2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)

Validating Bad Entity Ranking in the Panama Papers via Open-source Intelligence

Donald Winiecki
Dept. of Organiz. Performance & Workplace Learning
Boise State University
Boise, ID (USA)
dwiniecki@boisestate.edu

Katherine Kappelman
Dept. of Anthropology
Boise State University
Boise, ID (USA)
katherinekappelm@u.boisestate.edu

Bryant Hay
Dept. of Sociology
Boise State University
Boise, ID (USA)
bryanthay@u.boisestate.edu

Mikel Joaristi
Dept. of Computer Science
Boise State University
Boise, ID (USA)
mikeljoaristi@u.boisestate.edu

Edoardo Serra
Dept. of Computer Science
Boise State University
Boise, ID (USA)
edoardoserra@boisestate.edu

Francesca Spezzano
Dept. of Computer Science
Boise State University
Boise, ID (USA)
francescaspezzano@boisestate.edu

***Abstract*—The Panama Papers network maintained by the International Consortium of Investigative Journalists (ICIJ) represents a large set of relationships between people, companies, and organizations involved in the creation of offshore companies in tax-haven territories, mainly for hiding their assets. The Panama Papers network includes people or companies that had affairs with the Panamanian offshore law firm Mossack Fonseca, often with the purpose of laundering money. In our previous work, we proposed a ranking algorithm, namely the *Suspiciousness Rank Back and Forth* (SRBF) algorithm, that, given the Panama Papers network, leverages a blacklist of known bad entities to assign a degree of suspiciousness to each entity in the network. This algorithm proved to be efficient in detecting known bad entities in the Panama Papers, but we were not able to verify the accuracy of the produced entity ranking for non-blacklisted entities.**

In this paper, we propose to use the open-source intelligence (OSINT) methodology as a modern derivative of classical ethnographic and archaeological research methods that help us in validating with external open source data the ranking result of the *Suspiciousness Rank Back and Forth* algorithm. More specifically, we conduct a parallel, but independent, investigation using OSINT to assess the claims of SRBF algorithm. We identify positive outcomes from this study, describe current gaps in our process, and propose solutions to the gaps in order to better integrate the OSINT methodology with the SRBF ranking approach.

***Index Terms*—Security Informatics, Bad Actor Detection, Open-Source Intelligence, OSINT, Ethnography, Archaeology, Qualitative Social Science**

I. Introduction

The Panama Papers are a set of 11.5M documents leaked from the now-closed Panama-based offshore law firm Mossack Fonseca. The papers show how Mossack Fonseca facilitated the creation of numerous shell corporations, including many that have been used for illegal purposes, including money laundering, tax evasion, terrorist financing, and evading international sanctions. This data is made publicly available in the form of a node and link network [3].

In our previous work [4], [5], we addressed the problem of identifying bad entities (individuals or companies) by leveraging information contained in the Panama Papers network. As not all the people involved in the Panama Papers network have broken the law or acted improperly, we identified a set of bad entities to use as ground truth. More specifically, we compared entities present in the Panama Papers with several freely available online blacklists. By using an exact string matching approach, we identified around 576 bad entities and labeled them as bad, while labeling the remaining entities as unknown. Used blacklists were collected from the http://opensanctions.org website [6]. Opensanctions.org is described as "...a global database of persons and companies of political, criminal, or economic interest. It combines the most important sanctions lists, databases of politically exposed persons, and other public information into a single, easy-to-access dataset."

To identify suspicious entities, we developed an algorithm, called *Suspiciousness Rank Back and Forth (SRBF)*, that computes a suspiciousness score for each entity appearing in the Panama Papers network according to its connections to other known bad entities and by exploiting edge directionality alternation. This rank is used to prioritize entities for subsequent investigation.

We conducted a comparison of SRBF with existing techniques for node classification, such as centrality measures and network embedding models [7], [8], on the task of searching the Panama Papers network for bad entities contained in blacklists as indicated above. Our experimental results show that SRBF is effective and achieves an Area Under the ROC Curve (AUROC) of 0.85 and an Area Under the Recall Curve

The OSINT-social science process is being carried out by an ethnographic sociologist and technologist (first author), and two students (second and third authors). One of these two students has a BA degree in Anthropology and is a MA candidate in Anthropology, and the other has a BS degree in Sociology and BA in Spanish. Preliminary results of their research have been reported elsewhere [1] [2].

IEEE/ACM ASONAM 2020, December 7-10, 2020
978-1-7281-1056-1/20/$31.00 © 2020 IEEE

of 0.87, and both outperforms and finds bad entities earlier in the rank than existing techniques.

The results above suggest that SRBF can be a promising tool for using existing data sources such as the Panama Papers to efficiently suggest new members for further investigation to public officials. However, SRBF has been only validated by using a list of entities known through opensanctions.org to be associated with bad behavior.

Thus, we argue a need to seek other means to verify the entity ranking provided by SRBF, especially when ranking entities new to our blacklists. Therefore, in this paper, we propose to use a methodology based on Open-source Intelligence (OSINT), informed by ethnographic and archaeological social science, for this process.

In the following sections of this paper we present related research supporting existing computational work on this topic, and mathematical details of the SRBF algorithm, along with experimental results – specifically using the ICIJ Panama Papers database – then related social scientific research and theory underpinning our use of social science methods and OSINT to investigate the rankings of SRBF. We then present several examples that showcase how our proposed methodology is effective in validating the Panama Papers entity ranking provided by the SRBF. We conclude with details of our plans for merging the data scientific and social scientific aspects of this research in ongoing and future work.

II. Related Work

Rabab'ah et al. [9] analyzed the Panama Papers to understand financial transactions in the Middle East. Zheng and Skillicorn [10] studied the structure of the Panama Papers graph through spectral embedding techniques. Both of these studied are not informed by the ground truth about bad entities.

While not applied on Panama Papers, the problem of identifying bad actors in real-world scenarios has been addressed in many contexts such as terrorist networks, criminal networks, and nuclear proliferation networks [11]. The majority of these approaches are based on centrality measures. For instance, Memon and Larsen [12] defined new centrality measures for terrorist networks such as a Position Role Index to discover important roles in the network such as leaders, gatekeepers, and followers, and Dependence Centrality to determine who is depending on whom in a network. Ovelgönne et al. [13] proposed the notion of Covertness Centrality to uncover bad actors that want to hide in the network. The measure, inspired by Lindelauf et al. [14], considers a trade-off between the need to be central and being able to communicate through the network and the need to blend in with the crowd.

Many works focus on the problem of destabilizing criminal and terrorist networks. Petersen et al. [15] proposed a method to remove nodes in criminal networks based on the analysis of the new links generated by the removal. Callahan et al. [16] aimed to reduce the leadership re-generation ability of a terrorist network before performing normal attacks against high-value targets. Spezzano et al. [17] proposed the STONE framework to identify k people to "remove" in a terrorist network in order to minimize the organization's efficiency. The framework leverages the subproblem of who replaces a "removed" individual in the network when computing the solution. Skillicorn [18] considered the problem of retrieving the most suspicion records from large datasets collected by Intelligence and law enforcement agencies. These records are then analyzed by analysts for definitive classification. Andrews et al. [11] developed methods to classify previously unclassified entities as possibly involved in nuclear proliferation.

While OSINT is currently riding a wave of successes, especially following breakthroughs from investigative journalism organizations like the Bellingcat collective of OSINT investigative journalists (https://www.bellingcat.com/), the Digital Forensics Research Lab (https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/), popular podcasts and books [19], and use of OSINT to expose sensitive and even classified information [20], [21], it is at its heart a modern derivative of data collection and analysis strategies common to the classical social sciences and in particular, ethnographic and archaeological research methods. It has even been popularized as "netnography" (a neologism comprised from Internet and ethnography) [22]). It also bears substantial similarity in its usual applications to forensic investigations and detective work [19], [23]. It has also become common in cybersecurity where OSINT-informed "social engineering" has shown to be effective in identifying viable points for hackers to penetrate online security measures [24], [25].

Ethnography is the storied practice of anthropologists who travel to remote lands to "live with and like" a people in order to learn their ways and their values, and to then describe those things in a way that makes it accessible and understandable to those "back home." Archaeology is the practice of studying history in physical form by literally digging into the physical territory of settlements and using interpretive practices for analyzing and understanding arrays of physical artifacts to describe what has happened and why it happened. These classical practices are valuable to OSINT because they share with OSINT the desire to understand events and phenomena that are not straightforwardly visible without specialized interpretive processes and technical knowledge for how to discover and extract meaning from those events and phenomena. Sociological theory and literature is valuable to OSINT because it (sociology) is the study and explanation of both patent and deviant behavior of individuals and groups within modern societal structures and institutions.

On the surface, the principal differences between classical ethnography and archaeology and OSINT have to do with the usual "place" where data are located. Ethnographic research typically happens in a defined geographic place and with an identifiable set of people and things. Similarly, archaeology occurs in a defined physical space. In contrast, the place in which OSINT is applied is almost undefined; it is both everywhere and nowhere because that place is the Internet (however, see [23]). This requires OSINT practitioners to be more creative in identifying what is of interest and why it is of interest, and then to identify "where to go (online)" in

order find data. This is similar to the issues faced when an ethnographer or sociologist wants to study what are termed "hidden populations" made up of elite, distributed, and/or covert individuals and groups who have an interest in avoiding detection of their activities [26]–[28] (something which applies in an investigation such as what we are accomplishing here). Where the fieldworking ethnographer or archaeologist comes "to know" by coming to know the people and the places and the usual ways of activity, where to go, who to talk with, or what to investigate in order to understand what is happening, the OSINT investigator has to develop fluency in abstract technological search tools to track the actions of individuals wherever on the Internet that might be, and digital analysis processes to connect and make sense of the multiple forms of data uncovered. Like a sociologist or a detective, the OSINT investigator has to learn the multitude of imbricated political, organizational, economic, and other systems in which those data are found in order to make sense of them [29], [30], and then to innovate on methods to refine one's own skills as you go [31].

The product of the work of ethnographers, anthropologists, and OSINT investigators is similar also. In all cases the work is largely interpretive and hinges on appropriate applications of abductive, inductive, and deductive forms of reasoning to connect the points of data that can be identified. Value comes from the interpretive and logical quality of inferences we make, and narrative descriptions that encode and elaborate those inferences in ways that make our work understandable and convincing in a world of many competing plausible possibilities [32].

The approach we describe in this manuscript allows us to take advantage of two very distinctive and independently very powerful analytic processes. Computational techniques allow rapid depth-wise analysis of substantial quantities of data and the identification of structural patterns that would be all-but-impossible for humans to accomplish independently. OSINT informed by classical ethnographic and archaeological methods allows us to go beyond the identification of structural characteristics and to use logical analytic skills not yet acquired by computers to create descriptive accounts that support or refute the computational approach. Together these provide convergent tools that enable us to refine what we do as we do it so as to produce a more reliable product.

III. The Panama Papers Dataset

The principal collection of material on the Panama Papers is held by the International Consortium of Investigative Journalism (ICIJ), which was provided these materials through the German news source Süddeutsche Zeitung, which itself was the recipient of 11.5 million documents from Panamanian law firm Mossack Fonseca through an anonymous leak in 2016 (the documents included email correspondence, bank statements, passport photos, etc.). A volunteer team of 30 journalists working under the auspice of ICIJ analyzed these documents and produced a network abstracting their contents. The Panama Papers network [3] consists of 3M entities (individuals, companies, etc.) and 1.4M labeled edges expressing relationships between entities. Within the set of entities, 708K are individuals or companies. The data involves people and companies from more than 200 countries worldwide.

However, material contents of the Panama Papers are not actually publicly available. Instead, only the network can be consulted via the Neo4j graphing tool interface as a means to permit secondary inspection of ICIJ's abstractions. Hence, there should be some concern over the fact that it is not possible to independently analyze the actual leaked documents. The quality of any inference algorithm run on the Panama Papers network hinges on the unknown aspects of ICIJ's work. This provides both a need and an opportunity for a proper verification independent of what ICIJ provides, and at the same time presents a sizeable challenge. ICIJ's presentation of the Panama Papers and subsequent inference would not have been possible without an insider's leak, and then ICIJ's analysis of those data. The challenge in verifying any work based on ICIJ's database arises because the material contents of the leak are unavailable. This means that independent verification must find additional evidence "in the wild" (e.g., via OSINT) to help us verify inference algorithms, as the one described in the next section.

IV. Identifying Bad Entities in the Panama Papers

In our previous work [4], [5], we proposed a new ranking measure, the Suspiciousness Rank Back and Forth (SRBF), that is based on edge directionality alternation to transfer suspiciousness to connected entities in the Panama Papers network. SRBF is an iterative formula that is computed for a given number of iterations K. The intuition behind this algorithm is to avoid to block the propagation of some knowledge because of the edge directionality. Instead, we propagate the knowledge discovered in the previous iterations back and forth by alternating the edge directions in the computation of the proposed measure.

Given an unlabeled directed graph $G = (V, E)$ and a set $B \subseteq V$ of known bad entities, SRBF is given by the following equations:

$$\begin{aligned} SRBF^0(u,B,G) &= (1-\delta)b(u,B)+ \\ &+\delta \textstyle\sum_{(v,u)\in E} \frac{SRBF^0(v,B,G)}{|\{u'|(v,u')\in E\}|} \\ \text{where } b(w,B) &= \begin{cases} 1/(2\times|B|), & \text{if } w \in B \\ 1/(2\times|V\setminus B|), & \text{otherwise} \end{cases} \end{aligned}$$

$$\begin{aligned} SRBF^t(u,B,G) &= (1-\delta)b(u,B)+ \\ &+\delta(1-\alpha)SRBF^{t-1}(u,B,G^T)+ \\ &+\delta\alpha \textstyle\sum_{(v,u)\in E} \frac{SRBF^t(v,B,G)}{|\{u'|(v,u')\in E\}|} \end{aligned}$$

At the first iteration ($t = 0$), the suspiciousness rank of an entity $u \in V$ is computed as the recursive equation $SRBF^0$ inspired by the PageRank algorithms where the more a node is connected to suspicious nodes, the higher its initial suspiciousness rank is. It is thus a type of taint-calculating

TABLE I
AUROC RESULTS. SHADED CELLS DENOTE THE BEST VALUE FOR THE COLUMN. BOLDED VALUES ARE THE BEST IN THE WHOLE TABLE. DC: DEGREE CENTRALITY; LCC: LOCAL CLUSTERING COEFFICIENT; EC: EIGENVECTOR CENTRALITY; ACCM: DC+LLC+EC+PR; PR: PAGERANK; SR: SUSPICIOUSNESS RANK.

		Method									
Graph		TransR	Node2Vec	DC	LCC	EC	PR	ACCM	SR		SRBF
Original (G)		0.798	0.691	0.674	0.512	0.300	0.790	0.682	0.499	(G,G^T)	0.682
Reverse (G^T)		0.808	0.764	0.674	0.512	0.641	0.821	0.658	0.826	(G^T,G)	**0.851**

step. $b(w, B)$ is a bias introducing the label of an entity being suspicious or unknown. Since in our setting $|B| << |V \setminus B|$, i.e., the number of suspicious entities is much lower than the one of the unknown entities, the bias results higher for suspicious entities than unknown ones. In contrast with the PageRank, in our formulation, the bias is not the same for each entity.

In subsequent iterations, we reverse the graph G and compute a suspiciousness rank where we introduce two sources of bias instead of just one. The first bias is the same as $SRBF^0$'s bias. The second bias is given by $SRBF^{t-1}(u, B, G^T)$ and it is equal to the $SRBF$ score computed for the node u at the previous iteration, i.e., by considering the reverse graph. In practice, we propagate the information back and forth. In the above formulas, δ is the damping factor as in classical PageRank and α is a factor deciding the importance of the previous computation. We set $\delta = 0.85$ and $\alpha = 0.8$.

It is possible to show that $SRBF^t$ converges in a finite number of iterations since they can be reduced to irreducible aperiodic Markov chains. Also, there exists a finite number of iterations K such that $SRBF^{K-2} = SRBF^K$.

Experimental Results: To validate our proposed Suspiciousness Rank Back and Forward, we used a one-class machine-learning based approach where we did an extensive comparison of all the existing techniques (centrality measures and embeddings) and our proposed ranking measure. We will also explore the importance of the edges' directionality by computing the measures and the node embeddings in the original graph G and the reversed graph G^T. We also tried considering the graph as undirected, but the results were worse than the ones presented here. In addition, we also included the rank computed by the SRBF at the first iteration (*suspiciousness rank* (SR)), and used it as a baseline to empirically show the benefits of the back and forward process. For each case, we performed a 10-fold cross-validation experiment in which 90% of the blacklist was used as training data and the remaining 10% was used to test. This 10% of users used as test set were marked "unknown" in the training set. As we have one class of ground truth only, i.e., the blacklist of bad entities, we used One-class SVM as our classification model and compared the results according to the AUROC and the Area Under the Recall Curve. The Recall Curve is obtained by computing the recall@k for k varying in $\{1, 2, \ldots, |V|\}$. The idea of behind this curve is to have a budget k, corresponding to the number of people that is possible to investigate and show how the recall of the algorithm varies according to this budget.

Table I shows a comparison of AUROC values for each method and graph. The best method that maximizes the AUROC is SRBF with a value of 0.85, when initially applied on G^T. It is worth noting that the edge directionality is really important in the outcome of the experiments. As it can be observed in Table I, there exist a substantial performance gap between the results of the original graph G and the reversed graph G^T. This difference exists in all tested methods except the ones that do not consider edge direction (e.g., DC and LCC). Thus, the direction of the edges is crucial in order to describe what the particular entity is doing. The experiments for the recall curve show that SRBF is able to detect a greater number of bad entities earlier in the rank than the competitors, achieving an Area Under the Recall Curve of 0.870 compared to the 0.847 of the second best model, i.e. the Pagerank.

Overall, our experimental evaluation shows that SRBF outperforms the well-known PageRank measure (that is the best baseline) on the task of identifying known bad entities in the Panama Papers.

V. USING OSINT TO SUPPORT SRBF

In the previous section, SRBF is shown to achieve good performance when evaluated against a list of known bad entities. However, we lack a proper validation strategy for many entities that appear high in the rank, but that are unknown as they are not listed in any public blacklist. Therefore, we propose to use Open-Source Intelligence (OSINT) as a modern derivative of inductive social science research methods as a possible verification strategy for unknown entities (i.e., where ground truth is not provided). Specifically, our methods parallel conventional interpretations of digital ethnographic and archaeological research [22] augmented by ongoing developments in OSINT [19].

Accomplishment of OSINT relies on adaptation of well-established ethnographic and archaeological practices to accomplish inductively-informed online foraging. To do this we employ common and special purpose search tools to "find what others have left behind" in their day-to-day operations as individuals and members of organizations of various kinds, both private and public. The "others" are entities and individuals who are the focus of investigation. The fundamentals of archaeological and ethnographic data collection and analysis involve "going where they go" and looking for evidence documenting their activity and the activities of those they interact with.

Because this process is accomplished online, our "going where they go" involves searching online through common

social media as well as paywall restricted archives, and Pastebin-type sites where anonymous individuals may deposit material they have found online. Typical artifacts include official documents produced in bureaucratic processes (for example, E-mails of professional correspondence describing plans and situated activities, databases displaying a particular way of categorizing data, budget and other kinds of audit documents, contracts, photographs, etc.), personal documents (for example, social media postings including photos and videos displaying social events and members of peer networks, avocational activities that blend with work activities, and the like). Analysis involves inspection of those artifacts to find details that permit inductive reconstruction of shared activities in time and space as reflected across several or many of these artifacts – what happens, when it happens, and where it happens. As analysis allows these elements (what, when, where) to be described in more detail, one starts looking for overlapping evidence across locations, time frames, and actions of others in or around the same phenomena. This results in a qualitatively complex network of data connected through abductive and inductive coding and logic (see Figure 1 for an example of this network) that allows inductive conclusions to be made about the individuals/entities in the network and the network itself.

The glue that holds these things together is descriptive narrative built upon those logical determinations. As more data can be defensibly woven into the narrative and those stories intersect with the reason those actors and entities are the subject of analysis, we build support for our suspicions.

We began our process by looking for evidence on individuals/entities that have been arrested or otherwise implicated in illegal activity as reflected in the blacklists and SRBF results. In early stages this allowed us to focus on refining our data collection processes without necessitating our own independent determination of the "ground truth" of bad behavior. We reasoned that if we could independently locate evidence consistent with something already safely considered ground truth then our methods were appropriate for the overall task.

In order to improve our chances of locating something of use, each of the first three co-authors of this paper selected several individuals/entities in the top 100, between rank 225 and 250, and between rank 450 and 500, from the blacklists which were also ranked by SRBF. We investigated these individuals/entities independently and met weekly to report our results and compare notes. We determined that whichever of these investigations uncovered useful leads first, would become our shared focus.

One of us located a trove of E-mail correspondence involving individuals in a company operated by an individual and another company on the blacklists in the top 250 entities on SRBF's entity ranking. As with any discovery oriented process in social science we first "took inventory" of the data by (a) sorting the trove of correspondence into sequence according to date and time. We then (b) identified the nominal focus of each message and (c) located geographic place references on a Mercator projection map that enabled accurate measurement of space, and (d) identified and located on the map other individuals, companies and activities implicated in each message.

With this "inventory" of time, space, and actors, we could then begin searching for related details about those organizations and related individuals and activities that transpired somewhere around the same time(s) and place(s). This process follows the conventional focus of ethnographic and archaeological research around the three-part framework of time, space, and actors/actions.

With these concrete displays encoding time, space, and actors/actions, as we found additional related details we were able to elaborate on our initial inventory displays to add detail to our diagrams and draft speculative narratives of how the same people and things somehow intersected in time through particular activities (for example, see Figure 1).

At each point we compared the individuals and entities we found with those identified as suspicious by SRBF. We identified individuals and entities high on the SRBF ranking (including positions 31, 113, and 3976). We have a total of 708K entities. However, we also found that some of the individuals named in those documents were not in the Panama Papers. Based on the type of activities in which we found them in the data, those others often seemed to be clerical or other professional staff involved in what was for them routine activities and transactions on behalf of their employers. As the list of those unknown actors grew, the frequency with which some of them appeared in the documents increased. We developed the hunch that these individuals were part of the administrative apparatus of organizations high on the SRBF ranking, thus key in the mundane tasks involved in illegal corporate activity. With this, they became the focus of additional searches. Identifying additional involvement of those administrative operators could expose deeper or more frequent involvement in activities justifying their employers' and companies' placements in a high position by the SRBF ranking.

From the standpoint of ethnographic methodology and especially in forensic analysis of data, searching for activity of relative "underlings" as opposed to searching for more powerful figures is warranted with the idea that those underlings and their employers may be much less concerned with taking steps to obscure their activity than would be the more powerful and identifiable figures. By focusing our OSINT searches in this way, we hoped to find indirect links that would help us accomplish our goal of finding evidence to support SRBF. As indicated below, this resulted in some valuable findings.

VI. Results: Examples from our OSINT in support of SRBF

As an example of our findings, we have found materials independently implicating individuals and three companies accused of involvement in breaching 2011 United Nations embargoes and sanctions on the Syrian regime by delivering fuel oil to the Syrian government for use in its civil war.

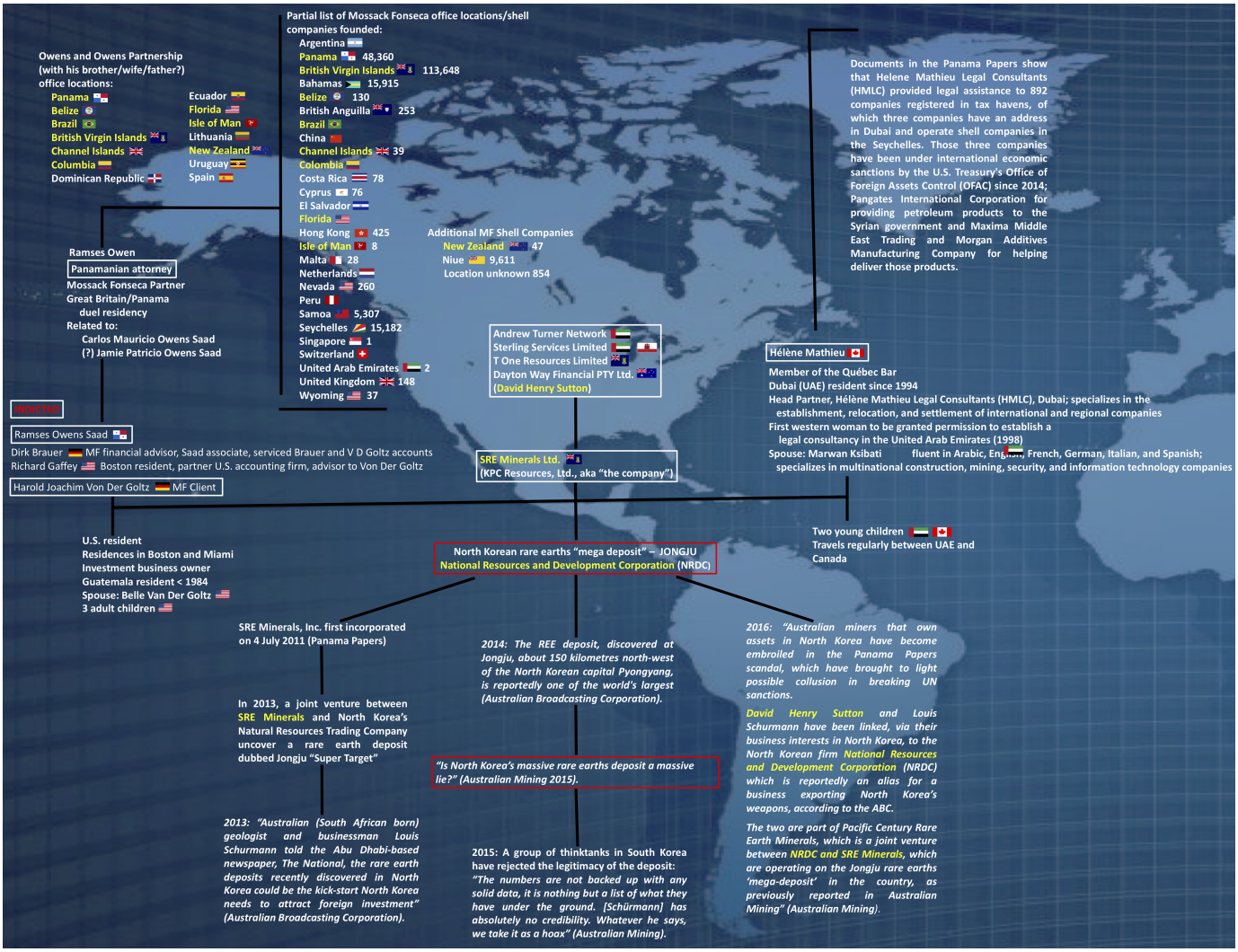

Fig. 1. Examples of Data and Connections Produced through OSINT Methods [2]

The three companies (Maxima Middle East Trading, Morgan Additives Manufacturing and Pangates International, ranked 247, 117, and 126 by SRBF, respectively, and on list of known bad actors) and individuals in positions of authority or acting on their behalf (including individuals at 141 on SRBF's list of known bad actors, and 113 on the list of unknown actors) are reflected in a collection of E-mail correspondence, photographs, social media postings, a disconnected set of news reports, and other materials that were discovered using OSINT methods. Importantly and as mentioned above, this collection was assembled from multiple sources by searching for names of the individuals we characterize above as underlings or administrative personnel. Focusing our searches on those individuals proved to be helpful in finding documents of relevance to our work. Analysis of the contents of these materials results in inductive support for the actual events of legal action against those companies and their principals, and thus the placement of those entities and their principals high on the SRBF ranking.

Specifically, our trail of evidence in this case begins in Nigeria, with E-mail correspondence between local officials and individuals at the organizations located at the positions noted above on SRBF's ranking. The correspondence was found in several corporate online databases associated with organizations in Nigeria and Italy and Pastebin-type collections unrelated to those organizations. This correspondence focused on fees and powers of attorney necessary for registration of a tugboat under the authority of a company we traced to a set of holdings associated with tanker ships and other individuals involved in 2011 illegal shipments of material to Syria. Tugboats are essential for guiding barges and large ships through shipping ports with high traffic, and Lagos, Nigeria is such a port and also a hub for shipments of material that was delivered illegally to Syria in 2011.

One of the individuals involved in this correspondence is located at 6856 on SRBF's ranking but is not a known bad actor using opensanctions.org. However, most of the people interacting in this correspondence are not on the Panama Papers or known blacklists. According to details in E-mail

headers and signature blocks, the one individual not belonging to the list of known bad actors is involved in this correspondence on behalf of a known bad actor entity which appears very high SRBF's ranking. Subsequent OSINT to locate more information about this individual found additional evidence showing involvement in other work of the same sort for that entity, but also enabled verification of previously unknown individuals high in the ranking. Focusing our OSINT on those previously unverified as bad actors led to more documents that could be abductively and inductively linked to the illegal shipments and other activities still being investigated.

The above accounts highlight two important items that support utility of OSINT in this case. First, we hypothesized that successful movement of material illegally would be facilitated by control not only of the freighters, but also vessels and "touch points" from port to port. Since a tugboat is essential in such a process, we considered the co-incidence of details related to the tugboat, including shared location with freighters and materials, and corporate connections between individuals involved, as supportive of placement of individuals and organizations high on the SRBF's ranking. Second, as stated above, locating documents naming staff members involved in workaday administrative duties for the case provided the opportunity to see if we could identify more information that would show how such individuals were involved in activities involving other entities high on SRBF's rankings. While our successes in this regard has not yet been conclusive, we can report anecdotal evidence supporting the idea that our OSINT is actually aided by looking for traces of evidence identifying actions by underlings rather than the main figures themselves.

Initially independent of the above, in an earlier stage of our OSINT we had found information related to an engineering company and pipeline construction company that was involved in building facilities to carry the same sorts of materials across Lebanon into Syria. Through our OSINT, we can identify links between these companies, and the company accused of illegal shipments of oil to Syria and an individual at 117 on the SRBF ranking. Remarkably, the engineering company and pipeline company are not included in either the Panama Papers or in SRBF's rankings or blacklists used in SRBF's process.

In our OSINT, we located one E-mail message from one of the apparent underlings involved in the tugboat correspondence, who was also involved in correspondence related to this engineering company and construction company. This provided a link in the overall path of illegal shipments to Syria.

The result of all this was an OSINT-produced set of data allowing us to independently support placement of four unknown entities high on SRBF's ranking. This tracking of actions by individuals across space and time reflects observations that have been made by ICIJ and others [33]. Together, these examples provide evidence that our methods are able to provide independent support for SRBF as described above.

Anecdotally related to the above is evidence discovered in our OSINT that one of the principals involved in the illegal movement of material to Syria is now under house arrest in that country. That individual is located at position 113 on SRBF's ranking and does not belong to the list of bad actors. Information identified through OSINT indicates that this individual has run afoul of the favor of rulers in the region and that is why he is currently held. While our OSINT does not allow us to make such claims with confidence, we wonder if this individual's house arrest serves a purpose of protecting that individual from legal prosecution that could expose other issues.

Finally, it is relevant to indicate that the unknown individual at position 3976 on the SRBF ranking is Ramses Owens, a Panamanian lawyer who worked for Mossack Fonseca and left shortly before the leak of documents that broke the Panama Papers. Owens was indicted in 2018 along with two others by the United States Department of Justice for a range of charges including conspiracy to commit tax evasion, wire fraud, money laundering conspiracy, and conspiracy to defraud the United States[1]. While unrelated to the contents of this paper, we take this to be additional support for Owens' appearance high on the SRBF list. As such, it should be considered another argument in favor of the quality of SRBF. We are pursuing other leads arising from this indictment that appear to connect to other unknown individuals high in thr SRBF's ranking.

VII. Conclusions

Principal goals of the work described here were to develop and test an independent methodology based on archaeological and ethnographic social science methods and OSINT for offering verification of (a) presence and (b) relative position of suspected bad actors on ranking produced by the SRBF algorithm. In both the computational and the social scientific aspects of this research we started with ICIJ's Panama Papers dataset. The computational aspect of the research used blacklists of known bad actors from opensanctions.org as a reference. The social scientific and OSINT aspects of the research made use of qualitative investigation techniques available on the open World Wide Web to develop, prototype and test an independent methodology for verifying the results of SBRF.

Through OSINT informed by classical archaeological and ethnographic perspectives we have been able to provide independent verification of connections both in ICIJ's reporting and selected entities high in the SRBF ranking, and hence suspected of being bad actors. Importantly, this also involves identification of links to other individuals or entities that are not named in ICIJ's data or opensanctions.org. In our OSINT some of these previously unidentified persons have provided new links between other known individuals and entities. In this latter case, the entities are in ICIJ's data but not shown by ICIJ to be linked in the ways our OSINT work has uncovered. Our work thus provides tacit support for the SRBF ranking, and because of the quality of those new links even provides supportive evidence for the rankings themselves.

Critiquing our own work, we want to emphasize that our inductive processes work on data "in the wild" and does

[1] See https://www.justice.gov/opa/pr/four-defendants-charged-panama-papers-investigation-their-roles-panamanian-based-global-law

not depend on the existence of pre-formatted data formatted like that found in the ICIJ Panama Papers trove and opensanctions.org. This is both its strength and its weakness. It is a strength because it does not rely on pre-categorized data that cannot be independently vetted for accuracy. It is a weakness because it requires – at present – highly time- and labor-intensive search and analysis processes by individuals with both particular social science knowledge and skills, and particular technical skills related to the use of OSINT tools.

For these reasons we are not yet able to offer a large quantity of data to aid in verifying SRBF across its entire span, as its results may vary across its full span of rankings. We are also unable at this point to offer a means for automating our social scientific and OSINT processes so they may be used with sufficient speed, and at sufficient scale to act as a viable companion or component of computational investigations.

As a consequence, while we have shown initial successes, substantive time and resource demands required by our social science and OSINT does not yet provide a method that can be automated to the point where it can be easily coupled with the SRBF process as a verification tool. With our progress as evidence of the promise of our methods toward the goal of providing independent verification of tools like that provided by SBRF, in the next phase of the combined research we are pursuing methods of using computational techniques to automate portions of the initial phases of the social science and OSINT components of the work.

However, with results reported here, we show that social scientific methods and OSINT provide independent verification of SBRF and its ranking of entities provided in ICIJ's Panama Papers database. It is thus able to add substantive value by improving the reliability and safety of tools like SRBF.

ACKNOWLEDGEMENTS

Support for the OSINT-social science aspects of this research was provided by a "2020 Research Seed Grant" provided by the Office of the Dean in the Boise State University, College of Engineering.

REFERENCES

[1] D. Winiecki and B. Hay, "Inductive qualitative social science research as a necessary element of data science." Pacific Sociological Association, Apr 2019.

[2] D. Winiecki, K. Kappelman, and B. Hay, "Inductive qualitative social science research as a necessary element of data science." Society for Applied Anthropology, Mar 2020.

[3] https://offshoreleaks.icij.org/pages/database.

[4] M. Joaristi, E. Serra, and F. Spezzano, "Inferring bad entities through the panama papers network," in *IEEE/ACM 2018 International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2018, Barcelona, Spain, August 28-31, 2018*. IEEE Computer Society, 2018, pp. 767–773.

[5] ——, "Detecting suspicious entities in offshore leaks networks," *Social Netw. Analys. Mining*, vol. 9, no. 1, pp. 62:1–62:15, 2019.

[6] http://www.opensanctions.org/#downloads.

[7] A. Grover and J. Leskovec, "node2vec: Scalable feature learning for networks," in *SIGKDD*, 2016, pp. 855–864.

[8] Y. Lin, Z. Liu, M. Sun, Y. Liu, and X. Zhu, "Learning entity and relation embeddings for knowledge graph completion," in *AAAI*, 2015, pp. 2181–2187.

[9] A. Rabab'ah, M. Al-Ayyoub, M. A. Shehab, Y. Jararweh, and B. J. Jansen, "Using the panama papers to explore the financial networks of the middle east," in *11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, Barcelona, Spain, December 5-7, 2016*, 2016, pp. 92–97.

[10] Q. Zheng and D. Skillicorn, *Social Networks with Rich Edge Semantics*. CRC Press, 2017.

[11] I. A. Andrews, S. Kumar, F. Spezzano, and V. S. Subrahmanian, "SPINN: suspicion prediction in nuclear networks," in *2015 IEEE International Conference on Intelligence and Security Informatics, ISI 2015, Baltimore, MD, USA, May 27-29, 2015*, 2015, pp. 19–24.

[12] N. Memon and H. L. Larsen, "Practical algorithms for destabilizing terrorist networks," in *Intelligence and Security Informatics, IEEE International Conference on Intelligence and Security Informatics, ISI 2006, San Diego, CA, USA, May 23-24, 2006, Proceedings*, 2006, pp. 389–400.

[13] M. Ovelgönne, C. Kang, A. Sawant, and V. S. Subrahmanian, "Covertness centrality in networks," in *International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2012, Istanbul, Turkey, 26-29 August 2012*, 2012, pp. 863–870.

[14] R. Lindelauf, P. Borm, and H. Hamers, "The influence of secrecy on the communication structure of covert networks," *Social Networks*, vol. 31, no. 2, pp. 126–137, 2009.

[15] R. R. Petersen, C. J. Rhodes, and U. K. Wiil, "Node removal in criminal networks," in *European Intelligence and Security Informatics Conference, EISIC 2011, Athens, Greece, September 12-14, 2011*, 2011, pp. 360–365.

[16] D. Callahan, P. Shakarian, J. Nielsen, and A. N. Johnson, "Shaping operations to attack robust terror networks," in *2012 International Conference on Social Informatics (SocialInformatics), Washington, D.C., USA, December 14-16, 2012*, 2012, pp. 13–18.

[17] F. Spezzano, V. Subrahmanian, and A. Mannes, "Reshaping terrorist networks," *Communications of the ACM*, vol. 57, no. 8, pp. 60–69, 2014.

[18] D. B. Skillicorn, "Computational approaches to suspicion in adversarial settings," *Information Systems Frontiers*, vol. 13, no. 1, pp. 21–31, 2011.

[19] M. Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. inteltechniques.com, 2019.

[20] A. Dascalescu, "Strava heat map incident: How civilian technology in military settings needs to be controlled," Aug 2018. [Online]. Available: https://www.cpomagazine.com/cyber-security/strava-heat-map-incident-how-civilian-technology-in-military-settings-needs-to-be-controlled/

[21] H. I. Sutton, "Military security could be compromised by surprising app," May 2020. [Online]. Available: https://www.forbes.com/sites/hisutton/2020/05/20/military-personnel-exposed-by-unlikely-social-media-app/

[22] R. Kozinets, *Netnography: Doing ethnographic research online*. SAGE Publications, 2010.

[23] J. Holden-Rhodes, *Sharing the secrets: open source intelligence and the war on drugs*. Praeger Publishers, 1997.

[24] C. Hadnagy and G. Media, *Social Engineering, Second Edition: The Science of Human Hacking*, 2018.

[25] M. Erbschloe, *Social Engineering: Hacking Systems, Nations, and Societies*, 1st ed. CRC Press, 2019.

[26] S. Schensul, M. LeCompte, R. Trotter, E. Cromley, and M. Singer, *Mapping Social Networks, Spatial Data, Hidden Populations*, ser. Ethnographer's Toolkit. AltaMira Press, 1999, vol. 4.

[27] S. Brayne, "Big data surveillance: The case of policing," *American Sociological Review*, vol. Prepublished August 29, 2017, 2017.

[28] N. Fielding, "New data and old dilemmas: Changes and continuities in online social research," *Qualitative Inquiry*, vol. 25, no. 8, p. 761–772, 2019.

[29] H. S. Becker, *Outsiders: Studies in the Sociology of Deviance*. The Free Press, 1963, deviance Rule making / makers Rule enforcing / enforcers moral enterprise moral crusade popular illegalities.

[30] S. Kleinknecht, "Hacking hackers: Ethnographic insights into the hacker subculture-definition, ideology and argot," Ph.D. dissertation, McMaster University, 2003. [Online]. Available: http://hdl.handle.net/11375/10956

[31] D. Winiecki, *Using ethnographic forms of research to study the social world and to make social theories studyable*. Nova Science Publishers, 2009, p. 5–57.

[32] J. Van Maanen, *In Pursuit of Culture*. Chicago University Press, 1988, p. 13–44.

[33] J. O'Donovan, H. F. Wagner, and S. Zeume, "The value of offshore secrets: Evidence from the panama papers," vol. 32, p. 4117–4155, 2019. [Online]. Available: https://doi.org/10.1093/rfs/hhz017