A Framework to Reveal Clandestine Organ Trafficking in the Dark Web and Beyond

Michael P. Heinl
Department of Computer Science, Volgenau School of Engineering, George Mason University,
mheinl@gmu.edu

Bo Yu
Department of Computer Science, Volgenau School of Engineering, George Mason University,
byu3@gmu.edu

Duminda Wijesekera
Department of Computer Science, Volgenau School of Engineering, George Mason University,
dwijesek@gmu.edu

A Framework to Reveal Clandestine Organ Trafficking in the Dark Web and Beyond

Cover Page Footnote

A FRAMEWORK TO REVEAL CLANDESTINE ORGAN TRAFFICKING IN THE DARK WEB AND BEYOND

Michael P. Heinl[1,2], Bo Yu[1], Duminda Wijesekera[1]

[1]George Mason University
Department of Computer Science
Fairfax, VA 22030, USA
{mheinl, byu3, dwijesek}@gmu.edu
[2]University of Ulm
89081 Ulm, Germany

ABSTRACT

Due to the scarcity of transplantable organs, patients must typically wait on long lists for many years to get a matching kidney. This scarcity has created an illicit marketplace for wealthy recipients to avoid long waiting times. Brokers arrange such organ transplants and collect most of the payment that is sometimes channeled to fund other illicit activities. In order to collect and disburse payments, they often resort to money laundering-like schemes of money transfers. As the low-cost Internet arrives in some of the affected countries, social media and the dark web are used to illegally trade human organs. This paper presents a model to assess the risk of human organ trafficking in specific areas and shows methods and tools to discover digital traces of organ trafficking using publicly available tools.

Keywords: Clandestine Organ Transplants, Organ Trafficking, Probabilistic Risk Model, Dark Web Crawling

1. INTRODUCTION

Due to the lack of transplantable organs, patients must wait on transplant lists for many years (sometimes six years for kidney transplants) and some die during the waiting periods of their transplants. In order to avoid this long wait, wealthy patients buy organs from poor people in countries that legally or illegally enable such transplants. Some hospitals and clinics do not enforce legal restrictions on such transplants, thereby facilitating a clandestine marketplace for illicit organ trade. Based on the findings from analyzing the collected organ trafficking data, the prices for kidneys have been more than doubled between 2008 and 2015, and prices for livers have also increased by the same absolute amount as kidneys. These higher profits attract more illegal organ trafficking around the world. However, interviewees of one study stated that although buyers pay more, sellers get far less for their organs. In addition, some recipients tend to become brokers at a later stage. Many researchers investigated clandestine organ trades have discovered that health conditions of sellers deteriorate after

clandestine sales and are subjected to social stigma so that they eventually regret their sale in 94% of the cases (Mijovic-Das, 2011).

According to Fraser (2016), the numbers of kidneys sold on social media have increased since 2010. One reason for this development is the "[...] uptake of low-cost internet access in source countries of trafficked individuals." There is a clear shift from buyers dealing with online rather than in-person brokers, that is in keeping with global trends, and additionally provides a layer of protection from law enforcement for brokers. Furthermore, direct contact using social media is beneficial for organ sellers and buyers because they can avoid high brokerage costs. Although kidneys are still sold in specific social media groups since 2015, administrators have started to block organ trade conducted on their social media platforms. Furthermore, due to the increasing awareness of the digital footprint left by sellers and buyers, more middlemen use hidden services in the dark web to arrange such illegal trading of human organs, as well as resort to using money laundering schemes to collect and disburse the majority of the payments.

The objective of our effort is to predict the evolution of organ trading networks, so that we can suggest some deterrent mechanisms for spreading clandestine organ transplants. One such deterrent mechanism proposed during a survey was to have a system to anonymously report patients during pre-transplant and post-transplant stages using an established system, as more drastic actions would be counterproductive to the treatment and well-being of recipient patients. In order to achieve our objective, we use some known data collected by translating hand-written notes produced by on-site investigators, in addition to mining dark web forums and marketplaces to create an organ trading risk model.

2. RELATED WORK

Human trafficking, sometimes referred to as modern slavery (Koettl, 2009) in the 21st century, continues to be a challenge to the international community. Many researchers and organizations concentrate their efforts to reduce human trafficking around the world. Mo introduced an aspiration-based model of human trafficking vulnerability in (Mo, 2018). The author expounded that an increased salience in relative deprivation can lead individuals to seek more risks, thereby subjecting themselves and their children at greater risk of being exploited. Furthermore, Aronowitz, Theuermann, and Tyurykanova (2010) investigated criminal gangs and their modus operandi using evidence-based research. They show that other factors, such as economic and social forces can also increase potential victims' vulnerability. Consequently, the more knowledge of involved factors in the human trafficking chain are available the better predictions can be produced and accurate warnings for early interventions provided.

About 0.3% of reported human trafficking cases involve organ trafficking, and persons trafficked for organ removal have been detected in 16 countries in all regions of the world according to the *Global Report on Trafficking in Persons* (United Nations Office on Drugs and Crime, 2014). Some tools have been developed to support the combat against organ trafficking. For example, the Coalition for Organ Failure Solutions (COFS)[1] developed the online reporting tool *XDOT* (eXpose and Disrupt Organ Trafficking), to collect and analyze case reports and examine linkages and patterns around the activities of human trafficking for organ removal. Although "an ounce of prevention is worth a pound of cure", the comprehensive

---

[1] http://cofs.org/home/

studies in organ trafficking are far behind as mentioned in (Aronowitz et al., 2010). We take such a challenge by developing a risk model of organ trafficking which associates with the amount of estimated damage. This risk model is meant to model real-world actions of organ trafficking in order to identify the potential organ traffickers which will help to intervene or even prevent the organ trafficking.

3. UNDERSTANDING ORGAN TRAFFICKING

To get an understanding of the complex process and impact of diverse attributes on human organ trafficking, this section summarizes existing research (Fraser, 2016; United Nations Office on Drugs and Crime, 2014, 2015; Ambagtsheer & Weimar, 2016; Gerken & Wagner, 2016; Yousaf & Purkayastha, 2016) and knowledge gathered during interviews with subject-matter experts. Due to its nature, human organ trafficking involves many logistics. However, a large part of this paper deals with the steps performed and the traces left in the digital world. Nevertheless, focusing on these traces and following the resulting electronic communication chains can provide indications that may support and lead to real-world investigations.

3.1   Actors

Many people with diverse backgrounds are involved in human organ trafficking. Figure 1 visualizes the relationships between four main roles in organ trafficking. The following paragraphs furthermore characterize them as well as their motivations:

- *Buyers:* Buyers of human organs are most likely patients from richer countries suffering from diseases such as renal insufficiency. Due to the limited storage
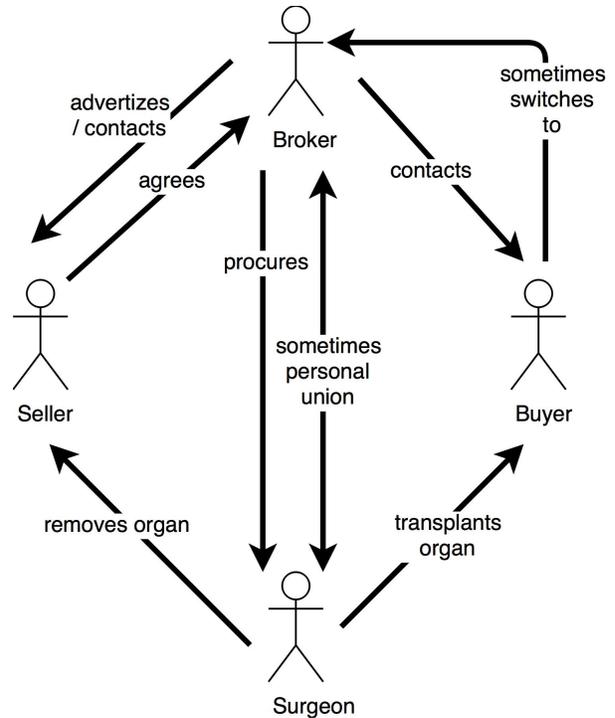
Figure 1. Main actors in the organ trafficking process and their relationships.

and transportation capability, it is unlikely that organs are physically bought with the intention to resell them after removal. Rather, buyers and sellers/donors are brought to the same location by brokers and the transplant is done by surgeons who also financially benefit from the procedure.

- *Sellers/Donors:* Sellers of organs are often poor, young males. While some sellers proactively search for opportunities to sell their organs to make money (either autonomously or motivated by their socioeconomic environment), others are attracted by advertisements offering money without clearly stating that the actual return is an organ removal. Another constantly increasing group are young refugees who are paying their own trafficking costs with organs.

- *Brokers:* Brokers are the central actors holding together the whole organ trafficking network. They are also the group financially benefiting the most. While sellers get a four to a low five-digit amount in US dollars, the buyers often pay a six-digit amount in US dollars for an organ.

- *Transplant Surgeons/Hospitals:* Although breaking legal and ethical standards, there are medical professionals that willingly transplant trafficked organs benefiting from the high prices payed for organs.

Additionally, several other actors may potentially participate in actions facilitating the organ trafficking process, such as arranging fake visas and passports, laundering the money paid for the trafficked organ, or providing covered or pre-textual transportation. Involvement of those groups varies from case to case. Due to their economic situation and the lack of awareness on the risks associated with trafficking and transplantation, sellers are regularly the most vulnerable party in the illegal organ trade system. Hence, the investigations' main focus should be on protecting these individuals.

3.2 Activities involved in the Organ Trafficking Process

Brokers play a significant role in organ trafficking. Sellers and buyers typically never communicate or meet in-person before the actual transplantation begins. Even at the time of the transplantation, they are usually not introduced. Rather, usually their single point of contact is the broker. Sometimes former buyers become brokers in order to get back the oftentimes high debts incurred in getting their own transplants. Surgeons that have already been involved in the transplanting of trafficked organs refer new patients to

old ones in order to reach out to their former sources/brokers. Hence, some surgeons themselves also act as brokers.

The process described so far depends on already established social relations between brokers, surgeons, and their current as well as former patients. Communication between these groups is usually private and not publicly analyzable. However, there are also exemplary scenarios in which actors have to communicate their desires to a broader audience:

- An ill patient desperately searching for a specific organ and has not established any connections to any person who is already involved in organ trafficking.

- A broker who has a potential buyer but has no available a seller yet.

Because organ trafficking cannot be openly advertised in the surface web, all groups of actors use more private channels of communication, bringing social media (deep web) and the dark web into play. In this case, the process can be generalized (approximately) as follows:

1. First contact using social media groups or dark web forums/markets.

2. Switching to another, more private channel which is usually using mobile messengers or email.

3. Negotiate terms and conditions.

4. Trafficking the donor to a safe house which is close to the surgical theater.

5. Prepare the donor and the recipient for the transplant.

6. Carry out the transplant.

Apparently, the presented process of organ trafficking is very dynamic. It cannot be directly applied to the data obtained from the dark or deep web. Usually, only the first step and its transition to the second step can be obtained without extended legal and operational capabilities. Hence, we focus on detecting clandestine indicators which can be used to enrich a risk model and to contingently start further investigations. To do so, we first extensively search the dark web for specific initial keywords using the methodology and tools described shortly. Then, we use the indicators found to derive additional keywords and focus on the most suspicious hidden services.

4. REAL-WORLD DATA COLLECTION

We received the organ trafficking data, in the form of summarized interviews from one of our collaborators. There are about 500 records that include basic information, such as operational location, nationalities, gender, and/or age of buyers and sellers, etc. Based on the collected data, we can understand the factors which may induce organ trafficking.

Answers of donors who stated to believe that they were smuggled into the hospital and specifically told to lie about the procedure of the transplantation are just one example of data we used in this study. Analyzing the years in which these statements were recorded, we found out that prior to 2011, transplantation procedures were more openly conducted and have become more clandestine after that year because law enforcement started to focus more on this issue. Hence, there was little need to smuggle buyers into the hospital prior to 2011. However, the data shows a shift from 2011 onward of buyers being smuggled into hospitals. There is clearly a progressive effort by surgeons and hospitals to avoid detection by authorities. Therefore,

political factors should be involved in creating a risk model for organ trafficking, as we did in this project.

During our research, we studied the Fragile States Index (FSI) (Fund For Peace, 2017) to quantify some aspects of political and social turmoil that may enhance organ trafficking risks. We found out that many factors are common between our risk model for organ trafficking and FSI. We also observed better views of relationships among the factors by analyzing the FSI. For example, in the questionnaire, the payment flow can be one of three categories: (1) cash payment to brokers or cash payments to surgeon, (2) bank account transfers, and (3) using online funds transfer company. We learned from the responses collected during interviews carried out in Egypt that kidney buyers in this country typically use multiple payment methods and those payment patterns for kidneys traded in Egypt have changed considerably since 2008. Importantly, there will likely be multiple payments made in each category. The idea of this appears to be ensuring that no single traceable transaction exceeds $10,000. Similar strategies are used in money laundering so that the involved banks do not necessarily trigger a report to the authorities. More importantly, the changes in payment methods from 2008–2016 indicate the current relationships among payments, brokers, and surgeons as we will discuss next.

Up until 2011, in Egypt, the surgeons were at the top of the trafficking hierarchy. The surgeons arranged the kidney donor/seller pairs, and received all payments directly from the sellers or their appointed brokers. The brokers were agents for or employees of the surgeon. From 2012 onward, kidney donors/sellers have been primarily sourced from Syria. Previous payments were made directly to Egypt whereas they afterwards have been directed to third countries instead. The brokers are now in charge of the traffick-

ing operations and the surgeons who perform the transplants are now employees of the brokers. Buyers from the USA, Japan, Turkey, and Germany often meet a broker in their home country before traveling to Egypt and payments are made to this broker. These brokers in the buyer's home country claim to be previous buyers of a kidney. They convey a sense of security and genuine sales. They check that the client is a bonafide buyer (not media, researchers or law enforcement), provide details of the transplant procedure and attempt to close the deal with the client. Such relationships should be taken into account during the development of our organ trafficking risk model.

5. DARK WEB DATA COLLECTION

There are three terms regularly used to categorize websites. The first category of websites is the so-called surface web, the well-known part of the web which is crawled and indexed by search engines. The second category of websites is the so-called deep web, websites and other information repositories such as databases which are protected by logins and not indexed by search engines and therefore harder to find. Apart from that, the technology to host and publish the deep web does not differentiate from the usual surface web. Once located and registered, its content can be reached by using normal web browsers. Furthermore, both owners of clients and servers are not more or less anonymous than in the surface web (Chertoff & Simon, 2015). The third category of websites is the so-called dark web, where the content is provided by web servers that are only accessible within dark nets. Similar to the deep web, information in the dark web is also not indexed by regular search engines like Google. Dark nets are a part of the Internet that can only be reached by making

use of special overlay networks. Although there are also other approaches such as *The Invisible Internet Project* (I2P)[2], this paper has its focus on *The Onion Router* (TOR)[3] because it is the most frequented dark net.

Services, such as websites, which are reachable within the borders of the The Onion Router (TOR) network have to use the Hidden Service Protocol (The TOR Project, 2017b) and are therefore referred to as *hidden services*. They are addressed by a 16-character long unique identifier and the `.onion` pseudo top level domain suffix. The identifier consists of the first 80 bits of the RSA public key's SHA-1 digest encoded in base32 (The TOR Project, 2017a; Bezem & Solberg, 2013). It is usually referred to as the `.onion` name. One of the most well known examples of an `.onion` name is `facebookcorewwwi.onion`, addressing an instance of Facebook's website hosted as a hidden service in the TOR network. In order to access it, users have to make use of the TOR browser[4] which is a modified version of Mozilla Firefox. Employing the TOR browser, the `.onion` name can be used just like a regular URL in the TOR browser's address bar. TOR enables both users (via the TOR browser) and content providers (via TOR hidden services) to act anonymously.

Hence, TOR is used by whistle-blowers and politically oppressed oppositions of autocratic and dictatorial states. However, there is also a growing number of people abusing the provided anonymity for clandestine activities. In addition to drug (Buxton & Bingham, 2015) and arms trade (Weimann, 2016), human trafficking (National Association of State Mental Health, 2016) is a major clandestine activity that has benefited from dark nets. Due to financial structures of clandes-

[2]`https://geti2p.net/en/`
[3]`https://www.torproject.org/`
[4]`https://www.torproject.org/projects/torbrowser.html.en`

tine organizations, just as human trafficking, illegal human organ trafficking does not only harm people who are directly affected (with or without their consent) but also threatens public safety in general (Weimann, 2016).

Because of the lack of major commercial search engines focusing on hidden services, the Defense Advanced Research Projects Agency (DARPA) initiated the Memex project (Defense Advanced Research Projects Agency, 2014) providing a collection of tools[5] to enable researchers, government agencies and non-governmental organizations to search and analyze information in the dark web. Some of the customized tools are already established and help law enforcement agencies to successfully fight human trafficking (Prosecutors' Center for Excellence, 2016). However, due to differentiating characteristics, tools developed to investigate human trafficking cannot be deployed one-to-one to investigate human organ trafficking.

Although more advertising and communication for illegal organ trades move from the deep to the dark web, there are still relevant social media groups pretending to be supportive sites for people affected by illnesses (for example dependent on dialysis). However, in the anonymous comments made on these pages, brokers often offer help in the form of organs. Once the initial contact is established, further communication is lead in the dark web to ensure anonymity.

We focused on activities undertaken in dark web platforms/hidden services that are heavily decentralized and anonymous. While manually searching the dark web for content related to organ trade (especially of kidneys), we found that this kind of advertisements are posted in regular forums and newsgroups rather than on the popular marketplaces that

are used for other illegal activities such as drug and weapon trades. We also present methods to adapt tools of the Memex program to reveal clandestine organ trade in the dark web.

In addition to the standard TOR browser which is used to manually enter, browse, and investigate the dark web, a mix of self-developed tools as well as tools from DARPA's Memex program are used. In the following sections, we describe these tools and their usage through chosen examples.
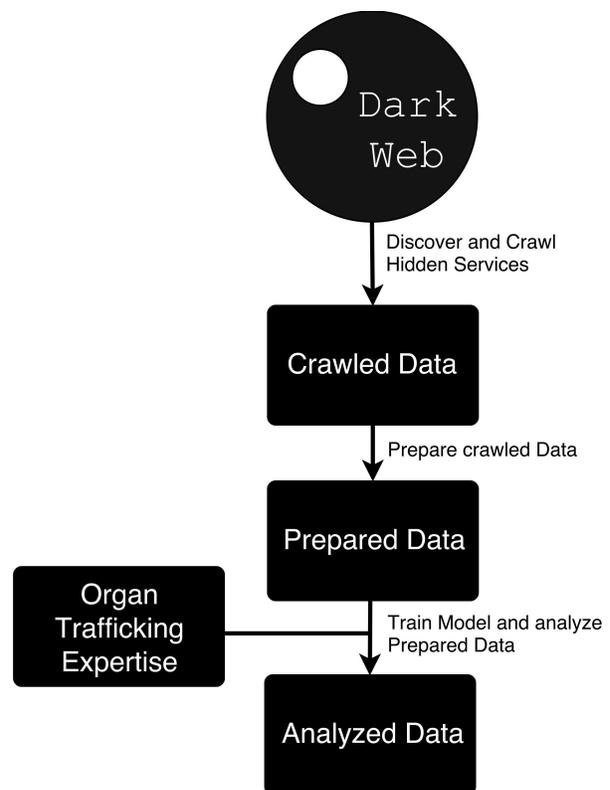
Figure 2. Methodology of dark web mining.

5.1 Hidden Services Discovery

Before the content of the dark web can be processed in order to find patterns of illegal human organ trafficking, the first challenge is to discover the actual hidden services. Because they are not indexed like the well-known surface web, other ways to access the provided data have to be developed. Hence,

---

[5] https://opencatalog.darpa.mil/MEMEX .html
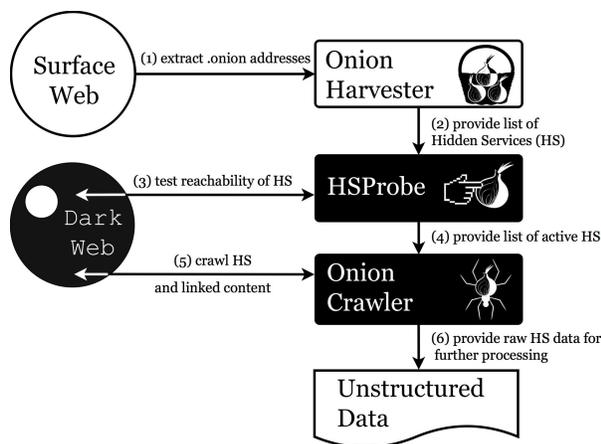
Figure 3. The tasks and interaction of tools in the process of hidden service discovery.

as shown in Figure 3, we propose to collect as many .onion addresses of hidden services as possible, test the reachability of these hidden services and finally crawl them in order to reveal their structure. Once the needed data is available, processing of the content can begin.

5.2   Harvesting

Considering base32's (Josefsson, 2006) alphanumeric character set (characters A–Z and digits 2–7: n=32) and the length of 16 symbols per .onion URL (k=16) (The TOR Project, 2017a), there are $n^k = 32^{16} \approx 1.2 \cdot 10^{24}$ .onion names addressing potentially available hidden services. Even quite optimistically assuming that 500 hidden services can be probed per second, it is still impossible to test all variations due to the high number of possible combinations, TOR's cryptographic and network overhead, and consequential network latency. A large range of possible ports other than the default HTTP port 80, such as the default HTTPS port 443 and the also commonly used port range of port 8000 to port 9000 are not even considered in this calculation. Thus, it is necessary to consider approaches other than brute force (trying all possibilities).

The most thorough method is to set up a large amount of TOR relays with specific fingerprints for a minimum of 25 hours in order to get the *HSDir* flag assigned. Properly configured, this would allow one to observe the deployment of hidden service descriptors which could be used to calculate .onion addresses (Biryukov et al., 2013). However, this way is very time and resource consuming.

Hence, in order to get a reasonably long list of hidden services representing a starting point for crawling more quickly, we created a Python script named *OnionHarvester*[6] to parse .onion names from publicly available websites such as hidden wikis. The tool uses a manually compiled list of websites, Google search results, or a combination of both. The corresponding parameters can be passed as values prefixed by the command line arguments -i (list of websites) and -s (Google search terms). Furthermore, an output file can be defined using the argument -o. The command below shows how to let OnionHarvester parse the websites listed in the file list.txt and additionally parse the content of the websites listed as results of the Google search for the term *hidden wiki*. The parsed .onion names are then written into the file harvest.txt.

```
$ ./onion_harvester.py -i list.
    txt -s "hidden_wiki" -o
    harvest.txt
```

5.3   Probing

Once the list is generated, the actual probing of the corresponding services can begin. An exemplary command handing over the formerly generated list containing hidden service identifiers to *HSProbe*[7] and defining some parameter reads as follows:

---

[6]https://github.com/mheinl/onion_harvester.py

[7]http://public.mtc.sri.com/MEMEX/hsprobe-2.1.tar.gz

```
$ ./hsprobe.py ---input-file
    harvest.txt ---output_file
    probing .log ---download-dir
    results ---probe-spec
    80,443,8080-8088:http , https
```

HSProbe creates a logfile (blurred example shown in Figure 4) listing the hidden service's unique identifier, the tested port, the Unix timestamp, the hidden service's status, and -if the probe was successful- the used protocol. Additionally, for every successfully answered probe request *HSProbe* creates a file named after the following scheme:

<onionURL>_<portNumber>_<protocol>

These files contain the whole response including HTTP message header and body. Hence, their content could technically already be used to make a pre-selection based on specific characteristics such as keywords. However, virtually none of the websites / forums involved in illegal organ trade indicate their actual content already on the landing page. Consequently, any successfully probed hidden service is going to be considered potentially interesting.

```
███████████████,80,1486952556,DONE,http
███████████████,80,1486952568,DONE,http
███████████████,80,1486952515,STATUS_TIMEOUT,
███████████████,80,1486952575,DONE,http
███████████████,80,1486952575,DONE,http
███████████████,80,1486952541,STATUS_TIMEOUT,
███████████████,80,1486952592,DONE,http
███████████████,80,1486952643,STATUS_TIMEOUT,
```

Figure 4. Extract of *HSProbe* logfile.

5.4   Crawling

Knowing which of the harvested `.onion` names do actually address active hidden services, they can be crawled using *Onion-Crawler*[8] which is similar to the Memex tool *Hidden Service Forum Spider*[9] developed by

---

[8]`https://github.com/mheinl/OnionCrawler`
[9]`http://public.mtc.sri.com/MEMEX/`
`forumSpider.tar.gz`

SRI International. Both tools are based on the Python-based scraping and web crawling framework *Scrapy*[10].

OnionCrawler provides two pipelines. One pipeline allows storing scraped websites into a file and directory-based structure within a specific folder. The other one stores the scraped websites into a previously set up PostgreSQL database. The default credentials specified in `settings.py` can either be changed in order to adapt to a already existing database or a new database using this default credentials can be set up.

To be able to crawl the TOR network, *OnionCrawler* has to be run over the TOR SOCKS proxy. This can be easily achieved by calling *Scrapy* with the preceding `torsocks` command: `$ torsocks scrapy crawl OnionCrawler`. However, when using the pipeline to write scraped websites into a PostgreSQL database, `torsocks` throws an error because it does not allow to connect to local resources by default. In order to fix that, the parameter   `AllowOutboundLocalhost 1`   in   the   `torsocks config`   file (`/etc/tor/torsocks.conf`   in   the   case of Linux) has to be uncommented.

Although it is usually not advisable for ethically working, commercial web indexing bots, the user agent has to be changed in order to avoid the hidden services' operators from evading. Thus, instead of a Scrapy spider, the configured user agent pretends to be a usual TOR browser in the most recent version available. Not obeying the hidden services' `robots.txt` allows one to explore also sites which are not intended to be discovered by crawlers. In addition to the above mentioned ways of customizing *OnionCrawler's* behaviour, it can also be controlled using command line arguments described in its `readme` file.

---

[10]`https://scrapy.org/`

Figure 5. Advertisement posted by a potential seller in the dark web forum *Moneybook*.

Figure 6. Advertisement posted by a potential buyer in the dark web forum *Moneybook*.

After mining the dark web using the aforementioned methods, we were able to obtain data related to organ trafficking, as shown in Figure 5 and Figure 6. Commonly provided information about the donor is gender, age, and blood group as well as the reasons for selling an organ. Those findings will also be used to develop our organ trafficking risk model.

6. A RISK MODEL OF ORGAN TRAFFICKING

Preliminary models of evolving real-world phenomena are always incomplete and inconsistent, and not different in the case of organ trafficking chains. However, the presentation of factors and their relationships causes people and organizations to get involved. Therefore, our risk model will be developed to be able to cope with the effects of uncertain phenomena. In other words, we developed a probabilistic knowledge-based risk model that is able to account for inherent uncertainties on evolving hypotheses. Our development process as follows:

- *Creating a collection of factors / nodes from literature studies and gained data:* In earlier sections, we illustrated how we collected data both manually and automatically, and provided some examples of how we are making nodes by the analysis of the data.

- *Retrieving the relationships:* We extracted the relationships from our learned knowledge of organ trafficking by representing it in the form of nodes. We identified actors at each stage of organ trafficking and the possible money flow among them.

- *Selecting modeling tools to design the model:* We chose the open-source Java application *UnBBayes*[11] which is able to build probabilistic models based on Bayesian probability and performing

---

[11]http://unbbayes.sourceforge.net/

plausible reasoning. Both a GUI (Graphical User Interface) as well as an API (Application Programming Interface) are available.

- *Generating the risk model:* Adding states for each node as shown in Figure 7.

Some basic characteristics of the model according to the *UnBBayes* documentation (Matsumoto et al., 2011) are:

- *Nodes* in a Bayesian network graph (Pearl, 1988) represent "random variables" which can contain several possible states. To each node a probability distribution of its possible states can be assigned. Among these possible values, exactly one of them "[...] will be the actual value at a given moment".

- *Edges* are direct links between nodes which express their probabilistic relationships and "[...] direct qualitative dependencies of the random variables."

- *A Conditional Probability Table (CPT)* represents the local probability distribution which is a function "[...] specifying the quantitative information about the strength of the dependencies."

Therefore, a Bayesian network is a structured, graphical representation of probabilistic relationships between several random variables. In Bayesian probability, the act of inference means updating beliefs as new information becomes available. Bayes' rule "[...] provides a method for updating the probability of a proposition when information is acquired about a related proposition."

Bayes' rule is represented by the equation $P(X|Y) = \frac{P(Y|X)P(X)}{(P(Y)}$ where:

- $P(X|Y)$: The probability of X given Y.

- $P(Y|X)$: The probability of Y given X.

- $P(X)$: The a priori probability of X.

- $P(Y)$: The a priori probability of Y.

The a priori probabilities are thereby the independent likelihoods before any evidence has been obtained. The reasoning systems of our selected modeling tool rely on Bayes' rule. The entity directory of our model is given in Table 1 which can be found in the Appendix because of its length. The Figures 9–13 represent an example in form of a partial view of our risk model which should help understanding how it works.

Based on the nature of each node, we added different states to the corresponding node. For example, node *PBR* (Potential BRoker) has been assigned two states Yes and No. Then, we initially generated a uniform probability distribution, which means that without any evidence we assign each state equal priori probabilities as it can be seen in Figure 8. That is, if we do not have any evidence for a given node, we equally divide 1 by the number of states in order to calculate its priori probabilities. Based on actual findings/evidence provided by users, these probabilities can be adjusted and the probabilities of subsequent related nodes will be re-calculated automatically.

The main task of our risk model is to identify a possible occurrence of organ trading based on evidence from a surrounding area. Basically, our risk model states that (a) an area that had been greatly impacted by organ trafficking in the past increases the risk of organ trading occurrences, (b) the vulnerability of states to collapse in a region is a risk factor for organ trading, and (c) the history of organ trafficking and the vulnerability of states to collapse in a region cannot be distinguished by occurrence of organ trading alone (Figures 9–13).
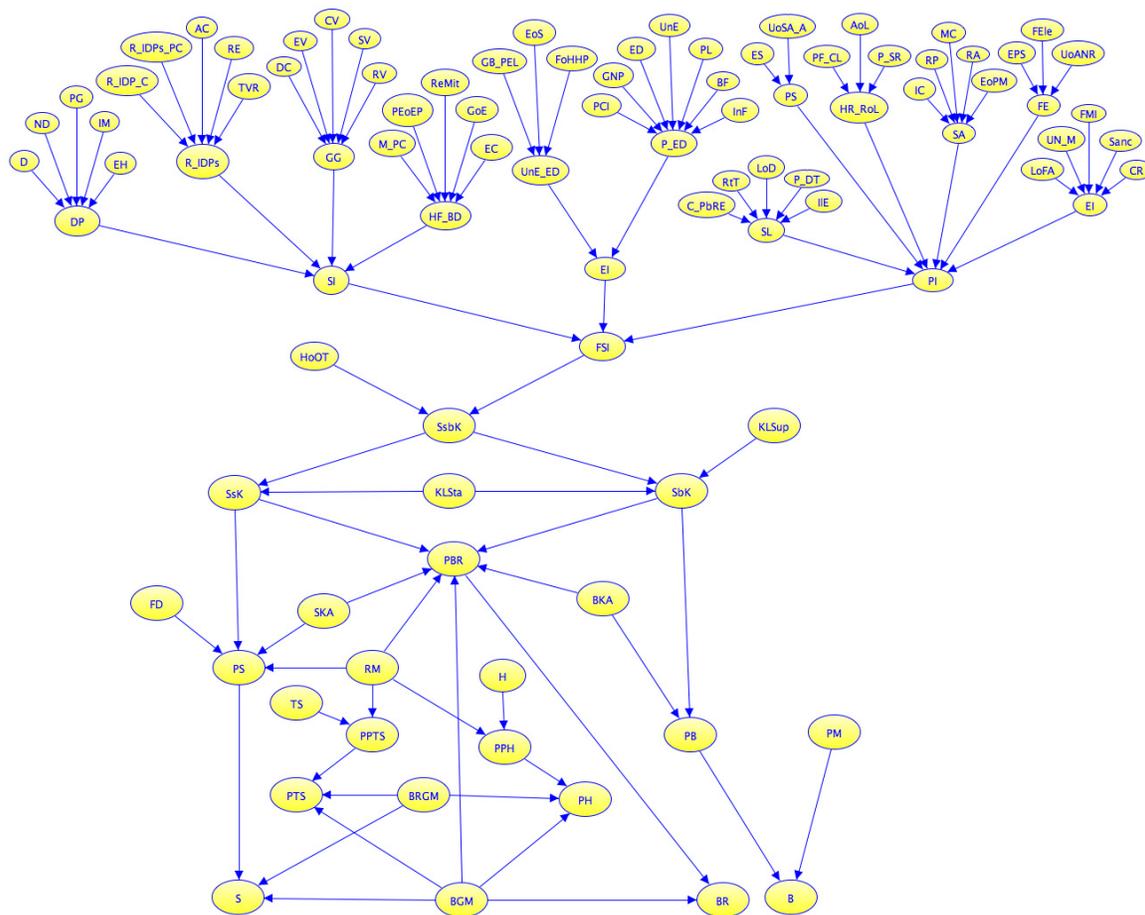
Figure 7. An overview of the risk model describing factors and relations influencing the process of organ trafficking.

Our model is able to visualize the relevant information that should be collected to better predict the results based on the actual situation. In addition, our model is sufficiently flexible to allow users to add uncertain information based on their goals.

In order to show the usage of our risk model, we used some sample runs and their conclusions. Figure 14 shows 20 randomly generated cases which were artificially created based on collected evidence. The data was generated by running *Netica* by Norsys[12], a tool providing methods to work with belief networks and influence diagrams. We used

Netica to create combinations of the nodes in different states, so called training data, during the learning process of our model. The automatically generated outcome of this learning process is the trained risk model shown in Figure 15.

The probabilities of nodes were changed from those in Figure 8. According to the facts, our model is able to provide suggestions such as type of information that should be collected by which organizations to better predict results. For example, a person who seeks to sell a kidney and also has posted a kidney for sale advertisement increases the chance of being identified as a potential vic-

---

[12]http://www.norsys.com/download.html
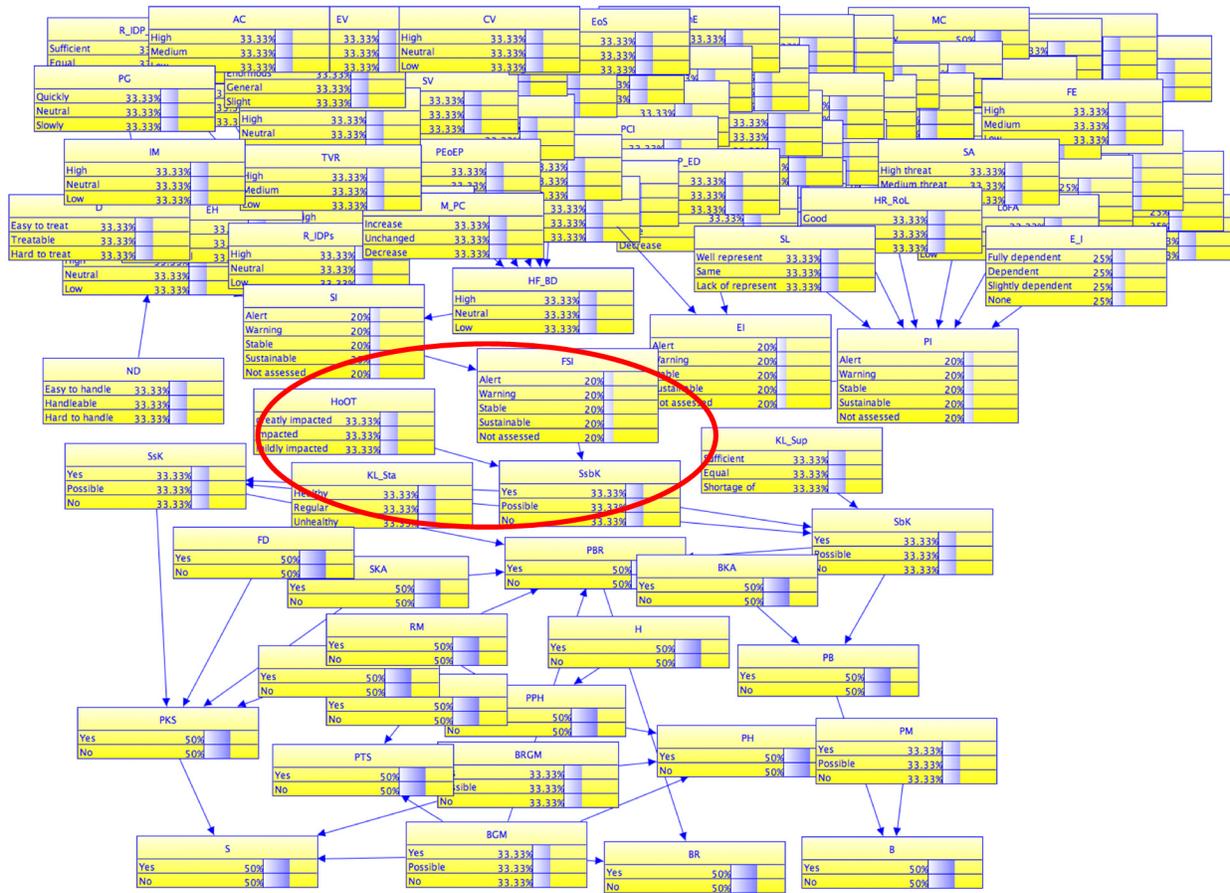
Figure 8. Risk model with a priori probabilities.
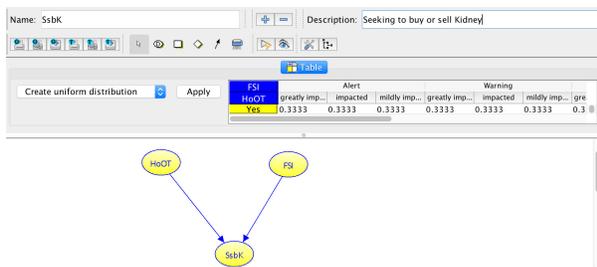
Figure 9. Partial risk model - events of seeking to buy or sell a kidney.
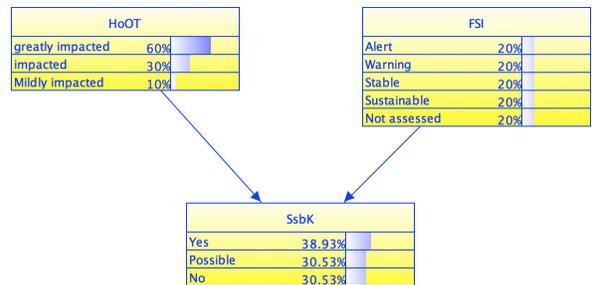
Figure 10. Assigning initial distributions to the nodes.

tim of organ trafficking. If law enforcement intends to stop such transactions, collecting recent online ads from both dark and deep web may be an effective method.

7. CONCLUSION & FUTURE WORK

The main contribution of this research is developing a risk model for organ trafficking based on collecting related data both manu-
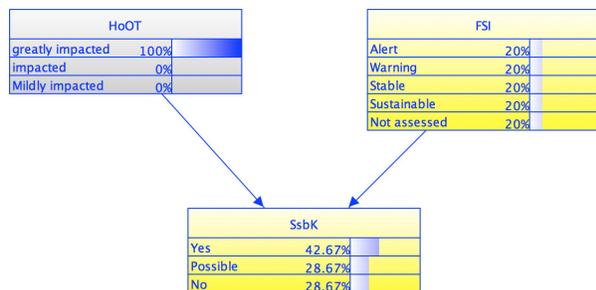
Figure 11. A place greatly impacted by organ trafficking.
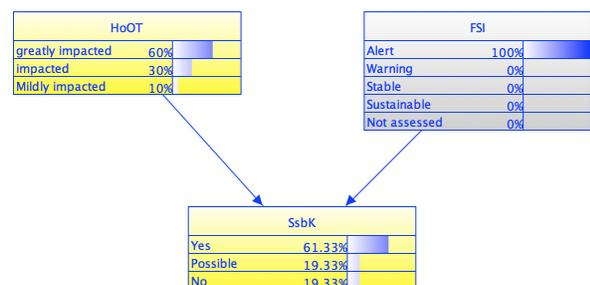
Figure 12. A place known for its high conflict rate.
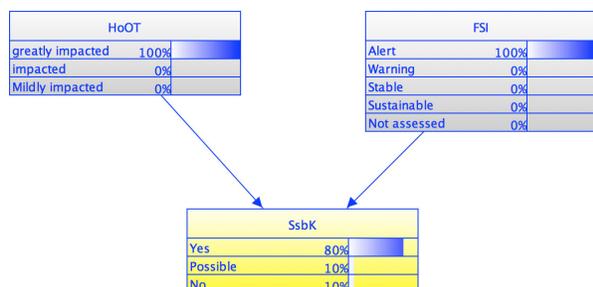
Figure 13. An area known for its high rate of conflict and great impact by organ trafficking.

ally and automatically. It enables users, such as policy makers, government agencies, and researchers to better understand the entire organ trafficking chain and to positively affect peoples' decisions. Moreover, our risk model is a probabilistic knowledge-based model that allows using incomplete, inconsistent information within the organ trafficking supply chain. That is, our model is sufficiently flexible to allow the users to add uncertain information

based on their goals. If users provided enough effective data, our risk model can conduct regular risk assessments regarding the constant changes of organ trafficking. Therefore, it will be a useful tool to develop policy response and operational interventions for such illicit trades.

In order to automatically collect related organ trafficking data, we provided a methodology and tools that can directly be used to support the search for clandestine human organ trade in the dark web. The current literature consist of research on crawling the hidden and dark web (Fu et al., 2010; Nunes et al., 2016) and how to identify web content related to organ trafficking (Pandey et al., 2013). However, at the time of this writing, to the best of our knowledge, there do not exist dedicated, publicly available research paper on how existing tools work and how to use them for use-cases such as revealing illegal human organ trafficking in the dark web. Our research combines and extends such previous research efforts to support the search for clandestine human organ trade in the dark web. Furthermore, because there is especially very little technical documentation about the tools provided by the Memex project, this work and corresponding repositories could also be useful for developers' own projects.

Topics for further research and development are specific tools to systematically explore social media channels. It could also be considered to partner with commercial vendors of dark web exploration tools in order to test their result rates for the use-case of organ trafficking. Furthermore, data already collected by projects like the IMPACT Cyber Trust[13] or the Carnegie Mellon University Online Anonymous Marketplace Research project[14] could be used to apply search patterns of organ trafficking in order to ex-

---

[13]https://www.impactcybertrust.org/
[14]https://arima.cylab.cmu.edu/markets/

IDnum	SI	R_IDPs	EI	PI	FSI	SsbK	HoOT	SsK	KL_Sta	KL_Sup	SbK	BKA	SKA	FD	PBR	PKS	PB	RM	PM	BGM
1	Stable	Low	Warning	Sustainable	Sustainable	No	mildly_impacted	Yes	Healthy	Shortage_of	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No
2	Sustainable	High	Stable	Not_assessed	Stable	Yes	impacted	Yes	Unhealthy	Shortage_of	No	No	Yes	Yes	No	Yes	Yes	No	No	Possible
3	Stable	Low	Warning	Warning	Stable	No	mildly_impacted	Yes	Unhealthy	Shortage_of	No	Yes	No	No	No	No	Yes	No	Yes	Possible
4	Warning	Low	Warning	Alert	Sustainable	Possible	impacted	Possible	Regular	Shortage_of	No	Yes	No	Yes	Yes	Yes	No	Yes	Possible	No
5	Alert	Neutral	Warning	Not_assessed	Sustainable	No	greatly_impacted	Yes	Regular	Sufficient	Possible	No	No	No	Yes	No	No	No	Possible	Possible
6	Alert	Neutral	Warning	Warning	Not_assessed	No	greatly_impacted	No	Regular	Sufficient	Possible	No	No	No	Yes	No	No	No	No	Yes
7	Stable	Neutral	Alert	Warning	Warning	No	mildly_impacted	No	Regular	Sufficient	No	No	Yes	No	No	Yes	Yes	Yes	Yes	Possible
8	Sustainable	High	Stable	Not_assessed	Warning	Possible	greatly_impacted	Possible	Unhealthy	Shortage_of	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9	Not_assessed	High	Sustainable	Stable	Alert	No	impacted	No	Healthy	Equal	Possible	No	No	No	Yes	Yes	No	Yes	Possible	No
10	Stable	High	Sustainable	Alert	Warning	Possible	mildly_impacted	Yes	Unhealthy	Shortage_of	No	Yes	Yes	Yes	No	Yes	Yes	No	No	Possible
11	Stable	Low	Stable	Stable	Sustainable	Possible	mildly_impacted	Possible	Unhealthy	Shortage_of	Possible	Yes	Yes	No	No	Yes	Yes	Yes	No	No
12	Warning	High	Sustainable	Stable	Warning	No	mildly_impacted	Possible	Unhealthy	Equal	Yes	Yes	No	Yes	Yes	Yes	No	No	Possible	Possible
13	Stable	Low	Not_assessed	Not_assessed	Not_assessed	No	mildly_impacted	Yes	Healthy	Sufficient	No	No	No	Yes	Yes	Yes	No	Yes	No	Yes
14	Stable	High	Stable	Sustainable	Warning	No	impacted	No	Unhealthy	Sufficient	Possible	No	Yes	Yes	Yes	Yes	Yes	Yes	Possible	Yes
15	Warning	Neutral	Not_assessed	Stable	Not_assessed	No	impacted	Possible	Healthy	Shortage_of	Possible	No	Yes	Yes	No	Yes	No	No	Yes	Yes
16	Warning	Low	Sustainable	Alert	Stable	Possible	mildly_impacted	Yes	Regular	Equal	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
17	Sustainable	Low	Alert	Warning	Alert	No	greatly_impacted	Possible	Healthy	Sufficient	Possible	Yes	No	No	No	Yes	No	Yes	Possible	Yes
18	Stable	High	Sustainable	Stable	Sustainable	Possible	impacted	Yes	Healthy	Equal	Yes	Yes	No	No	Yes	No	Yes	No	Yes	Possible
19	Sustainable	Neutral	Sustainable	Sustainable	Alert	No	impacted	No	Healthy	Shortage_of	No	No	No	No	Yes	Yes	No	No	No	Possible
20	Sustainable	Neutral	Not_assessed	Not_assessed	Warning	No	impacted	No	Healthy	Sufficient	Possible	No	Yes	No	No	No	No	No	No	Yes

IDnum	IM	D	EH	R_IDP_C	R_IDPs_PC	AC	RE	TVR	DC	GG	EV	CV	SV	RV	HF_BD	M_PC	PEoEP	ReMit	GoE	EC
1	Neutral	Hard_to_treat	Controllable	Shortage	Low	High	Enormous	High	Neutral	Neutral	Low	High	Low	High	Neutral	Decrease	Decrease	Decrease	Low	Decrease
2	High	Treatable	Hard_to_control	Sufficient	Medium	High	Slight	Medium	Low	Low	Neutral	Neutral	Neutral	Low	Neutral	Decrease	Decrease	Increase	Low	Increase
3	High	Hard_to_treat	Controllable	Shortage	Medium	Low	Enormous	High	High	High	Neutral	Neutral	Neutral	High	Low	Increase	Decrease	Decrease	Low	Increase
4	High	Treatable	Hard_to_control	Sufficient	Medium	Low	General	High	High	Low	High	High	High	Low	High	Unchanged	Decrease	Same	Neutral	Unchanged
5	Neutral	Hard_to_treat	Controllable	Shortage	Low	Low	General	High	Neutral	Neutral	Neutral	Low	Low	High	High	Increase	Increase	Same	Neutral	Unchanged
6	Neutral	Hard_to_treat	Hard_to_control	Equal	Low	Medium	Enormous	Low	High	High	Low	High	Neutral	Low	Low	Decrease	Decrease	Increase	High	Unchanged
7	Low	Hard_to_treat	Hard_to_control	Shortage	Medium	Low	General	High	High	Low	Low	High	Low	Neutral	Neutral	Increase	Unchanged	Same	Neutral	Decrease
8	High	Treatable	Hard_to_control	Equal	High	Low	General	Low	Low	High	Low	High	Low	Low	Low	Decrease	Unchanged	Decrease	Neutral	Decrease
9	Low	Easy_to_treat	Easy_to_control	Equal	Low	High	Slight	Medium	Neutral	Low	Neutral	High	High	Low	Neutral	Decrease	Increase	Increase	High	Unchanged
10	Low	Treatable	Hard_to_control	Sufficient	Low	High	Enormous	Low	High	Low	Neutral	High	Neutral	Low	Low	Unchanged	Increase	Decrease	High	Increase
11	Neutral	Easy_to_treat	Easy_to_control	Sufficient	Low	Low	General	Medium	Neutral	Low	Neutral	Low	High	Neutral	Low	Decrease	Decrease	Increase	High	Increase
12	High	Hard_to_treat	Easy_to_control	Shortage	Medium	Medium	Enormous	Low	High	Neutral	High	Low	High	Low	Low	Decrease	Unchanged	Decrease	High	Increase
13	Neutral	Easy_to_treat	Controllable	Equal	Low	Medium	Slight	High	Neutral	Low	Low	High	High	Low	Neutral	Decrease	Unchanged	Increase	High	Increase
14	High	Treatable	Easy_to_control	Equal	High	Low	General	High	Low	Neutral	Low	High	Neutral	Neutral	Low	Increase	Increase	Increase	Low	Increase
15	Neutral	Easy_to_treat	Hard_to_control	Sufficient	Low	Low	Slight	Medium	Neutral	Neutral	Low	Neutral	Neutral	Neutral	Neutral	Unchanged	Increase	Increase	Neutral	Decrease
16	Neutral	Hard_to_treat	Hard_to_control	Equal	Low	High	Slight	High	Low	Low	Low	Low	High	Low	High	Decrease	Unchanged	Decrease	Low	Increase
17	High	Hard_to_treat	Easy_to_control	Sufficient	Low	Low	General	Low	High	Low	Low	High	High	Neutral	High	Decrease	Decrease	Same	Neutral	Decrease
18	Neutral	Treatable	Hard_to_control	Sufficient	Low	Medium	Enormous	Medium	Low	Neutral	Neutral	Low	Neutral	Low	Neutral	Decrease	Increase	Same	High	Unchanged
19	High	Hard_to_treat	Controllable	Equal	Low	Low	Slight	Medium	High	High	High	Neutral	Neutral	High	Low	Unchanged	Decrease	Decrease	High	Unchanged
20	High	Treatable	Easy_to_control	Sufficient	Low	Medium	Enormous	High	Neutral	High	Low	Neutral	High	High	Neutral	Increase	Unchanged	Same	Low	Unchanged

Figure 14. Excerpt from 20 use-cases to train the risk model.

Figure 15. Trained risk model based on the 20 use-cases.

tract content and also to systematically spot platforms with high occurrences.

ACKNOWLEDGEMENT

REFERENCES

Ambagtsheer, F., & Weimar, W. (2016). *The HOTT project: Trafficking in human beings for the purpose of organ removal - results and recommendations.* Lengerich, Germany: Pabst Science Publishers.

Aronowitz, A., Theuermann, G., & Tyurykanova, E. (2010). *Analysing the business model of trafficking in human beings to better prevent the crime* (Tech. Rep.). OSCE Office to the Special Representative and Coordinator for Combating Trafficking in Human Beings.

Bezem, B., & Solberg, P. (2013). *Performance of hidden services in tor* (Master's Thesis). Norwegian University of Science and Technology.

Biryukov, A., Pustogarov, I., & Weinmann, R. (2013). Crawling for tor hidden services: Detection, measurement, deanonymization. *2013 IEEE Symposium on Security and Privacy*, 80-94.

Buxton, J., & Bingham, T. (2015, January). The rise and challenge of dark net drug markets. *Policy Brief 7*

(Swansea, UK: Global Drug Policy Observatory).

Chertoff, M., & Simon, T. (2015, February). The impact of the dark web on internet governance and cyber security. *Global Commission on Internet Governance, Paper Series No. 6*.

Defense Advanced Research Projects Agency. (2014). *Memex (broad agency announcement).* Retrieved 2017-02-19, from `http://go.usa.gov/BBc5`

Fraser, C. (2016). An analysis of the emerging role of social media in human trafficking. *International Journal of Development Issues*, *15*(2), 98-112.

Fu, T., Abbasi, A., & Chen, H. (2010). A focused crawler for dark web forums. *Journal of the American Society for Information Science and Technology*, *61*(6), 1213-1231.

Fund For Peace. (2017). *Fragile states index methodology and cast framework.* Washington, D.C., USA.

Gerken, J., & Wagner, L. (2016). *Understanding illicit trade: Impact of human trafficking and smuggling on the private sector* (N. Saperia, Ed.). Geneva, Switzerland: The Global Initiative against Transnational Organized Crime.

Josefsson, S. (2006, October). *The base16, base32, and base64 data encodings* (RFC No. 4648). Internet Engineering Task Force. Internet Requests for Comments. Retrieved from `https://tools.ietf.org/html/rfc4648`

Koettl, J. (2009). *Human trafficking, modern day slavery, and economic exploitation* (Tech. Rep.). The World Bank.

Matsumoto, S., Carvalho, R. N., Ladeira, M., Costa, P., Santos, L., Silva, D., ... Machado, E. (2011). UnBBayes: a Java Framework for Probabilistic Models in AI. In *Java in academia*

and research (p. 173-206). Annerley, Australia: iConcept Press.

Mijovic-Das, S. (2011). Organ trafficking and kidney transplantation. In *The international trafficking of human organs: A multidisciplinary perspective* (p. 117-130). Boca Raton, FL, USA: CRC Press.

Mo, C. H. (2018, March). Perceived relative deprivation and risk: An aspiration-based model of human trafficking vulnerability. *Political Behavior*, *40*(1), 247–277.

National Association of State Mental Health. (2016). *Technology and human trafficking.* Retrieved 2017-02-19, from `https://www.nasmhpd.org/sites/default/files/Assessment%203_Technology%20and%20Human%20Trafficking_0.pdf`

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., . . . Shakarian, P. (2016, September). Darknet and deepnet mining for proactive cybersecurity threat intelligence. *IEEE Conference on Intelligence and Security Informatics 2016*.

Pandey, S. J., Manandhar, S., & Kleszcz, A. (2013). Using sub-sequence patterns for detecting organ trafficking websites. *International Conference on Multimedia Communications, Services and Security (MCSS 2013)*, 167-180.

Pearl, J. (1988). *Probabilistic reasoning in intelligent systems: Networks of plausible inference.* San Francisco, CA, USA: Morgan Kaufmann.

Prosecutors' Center for Excellence. (2016, December). *Combatting crime on the dark web.* Retrieved 2017-02-18, from `http://www.ndaa.org/dyk/20161219-Dark%20Web_FINAL.pdf`

The TOR Project. (2017a). *Tor: Hidden service names.* Retrieved 2017-04-23, from `https://trac.torproject.org/projects/tor/wiki/doc/HiddenServiceNames`

The TOR Project. (2017b). *Tor: Hidden service protocol.* Retrieved 2017-02-19, from `https://www.torproject.org/docs/hidden-services`

United Nations Office on Drugs and Crime. (2014). *Global report on trafficking in persons.* Vienna, Austria.

United Nations Office on Drugs and Crime. (2015). *Assessment toolkit: Trafficking in persons for the purpose of organ removal.* Vienna, Austria.

Weimann, G. (2016, June). Terrorist migration to the dark web. *Perspectives On Terrorism*, *10*(3).

Yousaf, F. N., & Purkayastha, B. (2016, May). Social world of organ transplantation, trafficking, and policies. *Journal of Public Health Policy*, *37*(2), 190-199.

APPENDIX

Table 1. Descriptions of the risk model's nodes.

Node				Abbreviation	Description
FSI					Fragile State Index
	SI				Social Indicators
		DP			Demographic Pressures
				D	Disease
				ND	Natural Disasters
				PG	Population Growth
				IM	Infant Mortality
				EH	Environmental Hazards
		R_IDPs			Refugees and Internally Discplaced Persons (IDPs)
				R_IDP_C	The Presence of Refugee and IDP Camps
				R_IDPs_PC	Refugees and IDPs per Capita
				AC	Absorption Capacity
				RE	Relief Efforts
				TVR	Targeted Violence and Repression
		GG			Group Grievance
				DC	Discrimination
				EV	Ethnic Violence
				CV	Communal Violence
				SV	Sectarian Violance
				RV	Religious Violence
		HF_BD			Human Flight and Brain Drain
				M_PC	Migration Per Capita
				PEoEP	Particularly Emigration of the Educated Population
				ReMit	ReMittances
				GoE	Growth of Exile
				EC	Expatriate Communities
	EI				Economic Indicators
		UnE_ED			UnEven Economic Development
				GB_PEL	Group-Based Poverty and Education Levels
				EoS	Existence of Slums
				FoHHP	Fairness of Housing and Hiring Practices
		P_ED			Poverty and Economic Decline
				PCI	Per Capita Income
				GNP	Gross National Product
				ED	Economic Deficit
				UnE	UnEmployment
				PL	Poverty Levels
				BF	Business Failures
				InF	Inflation
	PI				Political Indicators
		SL			State Legitimacy
				C_PbRE	Corruption or Profiteering by Ruling Elites (RE)
				RtT	Resistance to Transparency
				LoD	Level of Democracy
				P_DT	Protests and DemonsTrations
				IlE	Illicit Economy
		PS			Public Service
				ES	Essential Services

Table 1. Descriptions of the risk model's nodes.

Node			Abbreviation	Description
			UoSA_A	The Use of the State Apparatus for Agencies that serve RE
		HR_RoL		Human Rights and Rule of Law
			PF_CL	Press Freedom and Civil Liberties
			AoL	any widespread Abuse of Legal
			P_SR	Political and Social Rights for individuals, goups, or cultural institutions
	SA			Security Apparatus
			IC	Internal Conflict
			RP	Riots and Protests
			MC	Military Coups
			RA	Rebel Activity
			EoPM	Emergence of state-related Private Militias terrorizing oppositionists
	FE			Factionalised Elites
			EPS	Elite Power Struggles
			FElec	Flawed Elections
			UoANR	Use of Aggressive Nationalistic Rhetoric
	EI			External Intervention
			LoFA	Level of Foreign Assistance
			UN_M	presence of peacekeepers or UN Missions
			FMI	Foreign Military Intervention
			Sanc	Sanctions
			CR	Credit Ratings
HoOT				History of Organ Trafficking
SsbK				Seeking to sell or buy Kidney
SsK				Seeking to sell Kidney
KL_Sta				Kidney, Live Status
SbK				Seeking to buy Kidney
KL_Sup				Kidney, Liver Supply
PBR				is Potential Broker
PFD				has Personal Financial Difficulty
SKA				has posted Sell Kidney Advertisement
BKA				has posted Buy Kidney Advertisement
PS				Potential kidney Seller
RM				Received Money
H				Hospital
TS				Transplant Surgeon
PPTS				Potential Participating Transplant Surgeon
PPH				Potential Participating Hospital
PB				Potential Buyer
PM				Pay Money
PTS				Participating Transplant Surgeon
BRGM				BRoker Gives Money
PH				Participating Hospital
S				Seller
BGM				Buyer Gives Money
BR				Broker
B				Buyer