potentielles de blanchiment d'argent au sein de ces réseaux.

- **Surveillance des ports et des zones franches**

Les données géospatiales peuvent être utilisées pour surveiller les activités dans les ports et zones franches, des zones vulnérables au blanchiment d'argent en raison de leur nature transfrontalière et de la régulation limitée.

- **Predictive Analytics**

Location intelligence, when combined with advanced analytics and machine learning algorithms, can enable the development of predictive models to anticipate potential TBML activities and facilitate proactive enforcement measures.

- **Collaboration and Information Sharing**

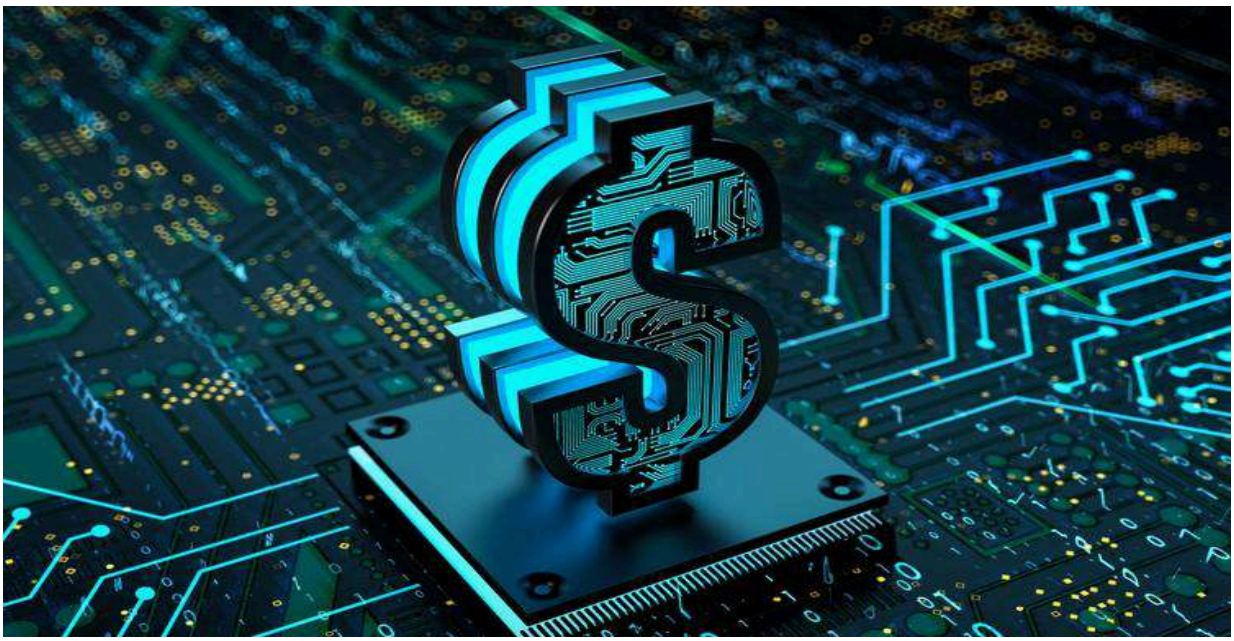
Geospatial data and location intelligence can be shared across agencies and countries to foster better collaboration in tackling TBML, as money laundering often involves international networks.

- **Analyse prédictive**

L'intelligence géographique, associée à des analyses avancées et des algorithmes d'apprentissage automatique, permet de développer des modèles prédictifs pour anticiper les activités de TBML et favoriser des actions proactives d'application.

- **Collaboration et partage d'informations**

Les données géospatiales et les informations de localisation peuvent être partagées entre agences et pays, facilitant ainsi une collaboration renforcée dans la lutte contre le TBML, en raison de la nature transnationale de ces activités criminelles.



Case Study

In February 2017, a significant event occurred at the Nigeria-Niger border, where the Nigerian authorities arrested four individuals while attempting to cross the border through an illegal path. Their mode of transportation consisted of two 4x4 jeeps. Upon their arrest, law enforcement discovered a substantial cache of weapons in their possession, as well as a considerable sum of money amounting to approximately 4 million dollars. Additionally, the authorities seized the four phones that belonged to these individuals.

The primary suspicion surrounding these individuals was their alleged connection to the funding of the Boko Haram terrorist organization. Boko Haram, a notorious extremist group based in Nigeria, has been responsible for numerous acts of violence and terrorism in the region. Their activities have led to widespread instability and fear.
The four suspected persons refused to cooperate with the investigators, confess the final destination of their smuggling activities, and divulge their accomplices.

In order to uncover and monitor such criminal activities effectively, the concept of the "VCIS solution" comes into play. The VCIS features allow law enforcement to reveal the links between criminals,

Étude de Cas

En février 2017, les autorités nigérianes ont arrêté quatre individus tentant de traverser illégalement la frontière entre le Nigeria et le Niger à bord de deux jeeps 4x4. Lors de l'intervention, les forces de l'ordre ont découvert une cache d'armes et une somme d'environ 4 millions de dollars en espèces. Les téléphones des suspects ont également été saisis, fournissant des éléments cruciaux pour l'enquête sur d'éventuelles connexions avec des activités criminelles transnationales et les communications liées à cette tentative de passage illégal.

Les principaux soupçons entourant ces individus concernaient leur lien présumé avec le financement de l'organisation terroriste Boko Haram. Boko Haram, un groupe extrémiste notoire basé au Nigeria, est responsable de nombreux actes de violence et de terrorisme dans la région. Leurs activités ont provoqué une instabilité et une peur généralisées. Les quatre suspects ont refusé de coopérer avec les enquêteurs, de révéler la destination finale de leurs opérations de contrebande et de divulguer l'identité de leurs complices.

Pour détecter et surveiller efficacement ces activités criminelles, la solution VCIS joue un rôle clé. Grâce à ses fonctionnalités avancées, elle permet aux forces de l'ordre d'établir des liens entre les criminels, de suivre les flux

track the flow of weapons and illicit money, identify illegal smuggling paths, and find out the cooperation between organized crime syndicates, terrorist organizations, and trade companies to combat the TBML and TBTF schemes.

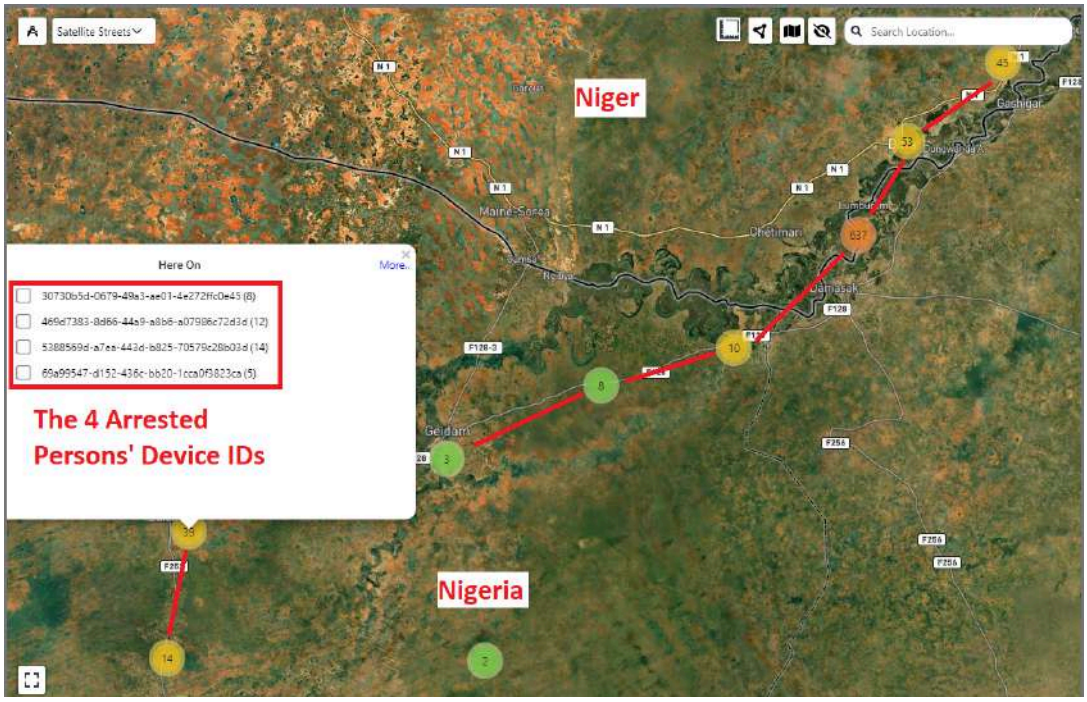
d'armes et de fonds illicites, d'identifier les itinéraires de contrebande et de révéler les collaborations entre syndicats du crime organisé, organisations terroristes et entités commerciales. Cette approche renforce la lutte contre les stratagèmes TBML et TBTF.

Chapter 1: Smuggling Pathways & Links to Organized Crime Groups

Executing a device history **DH** query for the four devices allowed us to discover that they are moving between the Alagarno forest (a region in the north east of Nigeria controlled by the fighters of Boko Haram) and the desert in Niger near Bilma through illegal paths, which indicates that they are involved in smuggling weapons, cash, and logistics for the benefit of a Boko Haram group. *(DH - Four Devices)*

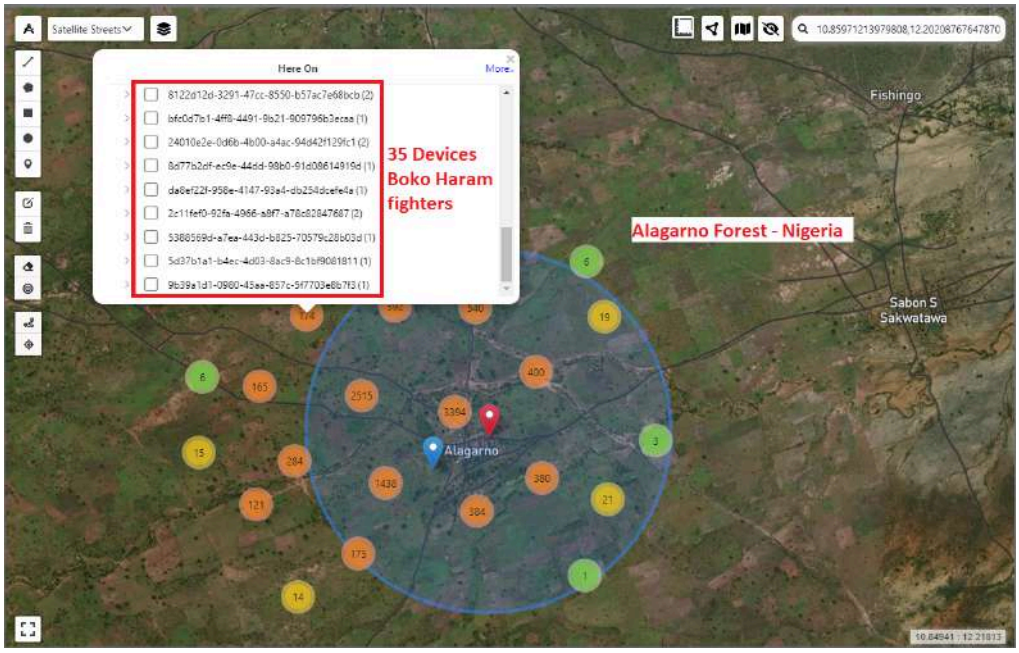
Chapitre 1: Voies de Passage Clandestin et Liens avec des Groupes du Crime Organisé

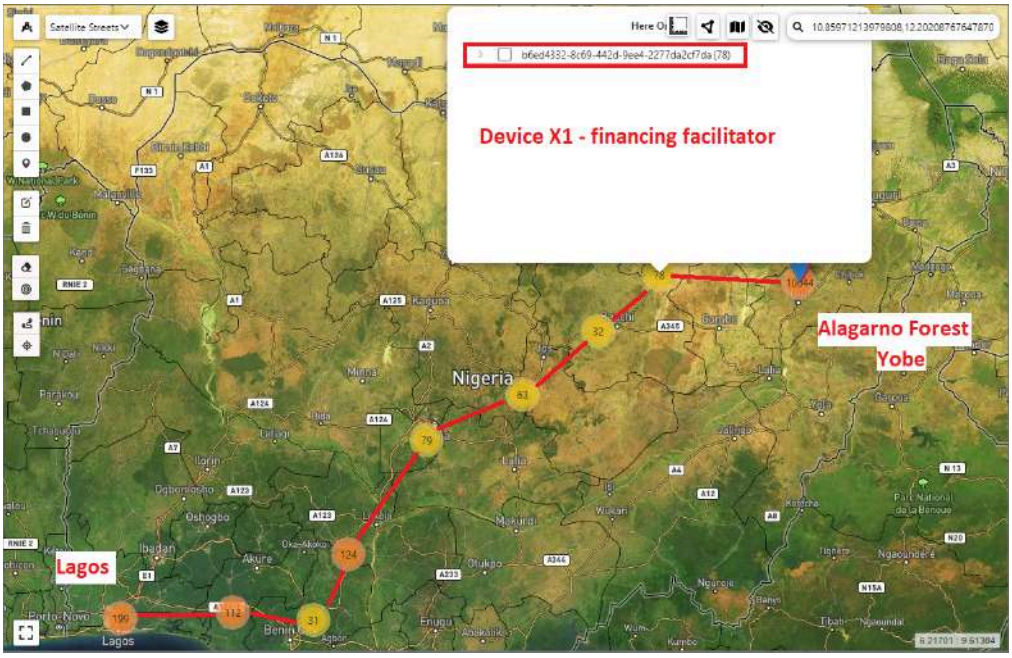
L'exécution d'une requête d'historique des appareils (DH) pour les quatre dispositifs a permis de découvrir qu'ils se déplacent entre la forêt d'Alagarno (une région du nord-est du Nigeria contrôlée par les combattants de Boko Haram) et le désert du Niger près de Bilma, en empruntant des chemins illégaux. Cela indique leur implication dans le trafic d'armes, d'argent liquide et de logistique au profit d'un groupe Boko Haram *(DH - quatre appareils)*



Executing a device history pattern **DHP** query in the Alagarno forest allows us to identify 35 devices in the same area, which probably belong to Boko Haram fighters. One of them is only moving between the Yobe district and Lagos, which probably belongs to a financing facilitator named X1, while the other devices don't have significant activities. This analysis permits us to discover the location of dormant terrorist cells.
(*DHP - Algarno Forest)*

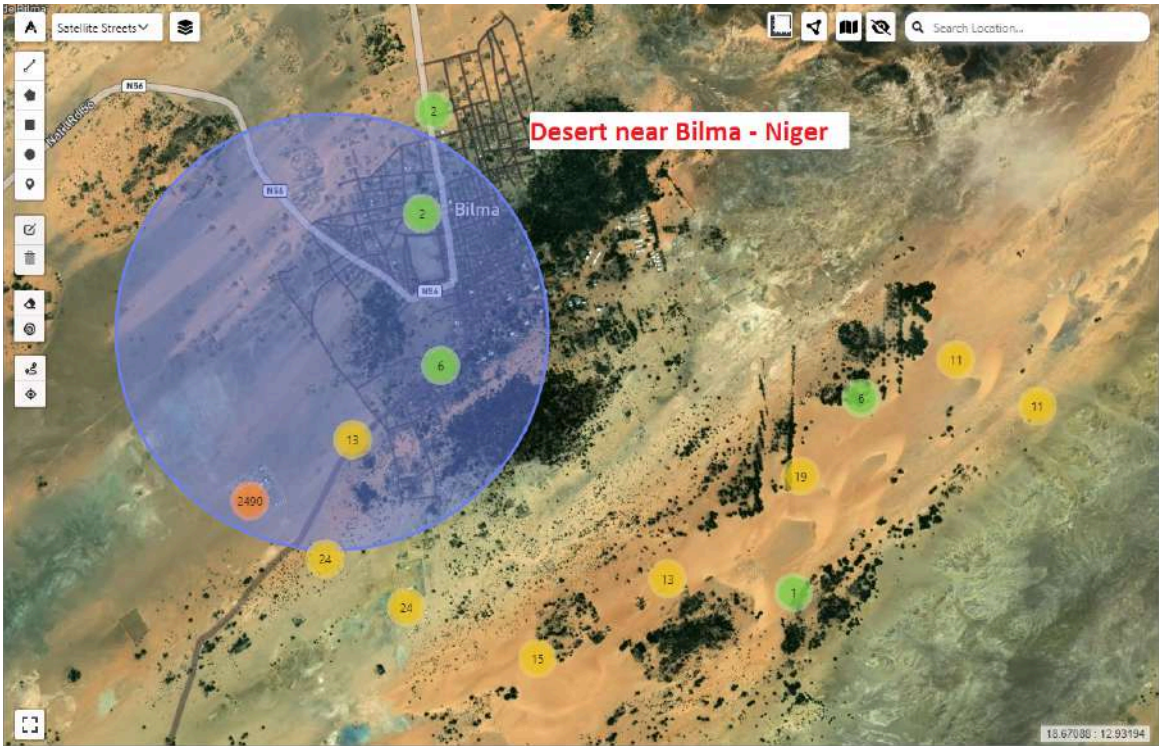
L'exécution d'un modèle historique de périphérique **DHP** dans la forêt d'Alagarno a permis d'identifier 35 dispositifs actifs dans cette zone, probablement associés aux combattants de Boko Haram. L'un de ces dispositifs se déplace exclusivement entre le district de Yobe et Lagos, suggérant un lien potentiel avec un facilitateur financier désigné X1. Les autres dispositifs présentent peu d'activité significative. Cette analyse permet d'identifier des cellules terroristes dormantes et de localiser leurs mouvements stratégiques. (*DHP - Algarno Forest)*

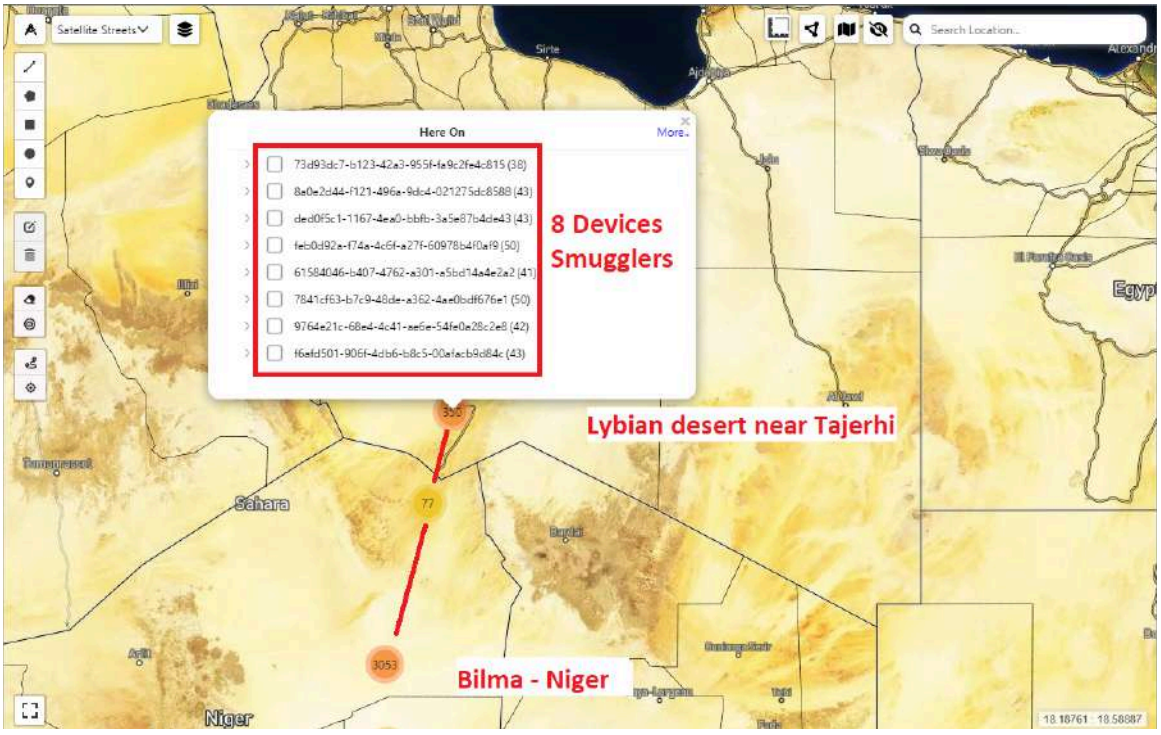


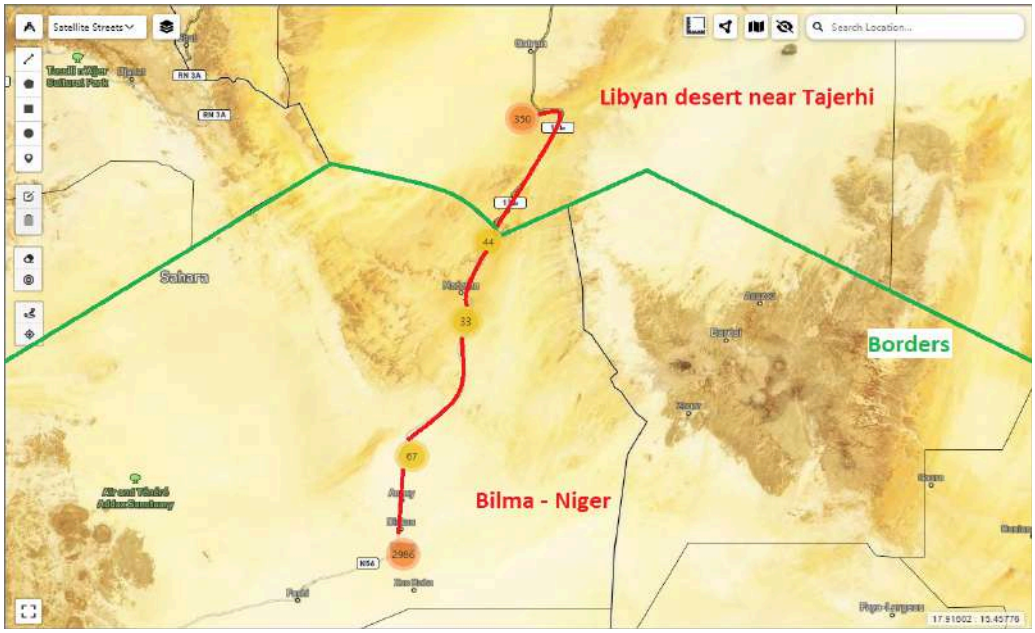


Executing a device history pattern **DHP** query in the desert near Bilma allows us to identify eight devices in the same area, which probably belong to smugglers. These eight devices are moving between Bilma and the Libyan desert near Tajerhi. *(DHP - Desert near Bilma)*

L'exécution d'un modèle d'historique de périphérique (DHP) dans le désert près de Bilma a permis d'identifier huit dispositifs actifs, probablement liés à des réseaux de passeurs. Ces dispositifs opèrent principalement entre Bilma et le désert libyen, près de Tajerhi, révélant des itinéraires de trafic transfrontalier. *(DHP - Désert près de Bilma)*



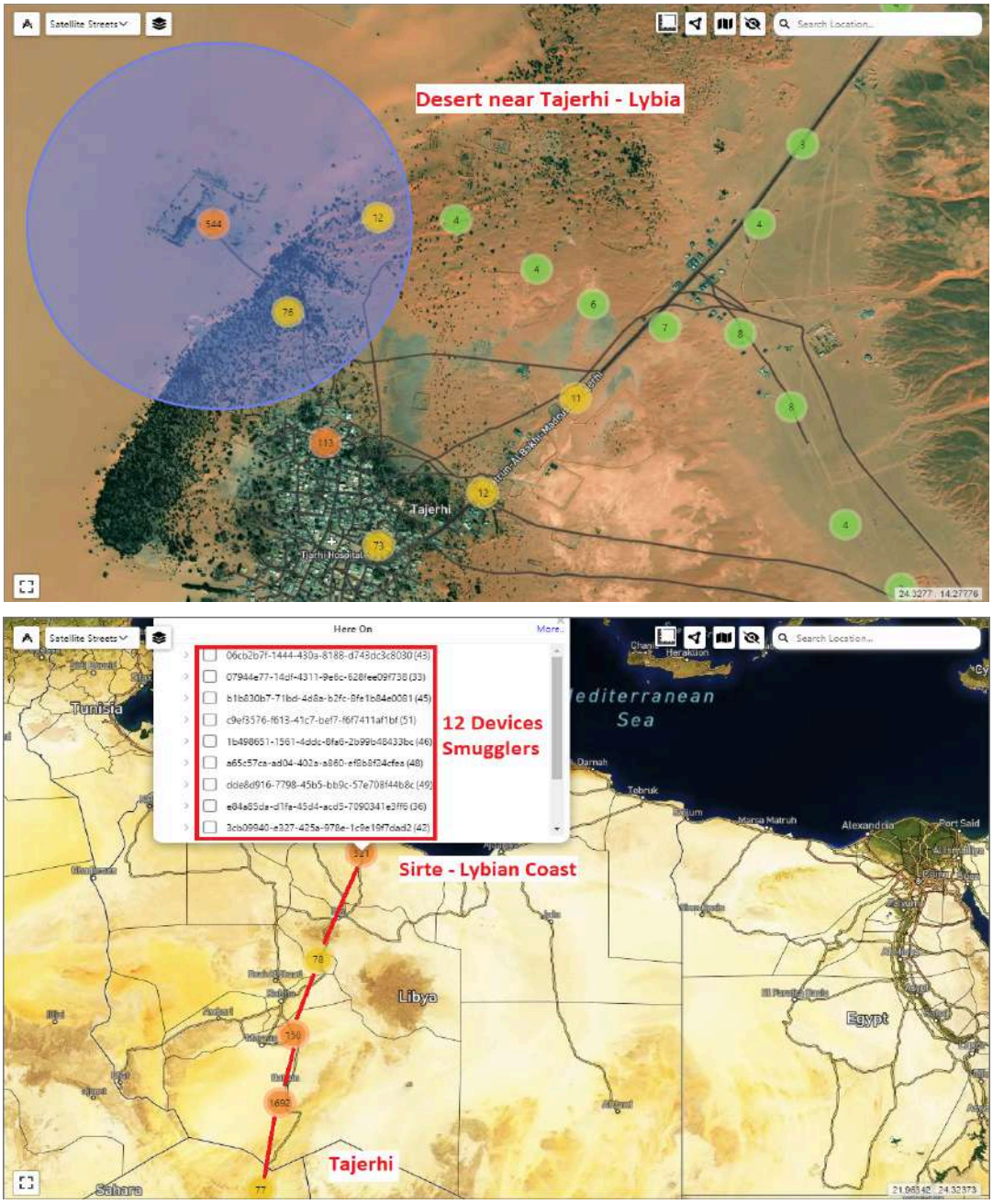




Trajectoire des 8 appareils entre Bilma et Tajerhi.

Executing a device history pattern **DHP** query in the desert near Tajerhi allows us to identify twelve devices in the same area, which also probably belong to smugglers. These twelve devices are moving between Tajerhi and Sirte on the Libyan coast.
(DHP - Tajerhi)

L'analyse d'un modèle d'historique de périphérique (DHP) dans le désert près de Tajerhi a identifié douze dispositifs, liés à des réseaux de passeurs. Ces dispositifs opèrent entre Tajerhi et Syrte, sur la côte Libyenne, révélant des itinéraires de trafic reliant le désert aux zones côtières stratégiques.
(DHP - Tajerhi)



Trajectoire des 12 appareils entre Tajerhi et Syrte

These analyses provide evidence on the paths used to smuggle weapons and cash to Boko Haram between Siret and Tajerhi in Libya, Bilma desert in Niger, and Alagarno forest for many of the individuals involved, who belong to several criminal organized groups.

Ces analyses apportent des preuves concrètes des itinéraires de contrebande utilisés pour acheminer armes et fonds vers Boko Haram. Elles révèlent des routes reliant Syrte et Tajerhi en Libye, le désert de Bilma au Niger et la forêt d'Alagarno au Nigeria, impliquant de nombreux individus affiliés à divers réseaux criminels organisés.

Chapter 2: TBTF scheme for Boko Haram & links with the ISIS group

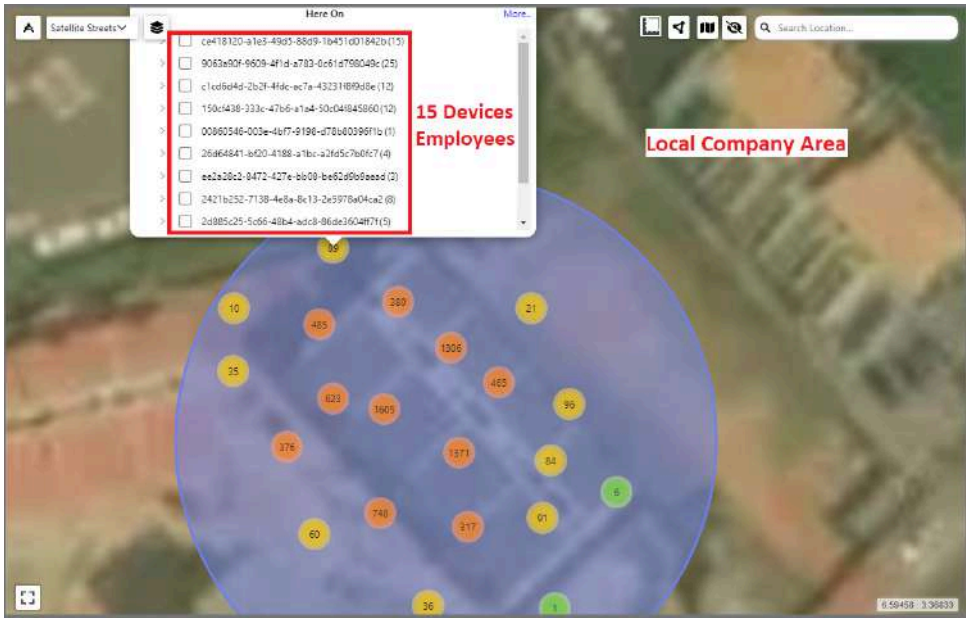
Executing a device history **DH** query for the financing facilitator device showed that he is moving between the forest in Yobe and Lagos and is frequently visiting a local trade company once per month before coming back to the forest.
(DH - Financing facilitator)

Chapitre 2: Programme TBTF pour Boko Haram et Liens avec le Groupe ISIS

Une requête d'historique de l'appareil DH a révélé que le dispositif utilisé par le facilitateur financier circule régulièrement entre la forêt de Yobe et Lagos, effectuant des visites mensuelles à une entreprise commerciale locale avant de retourner dans la forêt.
(DH - Financing facilitator)

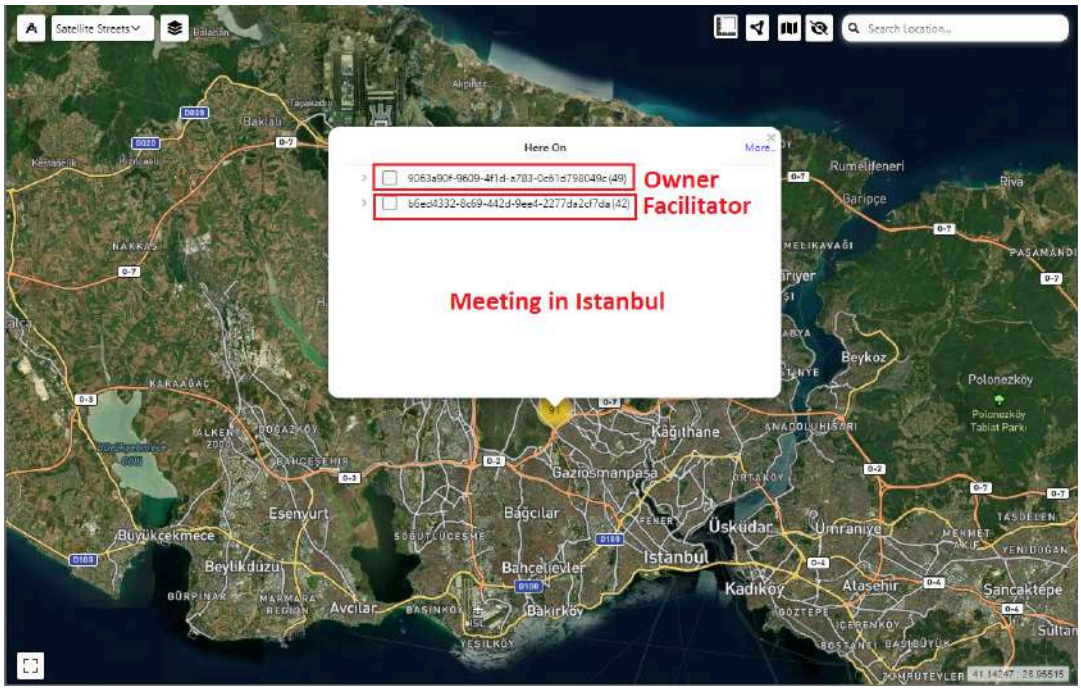
Executing an Activity Scan **AS** functionality around the local company allows us to identify 15 devices in the same area during working hours, which probably belong to the employees.
(company activity scan)

Exécution d'une analyse d'activité **AS** la fonctionnalité autour de l'entreprise locale nous permet d'identifier 15 appareils dans la même zone pendant les heures de travail, qui appartiennent probablement aux salariés.
(company activity scan)



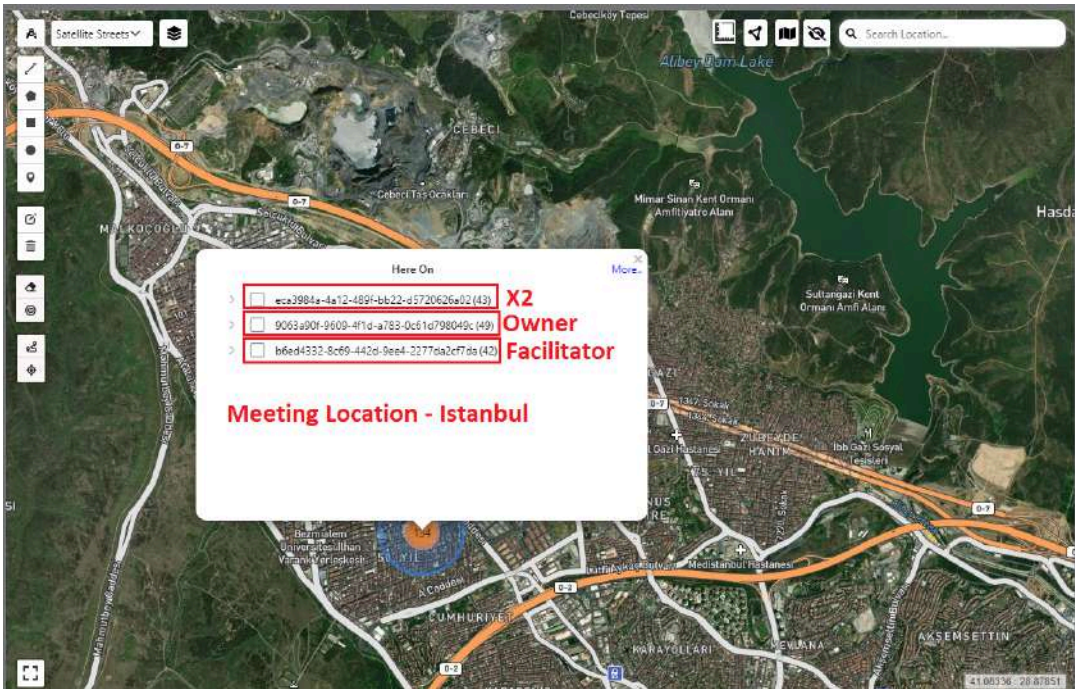
Executing a **POI** query for the financing facilitator and these 15 devices allows us to discover several meetings between the facilitator X1 and one of these devices in a restaurant near the Nigerian coast and three times in Istanbul, which probably belongs to the owner of the company. This company is a big importer of wheat from Ukraine. *(POI - 15 devices)*

Exécution d'un **POI** pour le facilitateur de financement et de ces 15 appareils nous permet de découvrir plusieurs rencontres entre le facilitateur X1 et l'un de ces appareils dans un restaurant près de la côte nigériane et à trois reprises à Istanbul, qui appartient probablement au propriétaire de l'entreprise. Cette entreprise est un gros importateur de blé d'Ukraine.
(POI - 15 devices)



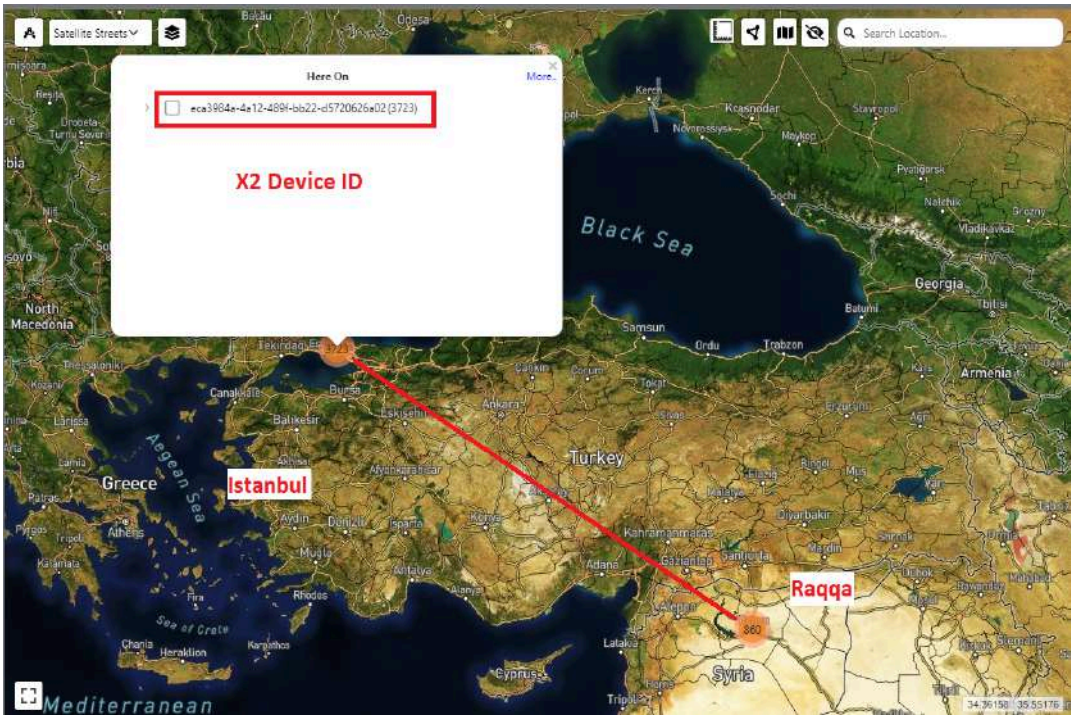
Executing a **DTP** query on the previous location in Istanbul for the 3 different times of meetings, a third device is detected (named X2) that was attending these meetings.
(AS - Istanbul Meeting)

Exécution d'un **DTP** requête sur l'emplacement précédent à Istanbul pour les 3 heures différentes des réunions, un troisième appareil est détecté (nommé X2) qui assistait à ces réunions.
(AS - Istanbul Meeting)



Executing a **DH** for X2 showed that was moving between Istanbul and Raqqa in the north-east of Syria, and he is used to visiting Beit Al Mal of ISIS, which probably belongs to a financing facilitator of ISIS. *(DH- X2)*

Exécution d'un **DH** car X2 montrait qu'il se déplaçait entre Istanbul et Raqqa, dans le nord-est de la Syrie, et qu'il avait l'habitude de visiter Beit Al Mal de l'EI, qui appartient probablement à un facilitateur de financement de l'EI. *(DH-X2)*



These analyses led us to discover that ISIS was paying the price of wheat shipments instead of the Nigerian company, whose owner gave the same sum of money to Boko Haram's financing facilitator, and in this way Boko Haram benefited from ISIS funds without moving the money between Syria and Nigeria.

Les analyses ont montré que l'État islamique a financé les expéditions de blé pour une société nigériane, dont le propriétaire a transféré la même somme à un facilitateur de Boko Haram, permettant à ce dernier de bénéficier des fonds de l'État islamique sans transfert direct entre la Syrie et le Nigéria.

Chapter 3: TBML scheme and drug trafficking between Europe, West Africa and Dubai

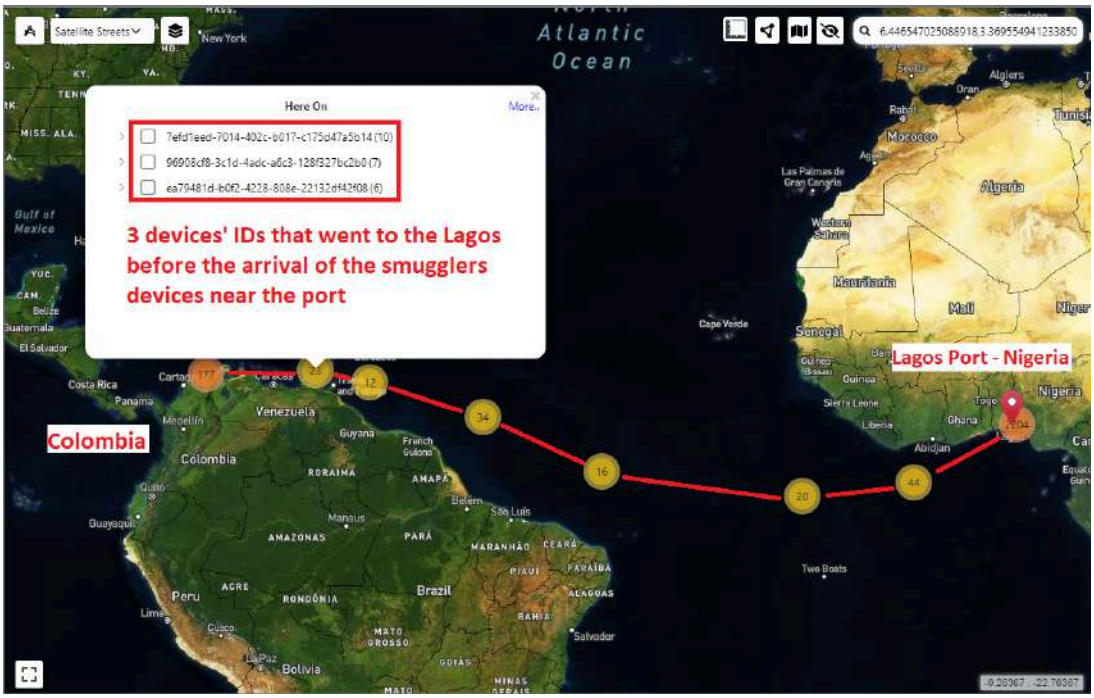
By going back in time during the period between 2016 and 2017, and executing a device history **DH** query for the eight devices identified near Bilma, we were able to discover several trips between Tajerhi in Libya and a warehouse near the Lagos port complex. *(DH - 8 Devices of Bilma)*

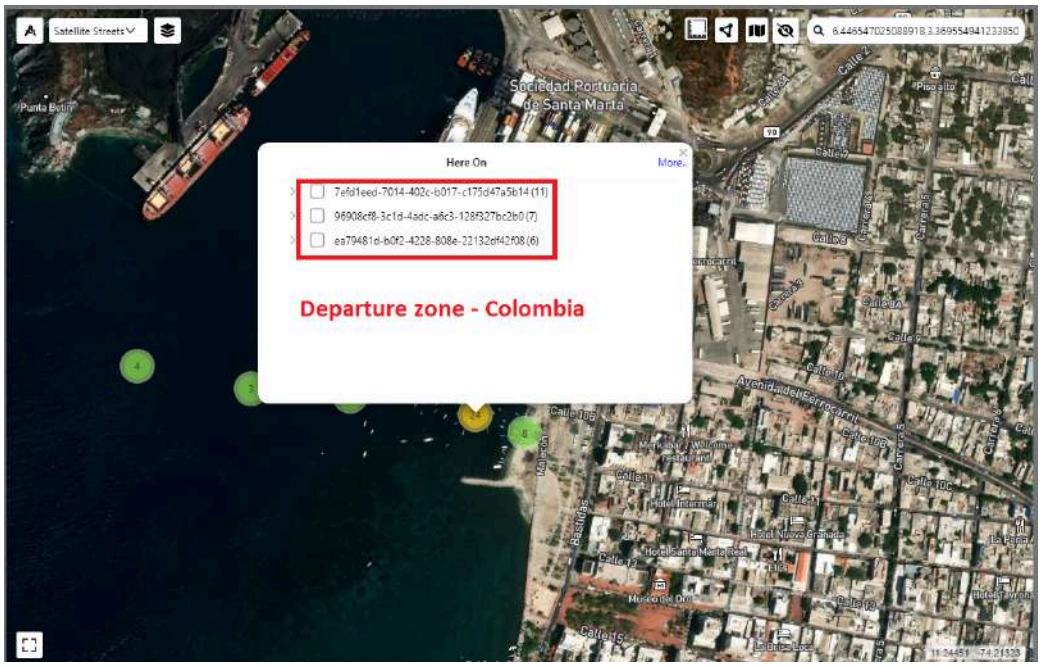
Chapitre 3: Programme TBML et Trafic de Drogue entre l'Europe, l'Afrique de l'Ouest et Dubaï

En analysant l'historique de 2016 à 2017 et en exécutant une requête sur les appareils DH, nous avons identifié plusieurs trajets entre Tajerhi, en Libye, et un entrepôt situé près du complexe portuaire de Lagos, à travers les huit appareils repérés près de Bilma. *(DH - 8 Devices of Bilma)*

Executing a device history pattern **DHP** query around the warehouse on the same date and time as the devices arrived at the warehouse allows us to uncover three devices that came from Colombia to the Lagos port before the arrival of the smugglers devices near the port, where all devices were encountered in the same location (the warehouse) for more than two hours prior to the displacement of the smugglers toward Tajerhi. This result indicates that they are involved in drug trafficking from Colombia to Libya through the Nigerian territories. *(DHP - Warehouse)*

L'exécution d'un modèle d'historique de périphérique DHP et une requête autour de l'entrepôt, au même moment que l'arrivée des appareils, ont révélé trois appareils en provenance de Colombie arrivant au port de Lagos avant les appareils des passeurs. Tous les appareils se sont retrouvés dans le même entrepôt pendant plus de deux heures, avant que les passeurs ne poursuivent leur trajet vers Tajerhi. Cette analyse suggère leur implication dans le trafic de drogue entre la Colombie et la Libye, en transitant par les territoires nigérians. *(DHP - Warehouse)*





Executing a device history pattern **DHP** query around Tajerhi at the same time as the arrival of the smugglers leads to the identification of four devices moved later from Tajerhi to Siret and then to Malta port, which indicate that the drugs are smuggled to Europe.
(DH - 4 Devices going to Malta)

Exécution d'un modèle d'historique de périphérique **DHP** requête autour Tajerhi en même temps que l'arrivée des passeurs conduit à l'identification de quatre appareils déplacés plus tard de Tajerhi à Siret puis au port de Malte, ce qui indique que la drogue est introduite clandestinement vers l'Europe.
(DH - 4 Devices going to Malta)

Executing a device history **DH** query on these four devices discovered above led to the identification of one of them as frequenting an expensive car trade company in Tripoli, Libya, which is one of the big importers of expensive cars from Italy to Dubai through Libyan territories, like Lamborghini, Ferrari, and others. *(DH - 4 Devices going to Malta)*

L'exécution d'une requête sur l'historique des appareils DH de ces quatre appareils a permis d'identifier l'un d'entre eux comme étant en contact fréquent avec une entreprise de commerce de voitures de luxe à Tripoli, en Libye, qui est l'un des grands importateurs de voitures de luxe d'Italie vers Dubaï via les territoires libyens, telles que Lamborghini, Ferrari, et d'autres. *(DH - 4 Devices going to Malta)*

This geolocation intelligence led us to identify a potential TBML scheme between organized crime gangs and a local company in Libya. Where the illicit funds generated from the drugs smuggled to Europe are used to export expensive cars to Libya before being sold in Dubai with the intention of transferring money later to Colombia.

Ces renseignements de géolocalisation nous ont amenés à identifier un éventuel stratagème TBML entre des gangs du crime organisé et une entreprise locale en Libye. Où les fonds illicites générés par la drogue introduite clandestinement en Europe sont utilisés pour exporter des voitures coûteuses vers la Libye avant d'être vendus à Dubaï avec l'intention de transférer de l'argent plus tard vers la Colombie.

Conclusion

In conclusion, the scenario described in February 2017 underscores the efforts of Nigerian authorities to combat terrorism and criminal activities.
The utilization of VCIS solution features helps them identify and disrupt various forms of illegal financial transactions and criminal activities, including TBML and TBTF schemes, as well as weapons and drug smuggling, which often involve the participation of multiple individuals and organizations in several countries.

By employing the VCIS solution's features, law enforcement agencies and intelligence organizations are better equipped to fight against two specific types of financial crimes: TBML (Trade-Based Money Laundering) and TBTF (Trade-Based Terrorist Financing), which are the most dangerous threats facing communities and where the criminals find big opportunities to exploit the international economic trade system to their benefits, far away from the supervision of the authorities and their ability to discover them.

This approach is crucial for supporting the investigations, maintaining national security and stability in the region, and implementing proactive security measures.

Conclusion

En conclusion, le scénario de février 2017 met en évidence les efforts des autorités nigérianes dans leur lutte contre le terrorisme et les activités criminelles. L'exploitation des fonctionnalités de la solution VCIS permet de détecter et d'interrompre efficacement diverses formes de transactions financières illégales et d'activités criminelles, notamment les programmes TBML et TBTF, ainsi que le trafic d'armes et de drogues, impliquant fréquemment plusieurs acteurs et organisations à l'échelle internationale.

Grâce aux fonctionnalités avancées de la solution VCIS, les forces de l'ordre et les services de renseignement disposent d'outils puissants pour combattre deux menaces majeures dans le domaine des délits financiers: le blanchiment d'argent basé sur le commerce (TBML) et le financement du terrorisme basé sur le commerce (TBTF). Ces menaces représentent des opportunités significatives pour les criminels d'exploiter les systèmes économiques et commerciaux internationaux à leur avantage, en échappant souvent à la supervision des autorités.

Cette approche est essentielle pour soutenir les enquêtes, assurer la sécurité nationale et la stabilité régionale, et mettre en place des mesures de sécurité préventives.