To be published in the 2016 European Intelligence and Security Informatics Conference (EISIC). DOI: 10.1109/EISIC.2016.34

Towards Designing a Multipurpose Cybercrime Intelligence Framework

Mariam Nouh, Jason R. C. Nurse, and Michael Goldsmith
Department of Computer Science, University of Oxford, UK
Email: *firstname.lastname*@cs.ox.ac.uk

***Abstract*—With the wide spread of the Internet and the increasing popularity of social networks that provide prompt and ease of communication, several criminal and radical groups have adopted it as a medium of operation. Existing literature in the area of cybercrime intelligence focuses on several research questions and adopts multiple methods using techniques such as social network analysis to address them. In this paper, we study the broad state-of-the-art research in cybercrime intelligence in order to identify existing research gaps. Our core aim is designing and developing a multipurpose framework that is able to fill these gaps using a wide range of techniques. We present an outline of a framework designed to aid law enforcement in detecting, analysing and making sense out of cybercrime data.**

I. Introduction

Cybercrime emerged at first as a threat to individuals and organisations; now it also impacts entire countries. Experts in the criminology field have reported that the existence of organised cyber criminals in the online world is growing rapidly [1]. According to the PricewaterhouseCoopers (PwC) 2016 Global Economic Crime Survey [2], cybercrime has jumped from 4th to 2nd place amongst most reported types of economic crime. From the globally surveyed organisations, 22% experienced losses between $100,000 and $1 million, and approximately 5% suffered losses of over $5 million, of these 1% reported losses in excess of $100 million. Focusing more specifically on UK reports, over half of organisations in the UK experienced economic crime in the past two years, of those around 44% had been victims of cybercrime (up from 24% in 2014). These figures clearly show that there is an increase in cybercrime incidents, which is correlated with a lack of proper technological response and support from law enforcement [3].

The area of cybercrime intelligence has attracted the attention of the research community with the aim of aiding law enforcement better to detect, analyse, and understand the threat landscape posed by online cyber criminals. Cyber criminals use the internet as their crime scene since it provides them with ease of communication, wider recruitment possibilities, and opportunities to form partnership with other national and international criminal groups [4, 5]. This results in them leaving several “crumbs” that collectively produce a digital footprint for each cyber-criminal. Previous research has studied these footprints in order to gain better understanding of the characteristics of these cyber-criminal groups [6–9].

In this paper, our aim is to study the state-of-the-art research in the area of cybercrime intelligence with special focus on research based on gathering intelligence from open online data sources (e.g., forums, web, and social media). We intend to classify previous efforts on the detection of cyber criminals in terms of methods and data used. Additionally, we investigate the different types of analysis that have been adopted by the research community to better understand these criminal groups. We also survey existing intelligence frameworks and tools. In doing so, our objectives are to bring to light open research problems found in this field. Moreover, we seek to study the characteristics of existing intelligence frameworks, to aid in identifying the gaps and facilitate the development of an enhanced intelligence framework to support law enforcement.

The contributions of this paper consist of: surveying the current literature related to cybercrime intelligence-gathering and understanding the methods and techniques used; identifying the main research problems tackled in the literature and the related gaps; based on the identified gaps, we propose the design of a cybercrime-intelligence framework that addresses many of the gaps found in existing frameworks.

The remainder of this paper is organised as follows: Section II provides a set of definitions and characteristics of cybercrime and cyber criminals. Section III gives an overview of existing literature and a classification of research tracks within the field, covering the main problems tackled, data sources utilised, methods and techniques used, and evaluation methodologies adopted. We discuss the main research gaps we identify and propose a novel cybercrime-intelligence framework in Section IV. Finally, Section V concludes this paper.

II. Definitions and Characteristics

Since this paper focuses on understanding the state-of-the-art research in the area of cybercrime, it is important to define what we regard as cybercrime and cyber criminals. There have been several arguments in the literature over the exact definition of cybercrime with no single universal definition [10]. Similarly, some articles use generic references such as computer-crime, Internet-crime, digital-crime, and most widely used cybercrime (or cyber-crime), as well as terms references to specific forms of crimes such as cyber-terrorism and cyber-stalking [11].

Some articles in the literature define cybercrime as any crime that involves computers or networks, others define it as purely digital crimes, or traditional crimes which are enhanced through the use of digital technology [12]. Initially, previous research drew a distinction between crimes, where the computers are the target of the crime (hacking, spam, terrorism-related offences), and crimes where computers act as tools to commit the crime (child pornography, phishing) [11].

Wall considers cybercrime to be one of three types: (1) Crime in the machine, (2) crime using the machine, and (3) crime against the machine [13]. Crime in the machine relates to the content of computers which include for example the trade of pornographic material, crime using the machine relates to any crimes committed using networked computers such as targeting victims by phishing emails, finally crimes against the machine covers the integrity of computers and networks such as hacking and planting of viruses and Trojans. Two main categories of cybercrimes exist in the literature: these are computer-enabled, and computer-dependant crimes. The former includes traditional crimes that are enhanced in scale and reach using computers, while the latter includes crimes that are committed using computers and networks [14].

In this paper we include in our definition of cybercrime all traditional crimes that are conducted online (e.g., tax fraud), new crimes that are dependant on the Internet (e.g., data manipulation, denial of service) and crimes that depends on intermediaries such as botnets to facilitate them. Similarly, we include those crimes that cover indirect use of computers such as using it for communication purposes or data storage, as part of our definition of cybercrime [15].

III. Literature Review

The broader aim of this paper is to understand the current literature related to cybercrime intelligence-gathering. We intend to identify the current gaps and the open research problems within this domain. To do so, we focus on studying which cybercrime related questions and problems are being tackled in the literature. We also consider the methods used to address these problems, the data sources they study, and the main validation and evaluation methods they adopt. We classify existing work in the area of cybercrime intelligence into three main research tracks (See Figure 1):

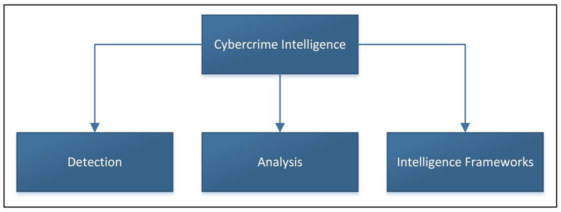

Fig. 1: Classification of cybercrime intelligence research tracks

A. Detection of Online Cybercrimes

This section covers research into detection of online criminals and content. Obviously the majority of online content (apart from DarkNets) is lawful; thus, the challenge is to detect outlier criminal content and behaviour. The majority of the literature in detection of online cybercrimes adopts a content-based methodology. They mainly focus on studying textual content through the use of Natural Language Processing (NLP) techniques in order to achieve the following: authorship profiling; authorship analysis; text classification; and sentiment analysis [8]. Others adopt different techniques from NLP, for example, using Social Network Analysis (SNA) to study the relations between criminals and the communities they form [16], Information Extraction to extract intelligence from large amount of text [17], and Machine Learning to classify users accounts and detect outliers automatically [18].

As for the data sources used, we find that forums and some social-media services such as Twitter and Facebook are the most used as open online data sources. Furthermore, other researchers used data gathered from different news websites and online auctions to detect fraudulent behaviours. When it comes to methods for evaluation, most of the existing research either lacks a proper evaluation method, performs manual evaluation [16], depends on expert evaluation [19], or uses measures such as recall and precision [20].

In the recent years, there has been an increase in online accounts advocating and supporting terrorist groups such as ISIS. This phenomenon attracts researchers to study the online existence and research ways to automatically detect these accounts and limit their spread. Ashcroft et al. make an attempt to automatically detect Jihadist messages on Twitter [18]. They adopt a machine-learning method to classify tweets as ISIS supporters or not. They focus on English tweets that contain a reference to a set of predefined English hashtags related to ISIS. Three different classes of features are used, including stylometric features, time features and sentiment features. Moreover, Sabbah et al. propose a hybrid feature selection method to detect potential terrorism activities from text based on term-weighting techniques [20]. They apply the method on data collected from Dark Web Forum Portal and use several classification techniques (Support Vector Machine, K-Nearest Neighbour). Evaluation of their method is conducted using measurements such as precision and recall.

Furthermore, one of the heavily studied research problems in the literature is the detection of online spammers and spam accounts. Machine-learning is arguably the most used technique for detection of spammers [22, 23]. McCord et al. present a traditional classifier to detect spam users in Twitter [22]. They use a combination of content-based and user-based features, and compare the performance of four different classifiers. Confusion matrix were used for evaluation. Looking at a different social-network platform, Beeutel et al. [24] study the problem of spammers performing Page Like behaviour, hoping to turn a profit. They propose a method called CopyCatch, aimed at detecting ill-gotten Page-Likes on Facebook by analysing the social network of users and Pages and the times at which the Likes were created.

Several other research efforts concentrate on identifying malicious bots (software agents imitating humans). These bots are able to mimic characteristics related to content, network, sentiment, and temporal patterns of activity. Everett et. al., [25] investigated how easily bots can deceive humans to the extent of believing that an automatically-generated text was written by a human. They identified a set of factors that contribute to how convincing the text is. In other work Thomas et al.

infiltrated the underground market of fraudulent accounts [23]. By collaborating with Twitter, they were able to investigate fraudulent accounts and develop a classification algorithm to retroactively detect millions of fraudulent accounts that were sold by the underground marketplace they infiltrated. For the classification they used features such as account-naming patterns, form-submission timing, and sign-up flow events.

Moreover, Yang et al., [26] perform an empirical study to study cyber-criminal communities in Twitter. They focus on developing a criminal-account-detection algorithm based on social relationships and semantic coordination. Their study focuses on identifying profiles that post malicious URLs as a starting point for identifying communities, then they look at social relations between these accounts. However, their approach is not considered a full detection system as it starts with a seed of criminal accounts. Savari et al., [16] built a social network from a seed of publicly leaked email addresses of criminals. They identified Facebook accounts associated with these emails and constructed their social graph. Through several SNA methods they identified multiple criminal communities and profile groups on Facebook. They use manual evaluation to study the effectiveness of their method.

Another topic that attracts several researchers is related to hate-speech forums. Yang et al., [21] study hate-group forums and introduce a technique that combines machine-learning and semantic-oriented approaches to identify radical opinions. Similar to previous research they use textual features to classify text. They perform cross-validation to validate the robustness of the technique, and use precision and recall for evaluation.

B. *Analysis of Cyber Criminals*

This section covers research into analysing the criminal content online to gain further insight into the structure and behaviour of these groups. The work of Stringhini et al. sheds light on the relations and interactions between different actors involved in the spam ecosystem [27]. The authors investigate the relations between email harvesters, botmasters, and spammers, where the analysis is based on correlating their behaviour based on indirect measurements. Thus, whilst insightful, a limitation of their work is apparent since no exact figures are calculated and only indirect measurements are considered. Moreover, Almaatouq et al. analyse the behaviour of spam accounts on Twitter [28]. Spammers are categorised based on their behaviour into two different categories: compromised accounts and fraudulent accounts. The authors then analyse the profile properties of the accounts, and their social interactions including following and mention-behaviour.

Chen et al. present a general framework for data-mining of criminal and terrorist behaviour [29]. Four categories of crime data-mining techniques were identified, namely entity extraction, association, prediction, and pattern visualization. Three tasks were performed using those techniques. First, they extracted named entities (e.g., person names, addresses) from police reports. Second, they detected deceptive criminal identities within police database using string comparators to measure similarities between strings. Finally, they worked on identifying subgroups and key members. Hierarchical clustering were applied to identify subgroups and centrality measures used to detect key members in each group.

Garg et al. study the organisation structure of criminals in three underground online forums [30]. They analyse the communities within these forums and compare topics of communication used by these communities using topic modeling. Additionally, they identify central members from each community using different centrality measures. Finally, they investigated the effects of removing misbehaving criminals on the criminal network. Results generalization is a limitation of this research, similar analysis should be repeated on larger dataset and different types of underground forums.

Lu et al. [7] empirically study a hacker community called "Shadowcrew", which is a known group for committing identity theft and credit-card fraud. The authors study questions related to the hacker network centralization, leadership and their influence on the group, and the existence of different subgroups within the community. The data was collected from newspapers, journals and law reviews that had a keyword match for "Shadowcrew". The methods used for the analysis was based on social graph analysis and the leaders were identified using centrality measures. This study has a couple of limitations: It is based on analysis of a single group, which means it can't be generalized. Additionally, the network was built based on data gathered from text documents, which doesn't capture the behaviour of the group.

In order to get a general understanding of how criminals organise online, Sarvari et al., have employed a community-detection technique based on modularity in order to discover communities inside a criminal network [16]. The network was built from an initial seed of known criminal emails which were linked to active Facebook profiles before they scraped the friend's list of the identified criminal profiles. For evaluation they manually analysed these profiles looking for evidence of criminal activity. Using centrality measures, they found that key members of this criminal network have high ranks in all centrality measures and in PageRank. Their conclusions suggest that highly connected members are located in central position of the graph and they are also connected to other well-connected members. However, it is yet to be validated whether this phenomena is accurate for other criminal networks.

Previous work has focused on analysing public reactions in social media towards real-world events as well as propagation of information. Burnap et al., [31] analyse the Woolwich, London terrorist attack that occurred in 2013 by building models that predict the public reactions in Twitter. They study measures related to opinion and emotions to predict the size and survival of information-flow related to the terrorist attack.

C. *Intelligence Frameworks*

This section covers research into the development of tools to support law enforcement in gathering intelligence by detecting or analysing online crimes, providing situational awareness to investigators. Several previous efforts have worked on developing frameworks for crawling the web and collecting extremist-related content [33–35]. Zhang et al. introduced the first version of the Dark Web Forum Portal (DWFP) [33]. The system supports several functions including data acquisition from different online forums, forum browsing and searching, multiple language translation and network visualization.

Mei et al. [34] present a semi-automated web-crawler for collecting extremist content using sentiment analysis. The system uses a decision tree that classifies the web pages into a set of classes by combining methods of web-crawler, parts-of-speech tagging, and sentiment analysis. The content is classified into: content with extremist sentiment (pro-extremist); news sources (neutral); government or anti-extremist organisations (anti-extremist); and content unrelated to extremism.

The work of Bouchard et al. [35] presents a web-crawler called the Terrorism and Extremism Network Extractor (TENE). The aim of TENE is to collect information about extremist activities online and help differentiate between extremist websites and other similar websites. The crawler starts at a user-specified webpage then analyses the content and further follows any hyperlinks in the page. In order to add the webpage to the analysis, it has to contain a set of user-defined keywords. TENE extracts around 200 characters before and after the user-defined keywords in order to determine the context in which the keywords were used. Although the context extraction is done automatically, the analysis of the context is performed manually. The COPLINK system [36, 37] was designed to aid law enforcement in extracting information from police reports and provide an environment for information-management in the intelligence domain. The system uses data-mining techniques to build a concept space of objects and entities and their associations, as well as social network analysis to study the relations between them. In addition, the system provides visualization functionality.

Furthermore, CrimeNet Explorer [38] is a framework for discovering criminal-network knowledge that incorporates both structural analysis and visualization methods. Similar to COPLINK, the framework uses data gathered from crime incident reports. The framework includes four main steps, network creation, network partition, structural analysis, and network visualization using multidimensional scaling. Limitations of the CrimeNet Explorer framework include the use of “concept space” to create the network, as this approach is fairly simplistic [38]. Additionally, the framework only focuses on analysing networks of people (criminals) and does not look at networks of people and entities (e.g., places, weapons).

The Isis toolkit [39] provides law enforcement with the ability to analyse digital personas in cybercrime investigations. The main features supported by the toolkit are establishing a stylistic language fingerprint, establishing the age and gender of the person behind the perosna, and finally establishing interaction patterns between a set of digital personas. The toolkit combines techniques from corpus-based natural-language analysis and authorship attribution. It presents the results in a visualization view, but it is based on a fairly simple, chart-like visualizations with no support for user interaction. Furthermore, the toolkit is able to detect deceptive personas (users with masquerading behaviour) with high degree of accuracy. Jigsaw [40] is a visual analytic system that supports investigative analysis. It provides visual representations of information extracted from textual documents to aid analysts in better understanding the documents. The analysis is based on extracting entities (e.g., person, place, date) and identifying connections and relationships between them. Two entities are connected if they appear together in one or more documents. The Jigsaw system consist of multiple views that provide the user with different perspectives of the data. Although the Jigsaw system provides rich visualizations, it does not provide any sophisticated data-mining or analytic capabilities.

Chen et al. [19] propose a semi-automated methodology for collecting and analysing Dark Web information. The methodology consists of collecting, analysing and visualizing information gathered from multiple web sources. The data collection is based on keyword search and websites of terrorist organisations. Unrelated sites such as news and government websites are manually filtered out. The analysis consists of clustering websites based on similarity measure calculated based on the number of hyperlinks in website A pointing to website B, and vice versa. Moreover, websites classification was performed based on their affiliation with a specific terrorist group. However, the classification was performed manually by reviewing the content of each website, which is not efficient and is error-prone especially for large datasets.

There are other frameworks that have more specialised purposes that can be applied to the cybercrime-intelligence domain. For example, TwitterHitter [41] which is focused on spatio-temporal analysis of Twitter data. The framework supports name/alias keyword search, which then provides a spatio-temporal record of the target user’s activity. Additionally, the framework provides relationship investigation analysis of users in a particular region, key players identification and detection of existing communities. TwitterHitter provides analysts with a map view that shows the location of hotspots where people are tweeting about a particular topic that match a given keyword.

EVILCOHORT [42] a system that detects malicious online accounts that are controlled by cybercriminals. The system relies on detecting criminal accounts by identifying the connection points (IP addresses) used to access them. Typically, these IP addresses correspond to bots controlled by the criminal. By identifying communities of accounts that are accessed by a common set of computers (botnets) they were able to pro-actively detect these malicious accounts even before they spread the malicious content (e.g., spam).

IV. Discussion

From our investigation, the main research problems tackled in the literature within the cybercrime-intelligence domain generally revolve around the following areas:

(1) Detection of communities and organisational structure – This includes the identification of key members in criminal networks, the discovery of sub-communities within the network and the different properties they possess, the detection of strong ties between nodes to evaluate relationships between criminals, and finally studying organisational structure of the criminal groups to understand the hierarchy of the criminal network. This aids law enforcement in detecting the leaders and influential members in order to target them instead of wasting resources on low-level non-influential criminals.

(2) Behaviour analysis and interaction patterns – This includes analysing behaviour and finding patterns in the cyber-criminal networks, establishing interaction patterns between individual actors or between sub-groups within the network. By observing how the network changes over time and studying meta data information, we can possibly predict when the network is conspiring for a crime.

(3) Disruption of criminal networks – This includes studying the effects of removing criminal nodes or ties on the survivability of the network. Network survivability can be measured by how effective the information spread within the network (number of hops), for example from central nodes to more peripheral nodes. An additional factor for network survivability is its ability to function properly with the leaders not isolated and have access to the wider network.

(4) Profiling cyber criminals – This includes identifying language stylometric fingerprints and author characteristics such as their age, gender, ethnicity, and so on. As most criminals use screen-names and disguise their information it is critical to study techniques that can reveal characteristic information about them. Profiling cyber-criminals aids in predicting if two online accounts are operated by the same individual, and to track criminals across different online platforms.

(5) Identifying disruptive events and predicting offline events – This includes identifying weak signals [32] (i.e., indicators that initially appear insignificant but actually are early indicators of large-scale real-world phenomena). Predicting tipping points, the likelihood of rumour spread, information propagation and the expected reactions of the public.

(6) Extraction and identification of online criminal content – This includes development of techniques to automatically identify criminal-related content or individuals. Building crawlers that are able to extract content and classify it as criminal-related or non-criminal content.

A. *Research Gaps*

We summarise some of the existing frameworks for cybercrime intelligence in Table I. The frameworks included in the table were selected based on the year of publication and number of citations, as well as the relevance to our topic. Moreover, based on the literature review presented in Section III, we identify several criteria to evaluate the frameworks (the columns in Table I). These criteria are chosen to identify the types of analysis used and the functionality provided by the frameworks: these are the data-sources used; type of cybercrime they target; whether they aim at detection or analysis; support for data acquisition or only operating on previously collected datasets; the types of analysis they use; and finally whether or not the framework supports visual analytics. If this criterion is satisfied, we also look at support for feedback and interaction from the analyst.

Through our analysis of the literature, we have identified several gaps which future research efforts should aim to fill. As observed in Table I, none of the previously developed frameworks cover all three stages related to detection, analysis, and visualization, and very few cut across both the detection and analysis stages. Thus, most frameworks are focused on a single functionality in order to solve a particular problem. Similarly, nearly all of the frameworks we examined focus on only a single data-source (very few papers combine different data-types), which make the framework dependant on a particular platform (e.g., Twitter) and the methods used are not generalizable to other data sources and types.

Moreover, with regards to the techniques used, we find that most frameworks adopt content-analysis methods. This includes the use of techniques such as NLP, sentiment analysis and syntactic analysis. Others use SNA together with content analysis to add additional dimension to the analysis. However, very few consider the spatio-temporal dimensions when studying cybercrime data, which is surprising since most criminal networks are dynamic and constantly changing. Thus, a framework with support for spatio-temporal analysis of criminal networks is needed.

Visual analytics for cybercrime is another area that requires additional attention from the research community. Most of the existing frameworks either do not support any form of visualization or provide very simple visualizations. Those who do provide visual representation of the analysis results do not necessarily support user interaction with the framework. In order for the investigator to be able to make sense out of the data and results they need to have a way to inject their own expertise and hypothesis into the framework analytics.

Another area that many of existing systems overlook is the evaluation aspect, which is mainly due to the challenges associated with obtaining ground-truth data in this domain. Very few proposals report evaluation of the framework by domain experts such as the police. The majority tend to use manual evaluation (e.g., in the detection of criminal accounts or content [16]), or adopt small-scale controlled lab experiments to evaluate the performance (e.g., [38]). Therefore, a proper evaluation should be performed by the prospective target users to ensure the effectiveness of the framework.

B. *Towards a Novel Cybercrime Framework*

We propose a novel framework, CyberCrime INTelligence framework (CCINT), that is designed to fill the gaps identified in the literature and based on requirements and design guidelines recommended for intelligence systems. Previous related literature [43, 44] has developed design guidelines that act as recommendations for system designers in order to minimize the occurrence of cognitive biases. In many situations the prior beliefs and experiences (i.e., biases) of the decision-maker (the analyst) influence his decisions, which may lead to incorrect results. To avoid such issues, information should be presented in a way that minimizes cognitive biases and supports the

TABLE I: Review of existing intelligence frameworks

Authors	Framework description	Data Sources	Types of cybercrime	Detection	Analysis	Data acquisition	Content analysis	Social network analysis	Time analysis	Spatial analysis	Sentiment analysis	Visual analysis	Analyst feedback
Almaatouq et al. 2016 [28]	Analysis and detection of microblogging spam accounts	Twitter	Spam	✓	✓	✗	✓	✓	✗	✗	✗	✗	
Gianluca et al. 2015 [42]	EVILCOHORT framework for detecting malicious online accounts	Generic online sources	General	✓	✗	✓	✗	✓	✗	✗		✗	
Mei et al. 2015 [34]	A sentiment analysis based web crawler for extremist content	Web pages	Terrorist/ extremist	✓	✗	✓	✓	✗	✗	✗	✓	✗	
Bouchard et al. 2014 [35]	Terrorism and Extremism Network Extractor (TENE)	Web pages	Terrorist/ extremist	✓	✗	✓	✓	✓	✗	✗	✗	✗	
Stringhini et al. 2014 [27]	Studies the relations between botmasters, spammers, and email harvesters	Emails	Spam	✗	✓	✗	✗	✗	✓	✓	✗	✗	
Burnap et al. 2014 [31]	Models the social media reaction to terrorist attacks	Twitter	Terrorist/ extremist	✗	✓	✗	✓	✓	✓	✗	✓	✗	
Rashid et al. 2013 [39]	Isis toolkit, identifies individual or group identities hiding behind multiple personas	Chat messages	General	✗	✓	✗	✓	✗	✓	✗	✗	✓	✗
White et al. 2010 [41]	TwitterHitter a framework for harvesting Insight from volunteered geographic information	Twitter	General	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓
Yong et al. 2010 [7]	Studies a hacker network called (Shadowcrew) using social network measures	News articles	Credit card fraud	✗	✓	✗	✓	✓	✗	✗	✗	✗	
Zhang et al. 2010 [33]	Dark Web Forum Portal that provides access to extremist web forums	Online Forums	Terrorist/ extremist	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗
Stasko et al. 2008 [40]	Jigsaw visual analytic system to support investigative analysis	Offline reports	General	✗	✓	✗	✓	✓	✓	✗	✗	✓	✓
Chen et al. 2008 [19]	Collection, analysis, and visualization of dark web pages	Web pages	Terrorist/ extremist	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗
Xu et al. 2005 [38]	CrimeNet a framework for discovering criminal network knowledge	Offline police reports	General	✗	✓	✗	✓	✓	✗	✗	✗	✓	✓
Xu and Chen 2005 [37]	COPLINK framework for criminal network analysis and visualization	Offline police reports	Terrorist/ extremist	✗	✓	✗	✓	✓	✗	✗	✗	✓	✗
Chen et al. 2004 [29]	A general framework for crime data mining	Offline police reports	General	✗	✓	✗	✓	✓	✗	✗	✗	✗	

sense-making process. Typically, analysts deal with large volumes of data with the objective of extracting insights and intelligence to make informed decisions. Cognitive biases may impact any step from the collection of raw data up to reaching actionable intelligence [43].

Additionally, one of the known issues with automated intelligence gathering tools is that over time analysts may become over-reliant on the tool and stop engaging their expertise in the analysis process. Such effect can be minimized by providing specific training to the analysts and raise their awareness.

Before designing the CCINT framework, we considered several guidelines in order to minimize cognitive biases and suit requirements from professionals in law enforcement for such tools. These include support for multiple visualization views to present the analyst with different perspectives of the data. Additionally, provide the ability to identify levels of uncertainty in the data by showing a confidence score associated with each data item. Previous research proposed different cybercrime investigation models to guide law enforcement through the investigation process [3, 45]. Although these models may seem different as they use different terminology to define the models' activities, most of them have similar processes. We study these models to elicit additional requirements to allow the framework to support the investigation process. One of the key features of the investigation process that was identified is its iterative nature, as new data is found the investigator needs to iterate through collecting evidence, taking actions, evaluation and making decisions [3]. This feature is reflected in our framework by supporting users feedback and interactions with the framework, as well as supporting storage

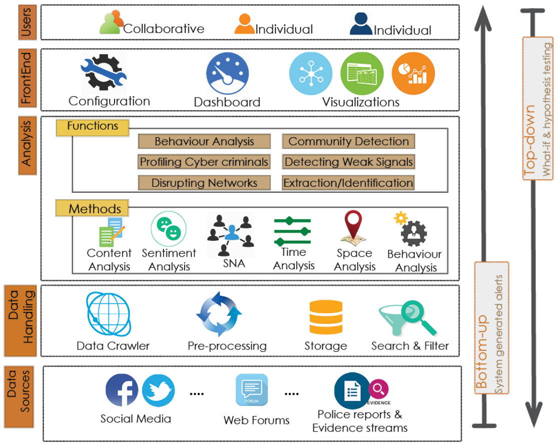

Fig. 2: CCINT Framework

of different case scenarios for future comparison and reference. Through the iterative and interactive nature of the framework false positives and negatives can be reduced. By providing the analyst with the capability of tagging events as false positives or negatives and feeding these tags back to the system to learn from and eventually reduce them. Thus, the more the analyst uses the system the better the system becomes.

An overview of the proposed framework is shown in Figure 2. The initiation of any investigation is usually triggered by either an internal event (uncovered intelligence information) or external event (reported crime). These are modelled in our framework by providing two modes of operation: bottom-up investigation where the system detects intelligence information from raw data and generates alerts to the user to further investigate, or top-down investigation where the investigator have an outside knowledge and want to generate a hypothesis in order to prove it using the data. Furthermore, typically any cybercrime investigation involves various specialists and investigator roles working together to solve a case, thus we design the framework with support for collaborative investigation sessions such that several specialists can work together on a shared case scenario. Additionally, the framework should be platform-independent to cater for the heterogeneity of hardware and software available in different police departments.

The CCINT framework is designed to aid analysts in making sense out of large numbers of open online datasets. The framework is designed to support the six key steps in the analytical process [44]: problem definition, hypotheses generation, information collection, hypotheses evaluation, selecting the most likely hypothesis, and continuous monitoring of new information. The framework consists of three main layers: data-handling, analysis and front-end, and two external layers: users, and data-sources. The data-sources layer contains any open online data sources that are of interest to the analyst and can be plugged into the framework through an API to feed real-time data to the data-handling layer. It is important to mention here that the framework can collect data from multilingual data-sources (English and Arabic languages will be our initial focus as these are the most used languages in extremist and criminal content).

The data-handling layer is responsible of collecting data from the online sources based on user's defined configuration. A plug-in for each data-source is created to facilitate the collection of the data. Moreover, this layer consists of data acquisition using a crawler, pre-processing and cleaning of the data, search and filtering, and a database for storage. The next layer is the analysis layer, which covers the detection and analysis of cybercrime accounts and content by supporting the six functions listed earlier in this section. Methods such as content and sentiment analysis, SNA, time analysis and geo-spatial analysis are used to perform these operations. The front-end layer supports user interaction and consists of a dashboard, multiple visualization views and a configuration panel for the analysts to customise the different processes within the framework. The top layer is the user layer that supports both individual and collaborative sessions.

Furthermore, the framework supports two modes of analysis: bottom-up and top-down. The bottom-up mode allows the analyst to start from the data level without having any previous hypothesis, and allows him to observe the data and look for anomalies and abnormalities. In this analysis mode, the system may suggest possible leads for the analyst to investigate in the form of alerts, based on anomalies detected and unusual patterns. For example, the system may alert the investigator if it detects an increase in the number of negative sentiment tweets originating from a given location of interest. Thus, the investigator would then hypothesise that some event may have occurred in that location and perform a more detailed investigation. On the other hand, the top-down approach allows the analyst to start with a hypothesis that they want to test, and examine different what-if scenarios in order to confirm or reject their hypothesis using the data. For example, the investigator may have a lead that two online personas are actually operated by the same criminal. He would then test this hypothesis using stylometric analysis, and the result would be the probability that this hypothesis is true.

V. Conclusion

In this paper, we have studied existing literature related to the area of cybercrime intelligence. We have investigated the different research problems tackled, and the associated techniques and methods used to solve them. We have discussed several research gaps found in the current literature relating to existing cybercrime intelligence frameworks. Based on previous research on user requirements related to cybercrime intelligence analysis, we present our initial design for the framework. One of the acknowledged challenges when designing generalized framework is that you loose specificity. Although our framework is multipurpose it is designed to accomplish specific functionalities for specific type of users (i.e., analysts). Future work will consist of developing this framework further, performing usability testing following concepts from human-computer interaction field, applying several case studies and evaluating them with law enforcement experts.

References

[1] Canadian Centre for Intelligence and Security Studies, "A framework for understanding terrorist use of the internet," Integrated Terrorism Assessment Centre (ITAC), Tech. Rep. Volume 2006-2, 2006.

[2] P. Reports, "Global Economic Crime Survey 2016: UK report," PWC, Tech. Rep., 2016.

[3] P. Hunton, "The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation," *Computer Law and Security Review*, vol. 27, no. 1, pp. 61 – 67, 2011.

[4] H. Jica, "Cooperation between cyber criminals and terrorist organizations," *Mediterranean Journal of Social Sci.*, vol. 4, no. 9, p. 532, 2013.

[5] K.-K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers and Security*, vol. 30, no. 8, pp. 719 – 731, 2011.

[6] R. Procter, J. Crump, S. Karstedt, A. Voss, and M. Cantijoch, "Reading the riots: what were the police doing on twitter?" *Policing and Society*, vol. 23, no. 4, pp. 413–436, 2013.

[7] Y. Lu, X. Luo, M. Polgar, and Y. Cao, "Social network analysis of a criminal hacker community," *Journal of Computer Information Systems*, vol. 51, no. 2, pp. 31–41, 2010.

[8] M. Edwards, A. Rashid, and P. Rayson, "A systematic survey of online data mining technology intended for law enforcement," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 15:1–15:54, Sep. 2015.

[9] M. Nouh and J. R. C. Nurse, "Identifying key-players in online activist groups on the facebook social network," in *2015 IEEE Int. Conference on Data Mining Workshops (ICDMW)*, Nov 2015, pp. 969–978.

[10] European Commission, "Towards a general policy on the fight against cyber crime," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF, 2007, [Accessed 11-May-2016].

[11] G. Urbas, K.-K. R. Choo, G. Urbas, and K.-K. R. Choo, *Resource materials on technology-enabled crime*. Australian Institute of Criminology, 2008.

[12] C. Hargreaves and D. D. Prince, "Understanding Cyber Criminals and Measuring Their Future Activity Developing cybercrime research," Lancaster University, Tech. Rep., 2013.

[13] D. S. Wall, "Policing cybercrimes: Situating the public police in networks of security within cyberspace," *Police Practice and Research*, vol. 8, no. 2, pp. 183–205, 2007.

[14] M. McGuire and S. Dowling, " Cyber crime: A review of the evidence. Home Office Research Report 75," Tech. Rep., 10 2013.

[15] The Global Affairs Canada, "Cybercrime," http://www.international.gc.ca/crime/cyber_crime-criminalite.aspx?lang=eng, 2015, [Accessed 11-May-2016].

[16] H. Sarvari, E. Abozinadah, A. Mbaziira, and D. Mccoy, "Constructing and analyzing criminal networks," in *Security and Privacy Workshops (SPW), 2014 IEEE*, 2014, pp. 84–91.

[17] J. F. Spencer, "Using xml to map relationships in hacker forums," in *Proceedings of the 46th Annual Southeast Regional Conference*, ser. ACM-SE 46. ACM, 2008, pp. 487–489.

[18] M. Ashcroft, A. Fisher, L. Kaati, E. Omer, and N. Prucha, "Detecting jihadist messages on twitter," in *Proceedings of the European Intelligence and Security Informatics Conference*, Sept 2015, pp. 161–164.

[19] H. Chen, W. Chung, J. Qin, E. Reid, M. Sageman, and G. Weimann, "Uncovering the dark web: A case study of jihad on the web," *J. Am. Soc. Inf. Sci. Technol.*, vol. 59, no. 8, pp. 1347–1359, Jun. 2008.

[20] T. Sabbah, A. Selamat, M. H. Selamat, R. Ibrahim, and H. Fujita, "Hybridized term-weighting method for dark web classification." *Neurocomputing*, vol. 173, pp. 1908–1926, 2016.

[21] M. Yang, M. Kiang, Y. Ku, C. Chiu, and Y. Li, "Social media analytics for radical opinion mining in hate group web forums," *Journal of homeland security and emergency management*, vol. 8, no. 1, 2011.

[22] M. McCord and M. Chuah, "Spam detection on twitter using traditional classifiers," in *Proceedings of the 8th International Conference on Autonomic and Trusted Computing*, ser. ATC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 175–186.

[23] K. Thomas, D. McCoy, C. Grier, A. Kolcz, and V. Paxson, "Trafficking fraudulent accounts: The role of the underground market in twitter spam and abuse," in *Presented as part of the 22nd USENIX Security Symposium*, Washington, D.C., 2013, pp. 195–210.

[24] A. Beutel, W. Xu, V. Guruswami, C. Palow, and C. Faloutsos, "Copycatch: Stopping group attacks by spotting lockstep behavior in social networks," in *Proceedings of the 22nd International Conference on World Wide Web*. ACM, 2013, pp. 119–130.

[25] R. M. Everett, J. R. C. Nurse, and A. Erola, "The anatomy of online deception: What makes automated text convincing?" in *proceedings of the ACM/SIGAPP Symposium on Applied Computing (SAC)*, April 2016.

[26] C. Yang, R. Harkreader, J. Zhang, S. Shin, and G. Gu, "Analyzing spammers' social networks for fun and profit: A case study of cyber criminal ecosystem on twitter," in *Proceedings of the 21st International Conference on World Wide Web*, ser. WWW '12. New York, NY, USA: ACM, 2012, pp. 71–80.

[27] G. Stringhini, O. Hohlfeld, C. Kruegel, and G. Vigna, "The harvester, the botmaster, and the spammer: On the relations between the different actors in the spam landscape," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '14. New York, NY, USA: ACM, 2014, pp. 353–364.

[28] A. Almaatouq, E. Shmueli, M. Nouh, A. Alabdulkareem, V. K. Singh, M. Alsaleh, A. Alarifi, A. Alfaris, and A. S. Pentland, "If it looks like a spammer and behaves like a spammer, it must be a spammer: analysis and detection of microblogging spam accounts," *International Journal of Information Security*, pp. 1–17, 2016.

[29] H. Chen, W. Chung, J. J. Xu, G. Wang, Y. Qin, and M. Chau, "Crime data mining: a general framework and some examples," *Computer*, vol. 37, no. 4, pp. 50–56, April 2004.

[30] V. Garg, S. Afroz, R. Overdorf, and R. Greenstadt, "Computer-supported cooperative crime," in *Financial Cryptography and Data Security*. Springer, 2015, pp. 32–43.

[31] P. Burnap, M. L. Williams, L. Sloan, O. Rana, W. Housley, A. Edwards, V. Knight, R. Procter, and A. Voss, "Tweeting the terror: modelling the social media reaction to the woolwich terrorist attack," *Social Network Analysis and Mining*, vol. 4, no. 1, pp. 1–14, 2014.

[32] C. Charitonidis, A. Rashid, and P. J. Taylor, "Weak signals as predictors of real-world phenomena in social media," in *Proceedings of the International Conference on Advances in Social Networks Analysis and Mining*, ser. ASONAM '15. ACM, 2015, pp. 864–871.

[33] Y. Zhang, S. Zeng, C. Huang, L. Fan, X. Yu, Y. Dang, C. Larson, D. Denning, N. Roberts, and H. Chen, *Developing a Dark Web collection and infrastructure for computational and social sciences*, 2010, pp. 59–64.

[34] J. Mei and R. Frank, "Sentiment crawling: Extremist content collection through a sentiment analysis guided web-crawler," in *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*, ser. ASONAM '15. New York, NY, USA: ACM, 2015, pp. 1024–1027.

[35] M. Bouchard, K. Joffres, and R. Frank, *Computational Models of Complex Systems*. Cham: Springer International Publishing, 2014, ch. Preliminary Analytical Considerations in Designing a Terrorism and Extremism Online Network Extractor, pp. 171–184.

[36] H. Chen, D. Zeng, H. Atabakhsh, W. Wyzga, and J. Schroeder, "Coplink: Managing law enforcement data and knowledge," *Commun. ACM*, vol. 46, no. 1, pp. 28–34, Jan. 2003.

[37] J. Xu and H. Chen, "Criminal network analysis and visualization," *Communications of the ACM*, vol. 48, no. 6, pp. 100–107, 2005.

[38] J. J. Xu and H. Chen, "Crimenet explorer: A framework for criminal network knowledge discovery," *ACM Transactions on Information Systems*, vol. 23, no. 2, pp. 201–226, Apr. 2005.

[39] A. Rashid, A. Baron, P. Rayson, C. May-Chahal, P. Greenwood, and J. Walkerdine, "Who am i? analyzing digital personas in cybercrime investigations," *Computer*, vol. 46, no. 4, pp. 54–61, 2013.

[40] J. Stasko, C. Görg, and Z. Liu, "Jigsaw: supporting investigative analysis through interactive visualization," *Information visualization*, vol. 7, no. 2, pp. 118–132, 2008.

[41] J. J. White and R. E. Roth, "Twitterhitter: Geovisual analytics for harvesting insight from volunteered geographic information," in *Proceedings of GIScience*, vol. 2010, 2010.

[42] G. Stringhini, P. Mourlanne, G. Jacob, M. Egele, C. Kruegel, and G. Vigna, "Evilcohort: Detecting communities of malicious accounts on online services," in *24th USENIX Security Symposium*. Washington, D.C.: USENIX Association, Aug. 2015, pp. 563–578.

[43] E.-C. Hillemann, A. Nussbaumer, and D. Albert, "The role of cognitive biases in criminal intelligence analysis and approaches for their mitigation," in *Intelligence and Security Informatics Conference (EISIC), 2015 European*. IEEE, 2015, pp. 125–128.

[44] R. J. Heuer, *Psychology of intelligence analysis*. Center for the Study of Intelligence. Lulu.com, 1999.

[45] S. Ó. Ciardhuáin, "An extended model of cybercrime investigations," *International Journal of Digital Evidence*, vol. 3, no. 1, pp. 1–22, 2004.