Hacking the Web: Exploiting Open Source Intelligence & Cyber-Related Information to Disrupt Illicit Financial Networks

Andrew P. Rudd, CAMS
CAMS-FCI Candidate White Paper
# Table of Contents

1. Executive Summary .......................................................................................................................... 3  
2. Introduction ........................................................................................................................................ 3  
3. AML/CTF Convergence with Cyberspace ....................................................................................... 4  
4. Understanding and Defeating Illicit Networks ................................................................................. 5  
5. Understanding Social Media, Open Source Intelligence, and Cyber-Related Information ............ 8  
6. Analysis and Exploitation of OSINT and CRI .................................................................................. 11  
7. Integrated Analysis .......................................................................................................................... 14  
8. Key Recommendations ..................................................................................................................... 15  
9. Conclusion ......................................................................................................................................... 16
1. **Executive Summary**

We live in an age in which all aspects of our lives are facilitated by technology. The advent of mobile computing has enabled us to accomplish various tasks in a manner that would have seemed far-fetched less than a decade ago. As a corollary, these advancements have also increased risk in an unprecedented fashion. Threat actors can now move money through the financial system from a cell phone in one country, while holding accounts which are operated through a series of shell or front companies in another. This reality highlights the value of AML/CTF Analysts having access to the proper tools, training and knowledge to conduct in-depth online research. This is truly critical to countering the threat to the global financial system by transnational criminal and terrorist organizations.

2. **Introduction**

This paper will explore the use of Open Source Intelligence (OSINT), including Cyber Related Information (CRI), to enhance an analyst's understanding of how it can be leveraged to identify illicit networks and any potential financial crime risk those networks bring to Financial Institutions (FI). For example an analyst with the ability to see the bigger picture, is able to identify previously unknown relationships and/or locate true beneficial ownership. Efforts to enhance these skills can enable compliance officers to “peel the onion” so they might understand hidden risks. The benefits of this will be readily recognizable to those familiar with examining front companies. Prior to addressing the usage of OSINT and cyber-related information to disrupt illicit financial networks, it is important to understand what these networks are and how they operate.

Illicit networks, (often referred to as dark or opaque networks), are able to effectively hide the true nature of their activity and business relationships. This is done through the creation of complex ownership structures and shell companies. This makes it difficult for law enforcement and FIs to peel back the onion to reveal true beneficial ownership and complicates efforts to discover connections between seemingly unrelated entities. If FIs are unable to identify the true beneficial ownership of an entity or detect the true nature of the business, they may not be able to see the bigger picture of activity related to an illicit network.¹

Relying exclusively on automated detection scenarios will fail to produce the holistic view necessary to comprehend complex criminal networks. Likewise maintaining a narrow Business As Usual (BAU) lens will prevent forward looking investigators from operating at their fullest potential. It is not only beneficial to FIs to identify previously unknown risks, but this can also provide more comprehensive Suspicious Activity Reports (SAR), thus assisting national Financial Intelligence Units (FIUs), such as FinCEN in the U.S. Effective use of OSINT aids in the identification of new investigative leads and typologies. FIs can utilize this information to modify detection scenarios and their understanding of the risk within their organization’s footprint. Through a holistic lens FIs can develop an understanding of common connection points found via detection scenarios. These connection points may be a crucial lynchpin to comprehending an illicit network.

---

¹ Financial Institutions (“FIs”) include banks, broker-dealers, insurance companies, mutual funds, residential mortgage lenders and originators, money services businesses and casinos who are required to file Suspicious Activity Reports (“SARs”).
With no way of being able to identify an entity’s links to other entities within the network, FIs face undeterminable amounts of risk. All too frequently compliance regimes fail to connect illicit counterparts due to the time constraints and operational bandwidth restraints. Compliance programs that are slow to evolve to advances in technology compound these frustrations. Often noted shortfalls can be found in limited or convoluted access to FI data, well-intentioned web search restrictions and a general lack of enterprise-wide technology solutions. Knowledge gaps, training failures and barriers to developing crucial raw information can all lead to AML program failures.

Using OSINT is a key methodology and intelligence gathering technique analysts’ leverage to gain valuable insights and information from internet-based sources. In recent years, social media/social networking platforms, such as Facebook, Twitter, LinkedIn, and VK, have grown exponentially across the globe due to the increased availability and access to the internet, which in turn has seen the development of Social Media Intelligence (SOCMINT) in 2012. Research has shown the interconnected nature of social media sites used as covert networks for criminals and terrorists to communicate, recruit, and seek financial support. Tracking and analysing threats can be mitigated by uncovering these covert networks through the use of Social Network Analysis (SNA) which is used by researchers to locate these hidden online communities, groups and relationships.²³

3. AML/CTF Convergence With Cyberspace

In 2015, Jennifer Shasky Calvery, former Director of FinCEN, stated that FIs should include CRI within their SARs, even though it was not a requirement through legislation, as it is incredibly important to law enforcement investigators. She also stated that less than 2 percent of SARs being filed actually contained IP addresses. While her comments were directed to specific cyber threats, such as ransomware, DDoS attacks, and malware, CRI should not be overlooked for its value in investigations where technology is used to move illicit funds linked to activity such as human trafficking, arms trafficking, narcotics trafficking, trade-based money laundering, sanctions circumvention and terrorist financing. This statement appears to show a nexus between CRI and AML/CTF investigations, and it appears FinCEN is sending a message that the value of this information can be used by their main stakeholders, U.S. law enforcement and the Intelligence Community (IC).⁴

In 2016, FinCEN released an Advisory Bulletin, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, which encouraged the reporting of cybercrime and cyber-enabled crime through SARs to them. Furthermore, they asked FIs to include relevant and available cyber-related information (e.g., internet protocol (IP) addresses with timestamps, virtual-wallet information, device

identifiers) in SARs and that this information should be shared with other FIs to detect and report money laundering, terrorist financing and cyber-enabled crime.5,6,7

The 2016 advisory stated that all relevant information should be included in SARs to ensure they are complete and accurate, which includes CRI. This demonstrates that the inclusion of CRI in SARs is essentially due to increasing reliance on electronic banking systems being used for financial transactions and therefore illicit financial activity will leave an electronic footprint. Leaving an electronic footprint means there is also the strong likelihood that this corresponds to the threat actors, their businesses and other related suspicious transactions.8

Internal data from within an FI can provide significant advantages to an AML/CTF investigation. For example - having access to the IP addresses for specific threat actors’ online banking activity can identify lifestyle, geolocation, patterns of activity, attempts to conceal their electronic footprint, links to other accounts and links to associated entities. There was increased attention on the inclusion of IP addresses, website information, emails and other internet data in 2012 when FinCEN launched a digital version of the SAR which asked compliance officers for this type of digital data to be included.9

For on boarding of clients, FIs are required to conduct Customer Due Diligence (CDD) in order to Know Your Client (KYC) or Know Your Business (KYB). During this process there should be a range of data collected that would prove useful to an analyst to monitor the clients account for unusual or suspicious activity. It is important that FIs collect, aggregate, and monitor digitized data and CRI for clients that have remote deposit capture, online banking and electronic banking, and especially where the account was opened online without face-to-face contact.10

Dr Shima Keene (2013) stated that finance and the internet have a close relationship due to globalization and that there are challenges posed by advancing technologies in the cyber environment which require a better understanding in the subject. In fact, while Keene is referring to its relevance to terror finance, it is applicable to any criminal organization wishing to use increasingly popular mobile payment systems as their money laundering vehicle of choice. According to John Cassara (2017), these new and emerging financial structures allow for greater flexibility to move and hide their illicit funds.11,12

4. Understanding and Defeating Illicit Networks

Illicit Networks - Illicit networks can be portrayed as hierarchical but often they are decentralized and horizontal in their makeup according to Stewart Patrick (2012). Transnational Criminal Organizations (TCO) such as the Russian Brothers’ Circle demonstrate that they appear as an umbrella

5 An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification, and location addressing.
6 Virtual Wallets are an easy to use payment information storage system, and are often directly linked to your bank account or debit card. You can use your virtual wallet online through a computer or cell phone to make purchases. Companies such as PayPal, Google Checkout, and Bill Me Later are some of the main providers.
7 Common device identifiers include, for example, media access control (MAC), internet protocol (IP) addresses, software, or device-unique token identifiers.
8 Digital footprints are described as the unique set of digital activities, actions, and communications that leave a data trace on the internet or on a computer or other digital device and can identify the particular user or device.
organization overseeing the activity of multiple smaller criminal networks globally with no specific overall leader being identified. TCOs have benefited from globalization greatly as their businesses have become far reaching and not bound by the borders of their countries. Patrick specifically stated that the impact of technology has cut both ways for illicit organizations. Illicit organizations are increasingly dependent on the use of the internet, cell phones and computer systems to launder money and the trafficking of illicit goods and services. The advantage to law enforcement and the intelligence organizations around the world is that they are able to exploit these technologies within their country’s legal framework. It therefore seems appropriate that if the illicit networks leave themselves open to exploitation through the internet, experienced analysts/investigators could begin to piece together parts of the organizations and start making links to their people and businesses they operate. Dennis Lormel (2015) suggests identifying financial chokepoints through building business models for terrorist organizations (TO) which would allow for the identification of red flags, understanding the flow of funds, as well as developing investigative, disruptive and preventive measures which would apply significant pressure on these networks. These TOs rely heavily on both the formal and informal financial systems to move funds in and out, it is however, a significant risk to these networks of being caught and denied access to the global financial system. This can be applied holistically to the understanding of illicit financial networks that don’t specifically have to focus on terrorist financing. Scott Helfstein (2014) through the Combating Terrorism Center at West Point conducted network analysis on open source data for 2,700 individuals linked by 15,000 relationships over 122 countries in which he stated “identifying financial irregularities is critical to tracking dirty money, questionable transactions and illicit actors.” It then stands to reason that FIs should be able to make assessments on the threats posed by these illicit networks to their banking footprint or client base through careful and detailed OSINT and transactional analysis to reduce the risk that they pose. 13,14,15,16

**Counter-Terrorist Financing (CTF)** - Government agencies have spent a great deal of time in their attempts to combat and disrupt TCOs and TOs globally. CTF is a multi-agency approach designed to bring together the US Intelligence Community (IC) and law enforcement to counter illicit finance in a strategic and targeted fashion. Often building a picture of the illicit network can take years of painstaking investigation and intelligence gathering which includes the analysis of a vast amount of financial data, along with other legal options available to gather evidence such as lawful interception, cell phone records, covert surveillance, recruiting human intelligence sources to name a few. The 2011 *Strategy to Combat Transnational Organized Crime* highlighted that the government should employ the Open Source Center (OSC) to draw upon what they describe as ‘grey’ literature, foreign press covering crime and social media to develop profiles of individuals, companies and institutions linked to transnational organized crime (TOC).

**Financial Institutions Role in Countering Threat Finance** - While FIs don’t have the ability to gather the same type of data as the government, they are in the unique position of being able to analyse transactions and make determinations of their potential link to money laundering and terrorist financing based on information derived from law enforcement engagement, adverse media, court documents,  

open source research, client information, inter-institution information sharing and requests for information across their own organizations. CTF agencies are only able to assess financial data that has been disclosed in a SAR or through legal process by a law enforcement agency and as such they rely on the accurate and timely reporting of suspicious activity by FIs.

Compliance programs using OSINT and CRI will allow their analysts to reach deeper into the understanding of the networks to find the illicit activity. Asher (2015) highlighted that broader measures should be introduced to allow bank intelligence units cleared personnel that are able to access a federal watchlist portal for terrorist financing and fanciers, providing more selectors of information to conduct open source research against.17,18,19

Public Sector/Private Sector Engagement Networks - Creating and maintaining a network to counter networks is crucial for a compliance program wanting to disrupt TCOs and TOs. Groups such as the Joint Money Laundering Intelligence Taskforce (JMLIT), based in the U.K., were set up to share information between law enforcement and the private sector to develop intelligence on individuals, groups and entities involved in illicit activity. Using a fusion type environment and leveraging the close contact will lead to “shedding more comprehensive light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions” according to Hutchings (2016) when she was exploring how 314(b) USA PATRIOT Act can be used in a fusion center approach to share information and intelligence. Section 314(b) allows for the sharing of transactional information between FIs and often this includes requesting further information on the other FIs client, such as Personally Identifiable Information (PII). During these requests for information analysts could potentially request the IP address, geolocation and device information for the transactions. This could be extremely valuable for the analysis of potential network activity and subsequently included in a SAR. An example of how both law enforcement interact with FIs and how institutions interact with each other can be seen here in ‘The Information Sharing Triangle’, which shows the interconnected way information is shared between each entity.20,21,22

Disruption of Illicit Networks - FIs have a number of tools at their disposal for the disruption of illicit networks. The FIs compliance program will have filters to block and reject transactions, account restrictions, law enforcement engagement and SAR reporting. Each of these tools will have some form

---

18 The Director of National Intelligence (‘DNI’) Open Source Center is the focal point for the intelligence community’s exploitation of open source material. It also aims to promote the acquisition, procurement, analysis, and dissemination of open source information, products and services throughout the U.S. Government. The Open Source Center was established at the Central Intelligence Agency and succeeds the former Foreign Broadcast Information Service.
20 The JMLIT is a Public-Private Information Sharing Partnership to Tackle Money Laundering: The primary objectives of the JMLIT are to: improve the collective understanding of the money laundering threat (Detect); inform and strengthen financial systems and controls (Protect); to inform the prosecution and disruption of money laundering activity (Disrupt).
22 Information Sharing Triangle: Created by Andrew Rudd to demonstrate the relationship of information sharing between the relevant law enforcement and financial institutions.
of effect on the network in the short term or long term causing them to change tactics or move their money through other accounts but not without delay and disruption to their organization.

5. **Understanding Social Media, Open Source Intelligence, and Cyber-Related Information**

**Open Source Intelligence (OSINT)** - OSINT is the collection, exploitation, analysis and dissemination of publicly available information in a timely manner to an appropriate audience to address specific intelligence requirements. Conducting OSINT research has become increasingly more accessible since the internet has rapidly expanded in recent years and as such can be done from your desk anywhere in the world and at any time, and you can remain completely anonymous while doing it.\(^\text{23,24}\)

Publically available information could include newspapers, radio, television, academic research, global economic datasets, commercial databases, open corporate data, leaked data and online forums. Using paid subscription-based sources of information such as LexisNexis, Clear, Accuity, TLO, Bureau van Dijk, Factiva, Panjiva and World-Check can provide a wealth of information to understand who a person is related to, associates, linked businesses, their locations, their addresses, phone numbers, email addresses and social media links. For businesses they provide valuable insight into company records, ownership, profit/loss statements and so on. Serious considerations should also be given to leveraging the wealth of free data sources such as the ICIJ Leaks Data, OCCRP Investigative Database Search, real estate records sites or business registration information sites such as Companies House (U.K.).\(^\text{25,26,27}\)

---


\(^{24}\) Peter Steiner (1993) “On the Internet, nobody knows you’re a dog”. The New Yorker Collection.

\(^{25}\) ICIJ Leaks Data: The International Consortium of Investigative Journalists is a global network of more than 200 investigative journalists in 70 countries who collaborate on in-depth investigative stories, focusing on cross-border crime, corruption, and the accountability of power.

\(^{26}\) OCCRP Investigative Database Search: The Organized Crime and Corruption Reporting Project (OCCRP) is an investigative reporting platform formed by 40 non-profit investigative centers, scores of journalists and several major regional news organizations around the globe. Our network is spread across Europe, Africa, Asia and Latin America. In 2006 they team up to do transnational investigative reporting and promote technology-based approaches to exposing organized crime and corruption worldwide.

\(^{27}\) Companies House: Provides business registry information on company directors, annual returns, document images, addresses, changes in the company’s management, and disqualified directors. Recently added is the ability to ‘follow’ companies and any changes that take place.
Hacking the Web: Exploiting Open Source Intelligence & Cyber Related Information to Disrupt Illicit Financial Networks

Former CIA director, James Woolsey, stated that 95 percent of all intelligence comes from open sources. However, what is interesting is that only a small portion of the U.S. IC budget goes towards OSINT which makes up approximately 40 percent of their reporting. It is unclear of an exact figure or even to what extent FIs use OSINT within their investigative frameworks. There is no measure of effectiveness for the analysts conducting the intelligence gathering but one thing is clear; there is likely to be no consistency across compliance programs. 28,29

**Social Media Intelligence (SOCMINT)** - The term SOCMINT was coined in 2012 by Sir David Omand, Jamie Bartlett and Carl Miller to cover the collection of intelligence from social media sites using either intrusive or non-intrusive methods and from both open and closed online social networks. Their paper argued that social media should be considered part of the intelligence framework, while considering legal, ethical and accountability issues. It should be noted that the legal framework they were referring to was the U.K.’s surveillance legislation known as the Regulation of Investigatory Powers Act 2000 (RIPA). The legislation covers how and when government agencies can conduct covert investigations. SOCMINT covers the growing mountain of social media sources, such as Twitter, Facebook, YouTube, Foursquare, LinkedIn, Reddit, Tumblr, VK and Google+. These sites contain potentially valuable pieces of intelligence from which analysts could identify previously unseen or unknown relationships or connections.30

SOCMINT can provide valuable information in a numbers of ways for analysts investigating network activity, such as age, names, marital status, employment history, educational history, friends, family, places visited, likes, dislikes, geolocations data, political views and so on.

Social media content is user generated and can be created, shared and edited easily and quickly. Smartphones and tablets have facilitated the ability for people to do this on the go and upload data anywhere in the world. This information can confirm that an individual is or is not the person you are investigating based on CDD information or information drawn from other sources. Reviewing their social media content might also support your investigative analysis and show that they have considerable assets (such as cars, boats, houses, vacations, expensive jewelry etc…) while their declared income does not appear to support that lifestyle. Financial Transactions and Reports Analysis Centre (FINTRAC), the Canadian FIU, investigates social media accounts of Canadians that have come to their attention.31,32,33

"It is important to remember that the perpetrators of these crimes often times have an online presence and actively use the web, including social media, to connect with associates, facilitate their activities and, in the case of terrorism financing, even raise funds." FINTRAC spokesperson Renée Bercier stated.

30 #Intelligence – Demos. (2012). Retrieved from https://www.demos.co.uk/project/intelligence/
Cyber-Related Information (CRI) - This is the information that describes technical details of electronic activity and behavior, such as IP addresses, time stamps, indicators of compromise (IOCs) and device identifiers. Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their patterns of behavior. It is important to note that information such as IP addresses, hosting services, domain ownership, dates, domain history, contact details and administration information can be obtained through examination of websites and emails associated to those domains providing CRI that can be exploited by the analyst. Fig. 1 & 2 below show how using CRI when investigating illicit network activity could be beneficial to the analyst.

Dark Web/Darknet - Most people have heard of the ‘Dark Web’ which sits below what we see when conducting our routine OSINT collection on the surface or deep web. The dark web, also contains the ‘darknet’ which is often associated with illicit marketplaces where drugs are trafficked, prostitution takes place, hitmen can be hired, human trafficking takes place and illegal pornography can be found. The darknet has seen recent investigations into illegal markets such as Silk Road and Alpha Bay where the government has seized the domains preventing any further trading to take place. From a FI standpoint certain pieces of information that can be gleaned from the dark web, such as carding sites, banking credentials, account information and money mule services.

Identifying this information would provide potential selectors to search within a FI's transactional data.

In 2016, George Cottrell, a political aide to the U.K. politician Nigel Farage was indicted for 21 counts of criminal activity, which included wire fraud, blackmail and money laundering. Cottrell came to the attention of the FBI on the darknet where he was offering his financial expertise to launder money and provide financial consultation services, and guaranteed that he could launder $150,000 per month through foreign and domestic bank accounts. Another individual, using the online handle Keno13, operates on darknet sites such as Agora and Evolution. Keno13 provides money laundering services, which includes cashing out for vendors, buyers and market administrators using stolen identities to create bank accounts.36,37

“Darknets are fast emerging as the preferred trading venue for organized crime networks and individuals to carry out illicit activities, with cryptocurrencies the preferred medium for paying for these criminal services,” Madan Oberoi, Director of the Cyber Innovation and Outreach Unit at INTERPOL.38

6. Analysis and Exploitation of OSINT and CRI

Threat actors are able to perpetrate threats by exploiting the internet by recruiting, transferring information or knowledge, sale and trafficking of illicit goods, as well as money to finance and coordinate their activities. While the threat actor uses the internet they leave themselves open and vulnerable to being potentially traced and/or monitored through OSINT collection and analysis. CRI can be exploited and analysed against internal and external systems or even through information sharing requests to see if the activity has been seen with other FIs.

OSINT and CRI can be exploited in a number of ways. Specifically one method is to conduct domain analysis on the website of the suspect entity to locate the IP address and person who registered the website. The domain analysis will also provide insight into where the site is hosted or if the registered owner of the domain is located in a specific country. Conducting further research can potentially identify linked websites or additional registration information that could be exploited to develop the understanding of the network. Fig.3 shows that the registered owner of a website is associated with a particular IP address and the analysis has linked the common IP address to two different company websites. The first website is for a designated entity that the analyst was investigating and the second website leads to a previously unknown company. If the analyst identifies transactions for the second company this could indicate this entity is linked to the designated group. It is not uncommon for websites to share common IP addresses and hosting services. In Fig.4 it demonstrates how conducting this analysis can locate multiple entities that could potentially be linked to the same network. Using OSINT on the new selectors of information the analyst can now further develop information on the network.39

39 Domain analysis could lead to the discovery of sanctions breaches or attempts to circumvent sanctions. If an entity is identified through an IP address or domain hosted in Iran, Syria, North Korea for example you may see Internet country code top-level domain (ccTLD) with .ir, .sy, or .kp respectively.
In a compliance program understanding the geographic risk of a network or the potential geographic exposure of an entity can provide an analyst with red flags. When exploiting open sources an analyst might be able to assess company websites. Using web analytic tools to provide both the audience geography and the key words used to get to the website which could be extremely valuable depending on the type of activity you are reviewing.

Being able to exploit OSINT may have been critical in locating shell companies and company service providers in the 2012 Global Witness report, *Grave Secrecy*, where more than 20 companies on the face of it did not appear to have any connection to one another. Reviewing the company information revealed a well-connected network covered multiple countries. The report documented an international criminal network with ties to Russia and Kyrgyzstan that were involved in money laundering, corruption and fraud. Once a network like this is identified through OSINT the analyst should be able to effectively locate transactional data which may yield counterparties not seen in the open source research. Fig.5 shows that during domain analysis you can compare the location of the registered site owner and the hosted location of the site. Depending on the type financial activity you are reviewing this could be beneficial to analysis of shell or front companies.

---

40 *Grave Secrecy: How A Dead Man Can Own A UK Company and Other Hair Raising Stories About Hidden Ownership From Kyrgyzstan and Beyond.* (2012). Retrieved from https://www.globalwitness.org/sites/default/.../kyrgyzstanreportgrave%20secrecy.pdf
Every Contact Leaves a Trace. It should be noted that every time an analyst visits the website of an entity they leave behind their own digital footprint. This could potentially start to tip off the threat actor to the FI’s interest in their business if the same site is visited several times by Bank A’s static IP address. TCOs and TOs might have people acting in their own counterintelligence roles to protect the illicit network. Al-Qaeda and Russian organized crime employed counterintelligence as part of their operations. If the FI is able to provide the analyst with the ability to conduct their research using the internet than they should consider using some form of anonymization masking the true IP address and even their device information. This would leave the analyst potentially vulnerable or even tipping off the group of growing interest to their entities.41,42,43,44

Compliance programs require the recording and retention of documentation. The analyst reviewing a network should maintain clear, concise and accurate records of the selectors that they are researching, which could include individuals, entities, addresses, account numbers, phone numbers and CRI. The key stage of OSINT is the collection and the storage of material that an analyst will need to exploit. When investigating networks an analyst could spend hours conducting research through multiple sources and with the use of certain tools they can facilitate the accurate recording of sites visited. Tools such as Hunchly and X1 Social Discovery have the ability to capture the full webpage content the analyst visits creating searchable pages which are stored locally on the analyst’s desktop instead of a cloud. The added features of these tools is that the data you’ve collected can be analysed and disseminated in the same format as if they were the original website. Once the search and websites are saved, and the original deleted, it won’t matter as you would have the exact page on your local drive as a file and

41 Locard’s Principle - Every Contact Leaves a Trace: The theory that anyone, or anything, entering a crime scene both takes something of the scene with them, and leaves something of themselves behind when they leave. In the digital world, this translates into that when two computers come in “contact” with each other over a network and they exchange something with each other such as technical data.
you won’t have to rely on the Way Back Machine (WBM), also known as the archive.org, which may not have even captured the cached version of the site.\textsuperscript{45,46,47}

7. Integrated Analysis

To ensure that the analyst is able to understand the full extent of the illicit network activity the integration of the data acquired through OSINT and CRI can be leveraged through Link Analysis, Social Network Analysis, Geospatial Analysis, Temporal Analysis and Trend Analysis. This holistic approach to investigating OSINT and CRI along with their transactional data can lead to the identification of previously unknown relationships, unmasking hidden ownership and the development of typologies.

Geospatial Analysis - This type of analysis would allow for the analyst to present the transactional data, including the flow of funds, in one layer and then add the CRI or open source data as another layer. Michael Wakeman (2015) examined the potential use for geographic information systems in terrorist financing investigations. He was able to use predicative analytics along with geospatial analysis to identify the movement of terrorist-related funding. In one specific example he examined potential accounts linked to border guards on the Turkey/Syria border. Based on Wakeman’s analysis and the inclusion of login information of the account holders to verify if they resolve back to a same device, same geolocation or same IP address showing the potential connection to a specific actor in the network depositing or managing the funds in their accounts. In this context relating to the Syrian border, did the border guards login from a specific location where they shouldn’t be or are multiple bank accounts sharing the same IP address or device information? For an analyst this could potentially be crucial information to an analyst’s investigation as to how inclusive individuals are within a network.\textsuperscript{48}

Social Network Analysis (SNA) - SNA is the use of visual and mathematical analysis to map and measure the relationships and flows of people, groups, entities, computers, IP addresses and anything else that appears to have a connected relationship. The data is often comprised from open source material. SNA allows an analyst to be able to understand and study a network by looking at the social relationship of the actors. It could also be used to identify the potential financial chokepoints to disrupt a network.

Europol and INTERPOL used SNA to investigate data they had collected, which included using OSINT and SOCMINT, on the largest networks they had identified related to migrant smuggling. This analysis allowed them to study the connections between networks, how widely spread they are, how links were established and who the main organizers are.\textsuperscript{49}

Roland Blatnik (2016) used SNA in order to identify the major groups across Europe and Latin America. He stated that if one or more groups were taken out of the network it would dismantle the

\textsuperscript{45} Hunchly - Better Online Investigations. Retrieved from https://www.hunch.ly/#time-machine
\textsuperscript{46} X1 Social Discovery - Social Media and Internet-Based Data Collection. (n.d.). Retrieved from http://www.x1.com/products/x1_social_discovery/
\textsuperscript{47} If visiting a website for the first time an analyst can save it using archive.is and viewed again later in the archive.org. It should be noted that using archive.is allows the viewing of the page, including images, as a cached page if blocked by internal internet filters.
majority of the network. In his conclusions he identified that the sources for the analysis were open source news, retired human intelligence sources and several reports on the groups involved.50

**Link Analysis** - i2 Analysts’ Notebook, Palantir, Maltego or similar link analysis programs can greatly improve the visual representation of activity. Viewing transactional data combined with the information drawn through OSINT will provide a holistic view of the network. Data visualization should be able to communicate effectively and clearly to the reader through traditional charting and plots.51

Large and complex transactional data sets relating to illicit financial networks can be challenging and the analyst has to be able to effectively identify key transactions and relationships within the data sets. If an analyst is focusing on long term network analysis they could identify hundreds of key actors along with associated businesses and produce thousands of transaction hits. This data will require further analysis to determine true matches as well as OSINT on their counterparties. Using link analysis at an early stage will help to process the transaction information into a visual representation to assist in determination flow of funds, potential financial chokepoints and country flows. The analyst can start importing further data such as OSINT and CRI to fully understand the activity and connectivity between key players within the network.

8. **Key Recommendations**

1. **Identify Key Internal and External Data**: FIs should be identifying internal and external sources to support their analysis of illicit financial networks.

2. **Disruption Tools**: The compliance program should have already well-established processes for transaction filtering, account restriction and activity reporting. Leveraging these programs within the FI and how they can be used to combat illicit networks.

3. **Training and Awareness**: Increased training and awareness in OSINT for analysts will ensure they become more productive in identifying financial crime risks when investigating money laundering and terrorist financing networks.

50 Blatnik, R. (2016, August 1). Social Network Analysis of Organized Crime Groups (OCGs) and Terrorist Organizations (TOs) Between Europe and South America. Retrieved from https://intelligenceobserver.com/


4. **Anonymization**: Protecting your analysts and your reputation by gaining anonymity online. Hiding your IP address using ‘The Onion Router’ through a standalone machine or using Virtual Machines (VM) / Virtual Private Networks (VPN) can add layers to your FI’s security when conducting online research. Consider having specialist analysts with access to Commercial off the Shelf (COTS) OSINT platforms and software which have built in security.53

5. **Threat Actors Hiding Behind the Keyboard**: Threat actors may use VPNs or TOR to conduct their online transactions. FIs could consider blocking TOR exit nodes and known VPN services to reduce the risk to the organization and increase the threat actors’ online exposure to disclosing a true IP address and geolocation. FIs often block TOR nodes to prevent malicious activity and fraud.

6. **Tools of the Trade**: Consider investing in some advanced tools that can be used to effectively map out online networks and subscriptions to services that assist in identifying potential beneficial ownership of unidentified businesses.

7. **Collaboration**: Working with law enforcement and other FIs is key to success in locating additional information to research through open sources. This information will expand the understanding of the network and locate further individuals and entities that were previously unseen.

8. **Task Force**: ACAMS should consider creating a task force to focus on the development of technology and its roles in preventing, detecting and investigating money laundering and terrorist financing.

9. **Conclusion**

   It is clear that FIs must rely on using OSINT as a routine task within their investigative framework. There is no other method of collecting information from open sources without an analyst being able to research internet-based sources.

   Outside of the routine, specialist analysts should be able to leverage OSINT to tackle more complex and challenging issues such as identifying and disrupting TCOs and TOs. This requires that the analyst be able to understand how the networks are structured, building out their business model, collecting their information from open sources and then start to analyse the associated transactions.

   It was estimated that 80 to 90 percent of suspicious activity reported to law enforcement were not useful. With an estimated 2.6 million SARs expected to be filed in 2017, for the U.K. and U.S., the value of information included in the SARs is critical to draw their attention. The use of detailed OSINT and CRI provided in SARs focused on illicit financial networks is likely to be more targeted and therefore dramatically improving value to law enforcement in the attempts to disrupt TCOs and TOs. FIs that invest in countering the threat of illicit financial networks through long term intelligence-led analysis and information sharing will reduce the financial crime risk posed by these networks.54

---

53 The Tor Project software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

By being proactive with OSINT and CRI FIs will develop a deeper understanding of illicit financial networks, business profiles, their methods, their electronic footprints and new typologies. Once they are able to do this identifying the financial chokepoint will lead to successful disruption of the illicit financial network.